FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS

PLAN DE NEGOCIOS PARA LA CREACIÓN DE UNA EMPRESA QUE OFERTE SERVICIOS DE MONITOREO DE INCIDENTES INFORMÁTICOS LLAMADO SOC (SECURITY OPERATION CENTER) PARA INSTITUCIONES FINANCIERAS EN LA CIUDAD DE QUITO

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Ingeniero Comercial con mención en Finanzas

Profesor Guía

Carlos D. Valladares, MBA

Autor

Renato Sebastián Pulgar Montero

Año

2016

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido el desarrollo inicial de este trabajo orientando conocimientos y competencias al estudiante para dar fiel cumplimiento a las normas dispuestas por la Universidad que garantizan originalidad a los trabajos de titulación”

_____

Carlos D. Valladares, MBA
C.I. 100212276-8

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

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

Renato Sebastián Pulgar Montero

C.I. 171607080-8

AGRADECIMIENTO

Agradezco a mi familia por todo el apoyo y cariño, los cuales han sido parte fundamental para cumplir mis sueños, metas y caprichos. A Dios, por darme la sabiduría para guiar mis pasos al éxito. Por último, a los profesores que colaboraron con su tiempo y paciencia en esta investigación, Tamara Erazo; mi coordinadora de la carrera, Sandra Muñoz y mi profesor y tutor guía Carlos Valladares, por sus guías acertadas e incondicionales.

DEDICATORIA

Dedico este trabajo a mi hermano Ramiro Pulgar por darme la idea para realizar este proyecto, a mi padre por sus consejos, a mi madre por su infinito amor, a mis hermanos y sobrinos por su apoyo y paciencia en esos momentos que no pude estar con ellos. Por último, a Dios, “porque todo lo puedo en Cristo que me fortalece”. Zoe.

Resumen

Este plan de negocio tiene como finalidad solucionar y minimizar el riesgo operativo de los sistemas de seguridad informáticos de las instituciones financieras, las cuales son propensas a ataques de hackers o grupos organizados que tienen como propósito beneficios económicos y reconocimiento por sus actos delictivos. Además, la investigación tiene como objetivo identificar las oportunidades y amenazas de competir en una industria en crecimiento, frente a empresas con capitales extranjeros y años de trayectoria en el mercado.

Los cambios tecnológicos y la globalización hacen que países en vías de desarrollo, como Ecuador, no hayan experimentado ataques informáticos considerables en industrias públicas o privadas, y son vulnerables a las nuevas formas tecnológicas delictivas de personas y países que poseen la infraestructura, conocimiento y tecnología capaces de corromper los sistemas informativos de Estados no preparados para proteger la información de las personas y la economía de las industrias.

El plan de negocio propone la creación de la empresa Owl SOC, la cual desea introducir un servicio focalizado en brindar seguridad informática a entidades financieras de todo tipo en la ciudad de Quito las veinticuatro horas del día, los siete días de la semana y los trescientos sesenta y cinco días del año.

Abstract

This business plan intented to solve and minimize operational risk of computer security systems on financial institutions, which are prone to attacks by hackers or organized groups that are looking forward economic benefits and recognition for their criminal acts. Moreover, this paper aims to identify opportunities and threats to compete in a growing industry, against to companies with foreign capital and years of experience in the market.

Technological changes and globalization make developing countries, as Ecuador, have not faced significant cyber-attacks in public or private industries becoming vulnerable to new criminal technological forms from people and countries with an infrastructure, knowledge and technology capable of corrode informatics systems of states, which are not prepared.

This business plan propose the creation of an enterprise called Owl SOC, which want to introduce a focused service on providing security to financial institutions of all kinds in the city of Quito 24 hours a day, 7 days a week, and 365 days a year.

ÍNDICE

Capítulo I: Introducción

1.1 Justificación del trabajo:

Este plan de negocio se creó con el objetivo de solucionar los problemas de seguridad en los sistemas financieros de control de monitoreo para incidentes informáticos. Las instituciones financieras (bancos, cooperativas o mutualistas) no monitorean los incidentes de seguridad informáticos a cabalidad dentro de sus sistemas de control, los cuales albergan el funcionamiento de: bases de datos de clientes, correos electrónicos internos, cajeros automáticos y sistemas operativos institucionales. Esto es una oportunidad de mercado dentro del sistema financiero porque se ofrece a dichas instituciones un servicio para precautelar la confidencialidad y seguridad de sus sistemas.

Según las resoluciones JB-2012-2148 y JB-2014-3066 de la Superintendencia de Bancos tienen como objetivo establecer parámetros para el control y monitoreo de incidentes informáticos las veinticuatro horas del día y los siete días de la semana dentro de todas las instituciones financieras del país. Requerimientos como continuidad de negocio, gestión de incidentes tecnológicos, respaldo y control del flujo de información que albergan los servidores de las entidades financieras, confidencialidad de la información de cuentas bancarias, perfiles personales y claves de acceso. Estos parámetros son los que dan soporte a la prestación del servicio que se propuso para este proyecto.

Por esta razón, se fomentó el escenario propicio para ofertar un servicio que cubra las necesidades y requerimientos del mercado en la ciudad de Quito. Este plan de negocio fue necesario ofrecer debido a la falta de oferta nacional, la escasez de expertos focalizados en el control y monitoreo de incidentes informáticos es escaso. Además, las empresas que ofertan estos servicios son entidades con experiencia internacional. Países como Colombia y México han formado parte de nuevas iniciativas para dar soporte legal en contra de actos informáticos fraudulentos. Por esta razón, en Ecuador están apareciendo nuevas leyes que tienen como objetivo penalizar estos actos delictivos. La globalización es un factor de gran impacto en economías que se encuentran en crecimiento, las nuevas tendencias tecnológicas conllevan actos fraudulentos desconocidos para países en vías de desarrollo.

1.1.1 Objetivo general del trabajo

Determinar la factibilidad comercial, la viabilidad operativa y la rentabilidad financiera de una empresa especializada en brindar seguridad informática para las instituciones financieras en la ciudad de Quito, las cuales son propensas a ataques informáticos que vulneran el bienestar de sus acreedores e instituciones.

1.1.2 Objetivos específicos del trabajo

- Identificar las amenazas y oportunidades para minimizar el riesgo externo, e incrementar las oportunidades del emprendimiento.
- Realizar el estudio de mercado para determinar el perfil de los clientes institucionales y sus necesidades e identificar la competencia directa e indirecta.
- Plantear una estrategia general de marketing para establecer el correcto mix de marketing con el objetivo de llegar al cliente potencial
- Proyectar los estados financieros y flujos de caja para determinar la viabilidad financiera y comercial para reducir el riesgo de pérdida financiera, con el objetivo de mitigar las variables que impidan la ejecución de este plan de negocio.
- Identificar cuáles son los procesos operativos indicados para optimizar recursos económicos y de talento humano.

Capítulo II: Análisis del entorno

2.1 Análisis del entorno externo

Actualmente las entidades financieras en el Ecuador están atravesando por cambios estructurales en las leyes. El Código Orgánico Monetario y Financiero del 2014, establece parámetros de seguridad que garanticen el buen uso de las plataformas tecnológicas, ya sea al interior o exterior de las mismas. También, indica que los organismos controladores como la Superintendencia de Bancos (SB) y la Asociación de Bancos Privados del Ecuador (ABPE), los cuales mediante resoluciones y requerimientos ordenan el perfecto funcionamiento de sus plataformas tecnológicas para prestar servicios bancarios. Además, deben garantizar que los parámetros establecidos dentro del Código Orgánico Monetario y Financiero se rijan con la debida responsabilidad (Asamblea Nacional del Ecuador, 2014).

Es importante conocer que todas las entidades financieras ya sean privadas o públicas deben poseer sistemas de seguridad informáticos eficientes. Esto con el objetivo de reducir los riesgos de actos fraudulentos, ya sea extracción de información confidencial, desvió de fondos o penetración a los sistemas financieros mediante programas o aplicaciones maliciosas que atenten directamente al sistema financiero (SBS, 2016).

Por otro lado, a nivel mundial los cambios tecnológicos y la globalización conllevan nuevos retos para todos los países. En los últimos tres años varios Estados, principalmente los de primer mundo, han experimentado ataques informáticos llamados denegación de servicios o fraudes bancarios. Los hackers vulneran los sistemas de seguridad y extraen las bases de datos de empleados y clientes de las entidades financieras para acceder desde cualquier parte del mundo y extraer el dinero que sea posible o almacenar información para venderla a organizaciones delictivas. Como resultado, las instituciones financieras son más propensas a sufrir ciberataques. Por esta razón, deben precautelar su seguridad informática para no perder la confianza de sus clientes (Privacidad del internauta y delitos informáticos, 2016).

2.1.1 Entorno externo

2.1.1.1 Político – legal

En el inciso 4.3.8.7 de la resolución JB-2012-2148 de la Superintendencia de Bancos menciona varios requerimientos para las entidades financieras. Algunos de estos parámetros son: implementar sistemas de monitoreo y emitir alarmas en línea que informen oportunamente sobre el estado de los canales electrónicos, con el fin de identificar eventos inusuales, fraudulentos o corregir las fallas. (2012). Además, según el inciso 4.3.8.2 de la misma resolución, establece procedimientos y mecanismos para monitorear de manera periódica la efectividad de los niveles de seguridad implementados en hardware, software, redes y comunicaciones. Adicionalmente, cualquier otro elemento electrónico o tecnológico utilizado en los canales electrónicos, de tal manera que se garantice permanentemente la seguridad y calidad de la información. (Superintendencia de Bancos del Ecuador, 2012).

Actualmente, el país afronta cambios estructurales importantes dentro de los requerimientos fundamentales para el funcionamiento de la banca nacional. Estos cambios comprenden nuevas leyes y parámetros los cuales velan por la seguridad financiera de los involucrados. El 12 de septiembre de 2014 entra en vigencia el Código Orgánico Monetario y Financiero, el artículo 155-protección, menciona “En los términos dispuestos por la Constitución de la República, este Código y la ley, los usuarios financieros tienen derecho a que su información personal sea protegida y se guarde confidencialidad” (Asamblea Nacional del Ecuador, 2014). Con lo cual los sistemas financieros deben poseer sistemas óptimos para el control adecuado de información confidencial de los usuarios internos y externos.

Además, dentro de las leyes del Ecuador existen varias entidades reguladoras, que tienen el objetivo de establecer requerimientos esenciales con respecto al uso de plataformas informáticas que brindan las instituciones financieras a terceros. El Código Orgánico Integral Penal (COIP), en los artículos 178, 190, 211, 230, 232, y 229, los cuales pretenden defender y precautelar la intimidad e información proporcionada por el cliente, también reconoce el crimen informático como un delito penal dentro de la misma (2014).

Por otro lado, en el Reglamento de la Ley de Comercio Electrónico, firmas electrónicas y mensajes de datos (Decreto No. 3496), establece en el artículo 21 que:

> "los servicios electrónicos prestados que impliquen él envió por parte del usuario información personal, confidencial o privada, requerirá el empleo de sistemas seguros en todas las etapas del proceso de prestación de dicho servicio. Es obligación de la entidad comunicar al usuario acerca del tipo de seguridad que utiliza, alcances y limitaciones. En caso de no contar con algún sistema de seguridad, se debe comunicar al cliente de forma clara y previo al acceso a los sistemas o a la información, se debe comunicar los riesgos que pueden presentar estos sistemas" (2002).

En base a lo mencionado en esta sección del ámbito político – legal, es importante mencionar que existen leyes que soportan y penalizan actos informáticos fraudulentos, por esta razón, existe la infraestructura legal para fomentar la industria de seguridad informática.

2.1.1.2 Económico

Según el índice de Doing Business ecuador para el 2015 se encontraba en la posición 114, para el 2016 descendió 3 puestos ubicándose en el 117 (Grupo Banco Mundial, 2016). Por esta razón, la viabilidad para realizar negocios o emprender alguno no brinda facilidades, el riesgo económico de pérdida de capital de inversión para constituir y formalizar el plan es alto. Según este índice se demora alrededor de 51 días constituir una empresa con todos los requerimientos de ley.

La crisis económica que presentó el país en 2016 por la caída en los precios del petróleo, provocó que los ecuatorianos en promedio perciban menos ingresos. Esto conlleva a que las instituciones financieras tengan menor liquidez. Por lo tanto, mantener inversiones en sistemas de seguridad actualizados y eficientes no se podrían considerar como primera necesidad, mantenerse al margen con sistemas necesarios para no incumplir con la ley sería una alternativa a esta crisis nacional (Expreso.ec, 2016).

Según el análisis financiero en el sistema de bancos privados en el periodo diciembre 2014 – diciembre 2015, la solvencia económica, liquidez e intermediación aumentaron en 19,02% respecto al año 2014. Por otro lado, los activos, rentabilidad, cobertura y la eficiencia se redujeron, dando como resultado mayor morosidad de los depositantes con 0.79% más con respecto al año 2014. Además, el índice de depósitos a la vista y a plazo para el 2015 descendió 13,33% respecto al año 2014 (Estudios y análisis técnicos, 2015).

En el aspecto económico, los bancos presentaron dificultades para el año en curso, la liquidez se ve afectado por los índices de morosidad vinculados con la tasa de desempleo que afronta el país. La caída de los precios del barril de petróleo fue un factor determinante para las industrias y personas del país. Además, es desalentador conocer que las facilidades para emprender un negocio son barreras de entrada. El riesgo económico que presenta el país no fomenta la intrusión de capitales extranjeros y por ende genera menores probabilidades de competitividad frente a industrias extranjeras.

2.1.1.3 Social

Según el último censo realizado en el 2010, la población de pichincha (2´576.287) el 87.2% posee un celular, 26.2% tiene acceso a internet y el 52.3% tiene un computador o laptop (JC Magazine, 2015). Con lo cual se puede establecer patrones de tendencia en los cuales las personas tienden a usar en mayor proporción su teléfono inteligente para ingresar con mayor facilidad a instituciones bancarias u otros lugares en internet.

En la actualidad los métodos para sustraer información o dinero son avanzados y sofisticados, ya no se requiere de un arma o intimidación de por medio, sino que se usan métodos como ingeniería social con el objetivo de manipular a las personas a través de técnicas psicológicas y habilidades sociales para extraer información (Seguridad, cultura de prevención para TI, 2011), con el propósito que el afectado no se dé cuenta que está siendo atacado. De esta forma se recopila información para poder acceder a sus cuentas bancarias, redes sociales o mails (Curso Hacker.es, 2014).

Según un estudio realizado a 19.000 personas en 144 países con el objetivo de estudiar si son capaces de reconocer un mail falso de uno verídico de alguna institución o persona, se obtuvo que solo el 3% pudo reconocer un correo falso, el 80% fue víctima de Phishing. Con esto es suficiente para los criminales informáticos acceder a sus cuentas bancarias, mails personales y otros sistemas electrónicos mediante contraseñas y usuarios provistos por la víctima.

2.1.1.4 Tecnológico

El analfabetismo digital en los quiteños según el último censo del 2010 para hombres y mujeres mayores a los 10 años de edad es de 17.4% (Instituto Nacional de Estadística y Censos, 2010).

Por otro lado, ecuador está experimentando grandes cambios tecnológicos, uno de los más importantes y que han pasado desapercibidos es el uso del dinero electrónico. Actualmente existen 53.348 cuentas activas hasta diciembre del 2010. El Director General del Banco Central del Ecuador, menciona que alrededor de $645.669 circulan como dinero electrónico. Las principales provincias del Ecuador como: Pichincha presenta mayor participación en el uso de moneda electrónica con 29.65% y Guayas 24.97% (M2 Commerce LATAM news, 2015).

Además, existe un método llamado la clonación de tarjetas o Skimming. Mediante el uso de un lector que escanea los datos de la tarjeta de débito o crédito de la persona, esta información se pasa a un computador el cual emplea un software, los criminales pueden extraer datos como: número de la tarjeta, numero de seguridad (CVV), fecha de expiración, nombres y apellidos del apoderado (BBVA, 2015). Las personas desconocen estos métodos de robo, son resultado del desconocimiento y falta de cultura al momento de ingresar a instituciones financieras, no se toman las debidas precauciones para no ser víctimas de estos crímenes que pueden pasar desapercibidos. Además, existe otro tipo de método para pago con tarjetas de crédito mediante el uso del celular denominado Data Móvil, es un servicio en el cual se usa un dispositivo externo o lector de tarjetas de crédito y débito, en el cual con una aplicación en el teléfono celular se debita el saldo a pagar.

Como resultado de lo mencionado anteriormente, es claro observar que las tendencias tecnológicas y los grandes cambios dentro de las instituciones financieras requieren de plataformas seguras que protejan la información de sus usuarios. En el anexo 2 se menciona los conceptos de Phishing, Skimming y Spoffing.

2.1.2 Análisis de la industria (Porter)

En el sistema financiero del Ecuador, existen veintidós bancos privados, cinco bancos públicos, cuatro mutualistas, y cerca de novecientas cooperativas divididas en cinco segmentos (Superintendencia de Bancos del Ecuador, 2016). Estas instituciones financieras pueden convertirse en posibles clientes para la adquisición de servicios informáticos para asegurar sus sistemas electrónicos financieros.

Según la investigación realizada, la Superintendencia de Compañías clasifica el giro de negocio con respecto a la Clasificación Industrial Uniforme (CIIU4.0) con el CIIU: J6201.02 (Anexo1, Tabla 1). Dentro de esta clasificación existen pocos competidores, los cuales ya tienen presencia en el mercado con varios años de trayectoria.

Los principales competidores directos que ya brindan servicios de seguridad informática y soporte de tecnologías de la información para instituciones financieras son: Level 3 Ecuador LVLT S.A, Digiware seguridad del Ecuador S.A. y Blue Hat Consultores Cía. Ltda. Los primeros dos poseen amplia experiencia dentro de esta industria, ya que pertenecen a empresas internacionales con filiales en varias partes del mundo. El tercer competidor es una empresa ecuatoriana, pero con grandes clientes a nivel nacional.

2.1.2.1 Barreras de entrada

Las barreras de entrada son amplias, requieren especialización y diferenciación de los servicios, debido a que es un servicio focalizado y con exigencias gubernamentales y legales, es claro que este tipo de servicios requieren de valor agregado. El alto costo de licencias y la avanzada capacitación que requiere el personal para este tipo de servicios es de alto nivel. El perfil de profesionales requiere altos conocimientos sobre seguridad informática. El manejo de sistemas de hardware y software son de suma importancia.

2.1.2.2 Barreras de salida

Por otro lado, las barreras de salida, muestra un índice medio alto, debido a que se requiere de inversión especializada en activos intangibles como licencias de costos considerables. Estas licencias tienen periodos de caducidad lo cual no influye a largo plazo.

2.1.2.3 Rivalidad de los competidores

Con respecto a la rivalidad de los competidores es alto, ya que existen grandes posibilidades de adquirir amplios márgenes por ser un mercado en etapas de crecimiento. Además, por ser un servicio especializado es una gran ventaja porque permite incrementar el valor agregado del servicio prestado.

2.1.2.4 Poder de negociación de los clientes

Con respecto al poder de negociación de los clientes, es baja, ya que existen leyes como las resoluciones JB-2012-2148 y JB-2014-3066 de la Superintendencia de Bancos que les obliga a las entidades financieras adquirir sistemas de seguridad óptimos para la operación de las mismas.

2.1.2.5 Poder de negociación de los proveedores

Con respecto al poder de negociación de los proveedores como Amazon uno de los principales ejes para este plan de negocio. Este provee la plataforma en la nube para almacenar los sistemas de seguridad. Además, se encuentra CISCO, el cual vende productos de seguridad informática y conoce como operan este tipo de servicios. Debido a que es una industria especializada con pocos proveedores y el costo de los mismos son altos. Por lo tanto, tiene un nivel alto en poder de negociación de los mismos.

En el Anexo 1, tabla 3 se realizó un análisis numérico, con ponderaciones en escala de uno a cinco, siendo cinco la escala más alta (color en amarillo). Además, se hizo un promedio general entre las 5 fuerzas de Porter para establecer un número que mide si es o no atractivo entrar en esta industria, siendo uno no atractivo y cinco atractivo. Vale recalcar que, si es un cinco existe competencia fuerte, o si es el caso que sea un uno, puede ser que existen barreras de entrada y salida considerables con amplios márgenes de pérdida.

Por esta razón según lo mencionado en el párrafo anterior, se obtuvo 3.2 de atractividad, lo cual nos indica que es medianamente atractivo. Es claro que existen grandes amenazas como la integración vertical de los proveedores. Además, la especialización con respecto al servicio debe ser focalizado en prestación de servicios informáticos para instituciones financieras, con esto se observa que se debe tener en nómina a expertos en el tema (Porter, 2008). Por otro lado, esta industria tiene la oportunidad de implementar estrategias como: la integración entre empresas que brindan servicios similares o trabajar con los proveedores como socios en conjunto para brindar servicios complementarios.

2.1.3 Conclusiones

Según el Anexo 1, tabla 2, Matriz de Evaluación de Factores Externos (EFE), se pondera los elementos clave que se presentan como oportunidades y amenazas dentro del estudio político - legal, económico, social, tecnológico y PORTER del plan de negocio.

Oportunidades

1. Se puede evidenciar que, en las oportunidades, las leyes y resoluciones que exigen a las instituciones financieras adquirir sistemas de seguridad informáticos óptimos y eficientes deben garantizar la seguridad y confidencialidad de los datos almacenados dentro de estas instituciones. Con lo cual se pondera con 0.2 por considerarse la mejor oportunidad para ofrecer este tipo de servicios.
2. Además, los cambios tecnológicos y las nuevas tendencias en el uso de dispositivos electrónicos para realizar movimientos bancarios, esto genera oportunidades para los ciberdelincuentes. Se pondera con 0.08, no se considera mayor peso debido a las nuevas tendencias tecnológicas.
3. Del mismo modo, el auge de fraudes bancarios y ciberataques no son reconocidos actualmente en Ecuador. El desconocimiento de este tipo de ataques, pueden generar grandes pérdidas financieras, debido a la falta de capacitación y conocimiento acerca de este tipo de fraudes. Por esta razón, es crítico brindar este tipo de servicios e incluso ofertar consultorías corporativas a instituciones financieras. Se pondera con 0.2, es muy importante debido al desconocimiento de este tipo de delitos.
4. Existen pocas empresas que ofrecen servicios de seguridad informática a nivel nacional, las existentes poseen participación mediante la oferta de servicios paralelos y no totalmente focalizados en el control y monitoreo de incidentes informáticos.

Amenazas

1. Los cambios estructurales en las leyes gubernamentales pueden restarle importancia a la adquisición de servicios de seguridad informáticos complementarios que garanticen la seguridad de sus sistemas financieros. Se pondera con 0,07 debido al cambio gubernamental que se viene para el año 2017.
2. Además, la prolongación de la crisis nacional puede generar incertidumbre en los nuevos emprendimientos. Las instituciones financieras pueden bajar sus niveles de ingresos y por ende no adquirir servicios paralelos de seguridad informática. Se pondera con 0,03 debido a la fortaleza financiera de las instituciones financieras.

3. Mayor aceptación en empresas extranjeras que ya tengan experiencia en seguridad informática. Se pondera con 0,07 debido a la campaña gubernamental por la contratación preferente de empresas nacionales.
4. Aumento de la rivalidad de las empresas ya establecidas en esta industria. Su experiencia y capital extranjero les permite obtener con mayor facilidad nuevos clientes. Se pondera con 0,08 debido al nivel de capital que manejan las empresas ya establecidas.
5. Es importante mencionar, que una de las barreras de entrada y salida de mayor consideración es la especialización en equipos y licencias, las cuales tienen grandes costos de operación. La capacitación e inversión en personal tienen grandes costos. Se pondera con 0,1 debido a la importancia en la adquisición de equipos de gran capacidad operativa para operar eficientemente con información susceptible a delitos informáticos.

Capítulo III: Análisis del cliente

3.1 Investigación cualitativa y cuantitativa

Para el estudio de mercado, se utilizó dos tipos de metodologías que fueron: las encuestas y entrevistas a profundidad, con el objetivo de comprender los problemas y requerimientos del mercado potencial, establecer el perfil del cliente, así como tendencias de adopción del servicio y el proceso de adquisición para plantear estrategias de marketing acorde con las necesidades del mercado. Por otro lado, se realizó una entrevista a profundidad que tiene como objetivo comprender las normativas y leyes que impone la entidad reguladora.

Es importante mencionar que hubo un acuerdo de confidencialidad con la persona entrevistada de la entidad reguladora, que solicitó el sigilo de su información personal y de la institución en la cual trabaja. Se anexa la carta firmada, en la cual consta este acuerdo (Anexo 2).

Por otro lado, es importante mencionar que no se realizó el grupo focal en esta investigación, ya que no era posible reunir a las personas encargadas y principales clientes de este servicio. El perfil profesional de los encargados de la seguridad informática en las instituciones financieras son gerentes operacionales, oficiales de seguridad y otros que se encuentran dentro de las instituciones financieras. Debido a esto, era inalcanzable reunir a este grupo de profesionales para realizar el grupo focal. Por esta peculiaridad del presente plan de negocios, la dirección de titulación de la facultad aprobó sustituir el grupo focal a cambio de realizar como mínimo 4 entrevistas a profundidad a expertos en el tema.

3.1.1 Entrevistas a expertos

En el Anexo 2, se encuentran los datos personales y los perfiles profesionales de los entrevistados. La mayoría de los cuatro expertos consideraron que la globalización ha sido un factor de influencia dentro del comportamiento de las personas, con lo cual mencionan que las tendencias tecnológicas han permitido dar mayores facilidades a la sociedad en general. Además, se consideró que las personas en la actualidad usan con mayor frecuencia un dispositivo móvil para acceder a las plataformas que tienen las instituciones financieras. Se demuestra que el acceso a los bancos para el uso de banca virtual y consulta de estados financieros y transferencias bancarias es de mayor uso por la facilidad y seguridad para evitar grandes riesgos al acudir a un banco.

Además, los expertos mencionaron que en la mayoría de los casos de fraudes bancarios se debe al desconocimiento y negligencia de los usuarios de las plataformas y servicios virtuales. En general, ellos recomendaron tener conciencia propia y sentido común. Por otro lado, se encuentran las instituciones financieras, las cuales deben poseer sistemas de seguridad que cumplan con los requerimientos del organismo de control y normas PCI (Payment Card Industry) para poder operar con tarjetas de crédito o débito (Security Standards Council, 2016).

También, los expertos mencionaron que los ataques informáticos más comunes son el: Pishing, Skimming y Spoffing; en el anexo 2 se explica el concepto de cada termino. Además, las instituciones financieras en la actualidad son objetivo de ataques informáticos debido al desarrollo de nuevas tecnologías que han permitido el cambio estructural de los sistemas de seguridad informática dando apertura al conocimiento de vulnerabilidades que aún no son descubiertas.

Las instituciones financieras tienen la obligación de cumplir con las normas de la superintendencia de bancos. Con lo cual, la entidad reguladora establece normativas y requerimientos para la operación y prestación de servicios a la comunidad. Se encuentran las resoluciones que son de carácter público: JB2012-2148 del 26 de abril del 2012 y JB2014-3066 del 2 de septiembre del 2014. Además, de preferencia el ente regulador impulsa la adquisición de estos servicios por parte de empresas nacionales, por otro lado, si estos proveedores son extranjeros deben someterse a las auditorías internas y externas del ente regulador nacional.

Según los expertos que proveen servicios de seguridad informática a corporaciones e instituciones públicas y privadas, comentan que los sistemas de seguridad informática implementados por las instituciones financieras no son totalmente seguras, ya que todo lo que se encuentra en la red puede ser susceptible a alteraciones por parte de Malware, término que engloba a todo tipo de programa o código informático malicioso (Info Spyware, 2009). Ramiro Pulgar y Pablo Sosa, se dedican a prestar servicios para la detección de vulnerabilidades en los sistemas informáticos. Además, mencionan que debe existir previamente el análisis de riesgo operacional de los sistemas informáticos y reconocen que los proveedores de estos servicios también pueden estar sujetos a intrusiones maliciosas para desprestigiar y robar información confidencial sobre las entidades que se encuentran bajo su tutela de seguridad.

En relación a lo que los expertos mencionan, el SOC (Security Operation Center) tiene el objetivo de ofrecer el monitoreo de incidentes informáticos para identificar los riesgos que presenta una organización. Además, Pablo Sosa comenta que este servicio tiene varios alcances, los cuales varían con el entorno interno de la organización, ya que la infraestructura de seguridad implementada por la entidad maneja sus propios índices de riesgo e infraestructura de seguridad. Además, estas organizaciones por el tema que está atravesando el país prefieren contratar empresas externas que se encarguen de la parte operativa de seguridad de la información.

Con respecto al montaje y operación del SOC, se menciona que debe tener infraestructura como equipos de comunicación, firewalls, IPS, licenciamientos para administración de información, este último depende del servicio que se quiere prestar. Asimismo, Pablo Sosa comenta, que si se monta un SOC se recomienda proveer capacidades tecnológicas de amplio alcance, como sistemas antivirus, sistemas DOS y balanceo de carga de servidores y que esto esté presente los siete días de la semana y veinticuatro horas al día. Este servicio debe demostrar capacidad de operación con certificaciones internacionales como por ejemplo la ISO26000.

Por otro lado, los expertos mencionan que los costos para poder montar un SOC dependen del servicio que se quiere prestar, la tendencia para la adquisición de estos servicios es que no sean más caros que la solución, por ejemplo, si el monitoreo cuesta más que el servicio para solucionar el problema obviamente se pierde poder de negociación con el cliente. Por lo cual, el servicio debe estar por debajo del costo de solución para que sea atractivo la adquisición. Pablo, menciona que el costo para las entidades financieras varía de acuerdo a su tamaño de infraestructura tecnológica. En el caso de PYMES, puede estar entre $2.000 a $3.000, para grandes corporaciones puede superar tranquilamente los $20.000 mensuales.

Con respecto al área operativa y de costos, Pablo Sosa en la entrevista al experto, menciona que puede ser costoso equipar una empresa que brinde estos servicios de

seguridad. Sin embargo, contrasta la información con el objetivo y alcance que se quiera enfocar el proveedor. Este alcance trata sobre el tipo de servicio que se quiera prestar. Si es el caso de un SOC (Security Operation Center), puede sobrepasar una inversión por encima de los diez mil dólares solo en equipos. Además, menciona que este tipo de negocios contemplan inversiones de capital que sobrepasan el medio millón de dólares. También, establece que estas empresas manejan bajos índices de apalancamiento.

Con respecto a la industria Ramiro Pulgar menciona que este tipo de servicios para seguridad informática se encuentran en auge, son pocas las empresas nacionales que brindan estos soportes. Por último, Pablo Sosa comenta que la competencia se centra más en los proveedores extranjeros, los cuales poseen la infraestructura, capital y respaldo por las leyes de su país de origen.

3.1.1.1 Encuestas

Es importante mencionar, que las encuestas realizadas a las instituciones financieras que prestaron su ayuda en esta investigación, por asuntos de confidencialidad de la información proporcionada para la elaboración de la misma, requirieron que se guarde el sigilo correspondiente y se use para asuntos netamente académicos. Por esta razón en las encuestas no se especifica la institución financiera a la cual fue aplicada la encuesta.

Para el formato de la encuesta se utilizaron preguntas de opción múltiple, escala y abiertas. En su mayoría las instituciones con mayor accesibilidad para el levantamiento de información corresponden a cooperativas de ahorro y crédito y bancos privados.

En total se realizó las encuestas a cincuenta instituciones financieras. El 66% de los encuestados corresponde a cooperativas de ahorro y crédito; con el 28% se encuentran los bancos privados, y mutualistas con el 6% de participación.

¿Cuáles son los ataques informáticos más comunes que afrontan las instituciones financieras? Se encuentra el Pishing y Skimming con el 46 y 27% respectivamente. Además, estos ataques informáticos tienen la característica de ser ocasionales. Según las encuestas el 74% de los encuestados menciona que los ataques son ocasionales. Por otro lado, el 16% indica que son frecuentes.

Sin embargo, el 32% de las instituciones financieras, establecen que los análisis de los sistemas para detectar o prevenir fraudes electrónicos lo realizan de una o más veces al mes, o en casos particulares donde el departamento de riesgo establece que no es necesario implementar el control continuo, ya que depende del nivel de vulnerabilidades presentadas en un periodo.

Por otro lado, es importante mencionar que el presupuesto que asignan las instituciones financieras para la adquisición de estos servicios para seguridad informática, dependen del servicio que necesite la entidad. Además, el departamento de gestión de riesgos debe establecer cuáles son las necesidades a cubrir. Adicionalmente, el presupuesto puede estar por encima o por debajo del mismo, esto fue mencionado en la entrevista a Pablo Sosa. Según la encuesta el 30% de las instituciones asignan entre $5.000 a $10.000 mensuales. También existe un porcentaje que refleja que las instituciones financieras con menor capital comparadas con las grandes, establecen presupuestos por debajo de los $5.000 mensuales. Además, se encuentran las grandes instituciones financieras que, por su capacidad de generar y recaudar fondos, son más propensos a los fraudes electrónicos, con lo cual pueden llegar a presupuestar por encima de los $50.000 mensuales.

¿Cuándo realiza estos análisis y encuentra vulnerabilidades, que medidas toma su institución financiera al respecto? El 85% de los encuestados proponen la evaluación

del riesgo operativo para establecer parámetros de seguridad para la adquisición adecuada del servicio que vaya acorde a la vulnerabilidad que se presente.

Para la toma de decisión para la adquisición de estos servicios de seguridad informática el 58% corresponde al gerente del departamento de TICs y el 34% el oficial de seguridad o el llamado gerente operativo. Ellos por lo general presentan la información para que gerencia o el llamado oficial de seguridad del área de las TICs, busque soporte, consultoría o adquisición de hardware y software para disminuir o anular las vulnerabilidades presentadas.

Lo más importante para la adquisición de servicios para seguridad informática, según los encuestados el 32% mencionó que la confidencialidad de la prestación del mismo debe ser drástica, ya que se encuentra en las manos de los especialistas de seguridad informática la información sobre seguridad de sus sistemas bancarios. Además, mencionaron que el servicio post-venta (23%), eficiencia (15%) y precio (16%) deben reflejar la calidad del servicio adquirido.

Es claro que en la pregunta nueve, donde se consulta a los encuestados si tienen o no algún sistema de seguridad informático, programa, software o servicio externo para impedir amenazas informáticas. Según las normas de la entidad reguladora, todas las instituciones financieras deben poseer algún servicio anteriormente mencionado. Por lo tanto, todos los encuestados respondieron que si tienen algún sistema, programa o software para impedir ataques maliciosos.

El 64% de los encuestados mencionaron que están satisfechos con lo que el mercado ofrece con respecto a seguridad informática. El otro 36%, mencionó que estos servicios pueden generar incertidumbre, debido al manejo de información confidencial. Además, ya existen empresas que brindan estos servicios, pero por la falta de oferta en el mercado, estas empresas manejan altos precios, por lo tanto, un servicio de altos niveles de calidad puede ser muy costoso.

Por último, según los encuestados, mencionaron que existen varios canales para informarse acerca de estos servicios de seguridad informática. El 26% comentó que ciertas empresas realizan publicidad personalizada mediante el uso de mails corporativos, los cuales se centran específicamente en la entidad y en las necesidades que vayan acorde al tamaño y presupuesto que manejan las instituciones financieras. Además, el 22% tiene mayor acceso a través de portales web. También, existen las redes sociales, las cuales con el 21% se centran más en la propagación de publicidad masiva a través de redes sociales. Por otro lado, el 10%, mencionó que pueden buscar información a través de revistas especializadas. También, eventos o conferencias que se centren en la capacitación y prestación de servicios específicos para seguridad informática.

En conclusión, en base a los datos obtenidos mediante el uso de las entrevistas a profundidad y encuestas, se observa que existe un mercado potencial insatisfecho con lo que se ofrece actualmente a nivel nacional. Por otro lado, la entidad reguladora les exige a las instituciones financieras que cumplan con las normas y posean sistemas de seguridad que garanticen la confidencialidad y el funcionamiento adecuado de los sistemas informáticos.

Además, la adquisición del servicio depende de la necesidad que la institución requiera, con lo cual el tipo de servicio debe ser personalizado para que sea congruente con el análisis de riesgo operativo encontrado por la entidad financiera. Adicionalmente, la mayoría de las instituciones financieras presentan ataques informáticos en sus sistemas de seguridad. Por ende, existen oportunidades de crecimiento en esta industria.

Capítulo IV: Oportunidad De Negocio

4.1 Descripción de la oportunidad de negocio encontrada, sustentada por el análisis interno, externo y del cliente.

En el entorno externo se pudo observar varios puntos a favor. El primero corresponde al aspecto legal por parte del ente regulador, la Superintendencia de Bancos. El cual obliga a las instituciones financieras a adquirir software o hardware para blindar sus sistemas informáticos. También, es importante recalcar las leyes que actualmente están presentes en El Código Orgánico Integral Penal (COIP). Este reconoce el crimen informático como un delito penal, con lo cual las empresas que brindan seguridad informática tienen el respaldo para identificar y denunciar actos fraudulentos.

Por otro lado, una amenaza sería la crisis económica por la que atraviesa el país por la reducción de los precios del barril de petróleo y la apreciación del dólar, en el cual las empresas que tienen como mercado objetivo a las instituciones financieras pueden verse afectadas. Por carácter de priorización de recursos pueden apegarse al cumplimiento de la ley, pero pueden bajar la frecuencia de adquisición o contratación de servicios para seguridad informática.

Una oportunidad importante de mencionar, son los constantes cambios tecnológicos. Además, las instituciones financieras pueden tener sistemas de seguridad para ataques informáticos, pero esto no les garantiza que nuevos programas maliciosos estén por encima de estos sistemas bancarios. Por lo tanto, las empresas que brindan servicios de seguridad a cualquier entidad deben estar un paso al frente de las tendencias tecnológicas.

La industria a la cual apunta este plan de negocio se encuentra en desarrollo, prácticamente como mencionan los entrevistados, Ecuador todavía no experimenta ataques informáticos de grandes magnitudes. Pero aclaran que es cuestión de tiempo, en el cual posibles hackers pretendan introducirse a países en etapa de desarrollo tecnológico, el cual para ellos es fácil por la ausencia de sistemas de seguridad informáticos que garanticen la confidencialidad y seguridad de los acreedores de la banca nacional.

La competencia y la rivalidad de los competidores se centran en empresas extranjeras, los cuales por su experiencia y capital social pueden ser una gran amenaza para el emprendimiento de nuevos negocios alineados a esta industria. También se encuentran las empresas nacionales que tienen como estrategia de mercado, la asociación estratégica entre entidades extranjeras para fortalecer la presencia de la marca. Es claro que no se puede competir a la par con entidades extranjeras, pero es alentador saber que el Gobierno nacional promueve la empleabilidad de empresas nacionales.

Por último, todas las instituciones financieras sin importar el tamaño de su entidad, ya sean bancos privados, públicos, mutualistas o cooperativas de ahorro y crédito están sujetas a lo que les exige la entidad reguladora, por ende, deben tener sistemas de seguridad que monitoreen las veinticuatro horas del día los siete días de la semana. Por otro lado, con respecto a las entidades encuestadas, el 36%, comentaron que los servicios de seguridad informática generan incertidumbre en el cliente. Esto se debe al manejo de información que puede caer en malas manos, para estas entidades la calidad y confidencialidad del servicio es sumamente importante. Además, los entrevistados mencionaron que la falta de oferta y el crecimiento de esta industria hace que los precios de estos servicios de seguridad informática para cualquier entidad financiera, ya sea pública o privada sean caros, la falta de oferta hace que las empresas establecidas pongan precios altos al servicio, la calidad percibida por el cliente no tiene puntos de comparación debido a la escasez de oferta.

Por ende, es una gran oportunidad de negocio ofrecer servicios de seguridad informática debido a que el mercado se encuentra en etapa de crecimiento. También, por el desconocimiento de nuevos tipos de delitos que requieren de un computador para poder vulnerar sistemas bancarios los cuales, pueden generar grandes pérdidas económicas.

Capítulo V: Plan de marketing

5.1 Estrategia general de marketing

5.1.1 Mercado Objetivo

Se estableció el mercado objetivo hacia las entidades financieras en la ciudad de Quito. En total se encuentran veintidós bancos privados, cinco entidades públicas, diez sociedades financieras, cuatro mutualistas y cerca de novecientas cooperativas de ahorro y crédito divididas en 5 segmentos.

5.1.1.1 Segmentación Geográfica

Según la Superintendencia de Bancos, en la ciudad de Quito se encuentran las principales matrices de la mayoría de las entidades financieras. Diecisiete bancos privados, dos mutualistas, y más de veinticuatro cooperativas de ahorro y crédito divididas en cinco segmentos, todas estas entidades se encuentran dentro de la provincia de Pichincha, en la ciudad de Quito.

5.1.2 Propuesta de valor

Ofrecer al cliente potencial un servicio de seguridad de la información las veinticuatro horas del día los siete días de la semana, el cual tiene como objetivo principal el control y monitoreo de incidentes informáticos, mediante el uso de un SOC, el cual brinde calidad, eficiencia, servicio post venta y confidencialidad de la información de la entidad financiera. Es importante mencionar que el aspecto de confidencialidad de la información para la prestación de este tipo de servicios es de suma importancia, debido a la susceptibilidad que presenta el manejo de información de entidades financieras. Además, este servicio como beneficio para el cliente se basa en los requerimientos del mismo de acuerdo a su estructura de análisis de riesgo operacional. Asimismo, se busca identificar las vulnerabilidades de los sistemas informáticos y el origen del problema, para posteriormente solucionarlo mediante el uso de otro tipo de software para conocer el origen y magnitud del incidente.

5.1.3 Estrategia general de marketing

La industria de seguridad informática, ya sea para entidades financieras o empresas en general se encuentra en desarrollo, con lo cual, para establecer la estrategia general de marketing, se usa la estrategia del especialista (Lambin, 2009, pág. 287), enfocado con la estrategia de desarrollo de producto (Lambin, pág. 291) con el objetivo de mejorar las características del servicio. Además, con el posicionamiento de más por lo mismo, esto corresponde a entregar mayor servicio por el mismo precio.

Además, con esta estrategia se deseó mantener el precio para ser más competitivo frente a la industria. En comparación con la competencia esta no realiza análisis posterior a la detección de programas maliciosos para el cliente, sino que su función se limita a informar y no solucionar. Actualmente, según el experto Pablo Sosa, menciona que no existen empresas netamente focalizadas en el control y monitoreo de incidentes, sino que se basan en un pequeño control y mas no en la solución global para la detección del origen del mismo. Con estas estrategias se buscó optimizar el alcance del servicio y se busca especialización, ya que este plan de negocio apunta específicamente a instituciones financieras.

Esta industria por sus características de nicho de mercado y falta de oferta focalizada directamente al control y monitoreo de incidentes informáticos por parte de empresas nacionales, permite introducir servicios totalmente focalizados, en comparación a la

competencia que no posee especialización sino mantiene líneas de negocio complementarias. Esto permite que las estrategias escogidas sean propicias para la introducción de esta idea de plan de negocio en el mercado.

5.1.4 Posicionamiento

Para las instituciones financieras que brindan facilidades a los usuarios mediante el uso de plataformas virtuales, cajeros automáticos, mails de confirmación de identidad y otros servicios vinculados con plataformas tecnológicas, la empresa de seguridad informática “Owl SOC” es una institución que ofrece servicios de seguridad para el monitoreo de incidentes informáticos con el objetivo de identificar posibles vulnerabilidades en los sistemas conectados a una red, que garantice la seguridad y credibilidad en las capacidades del servicio para solucionar sus problemas de seguridad informática.

5.2 Mezcla de Marketing

Para la elaboración de la mezcla de marketing se usó el libro Marketing de Servicios de Christopher Lovelock y Jochen Wirtz. Se usará la metodología de este libro para focalizar el análisis de marketing hacia un servicio.

5.2.1 Personas

El personal dentro de la prestación de este servicio es sumamente importante, deben expresar seguridad y credibilidad. La imagen del consultor debe mostrar la experiencia suficiente dentro del área de seguridad informática, sus capacidades y fluidez de conversación con los clientes debe abarcar el conocimiento sobre los sistemas de seguridad que usan las instituciones financieras. Ramiro Pulgar, en la entrevista mencionó que el Ingeniero SIEM encargado de la parte operativa del SOC es el indicado para explicar al cliente el funcionamiento del mismo. Para el cierre de contratos y decisión se encuentra el Gerente general, el cual es el representante legal de la empresa.

La actitud y el comportamiento del consultor y el experto en seguridad informática deben mostrar alto grado de confidencialidad sobre el servicio a prestar, ya que los datos que entrega la institución financiera contiene información susceptible. Por ende, el encargado principal para el contacto oportuno es el ingeniero SIEM (Security Information and Event Manager), especialista en seguridad informática.

5.2.2 Proceso

El proceso para la adquisición de este servicio de seguridad informática para instituciones financieras parte de la necesidad básica del cliente. Según las entrevistas a los expertos, el departamento de análisis de riesgo de cada entidad financiera debe identificar cuáles son las debilidades y amenazas potenciales de sus sistemas informáticos. A partir del análisis propio de cada institución, se identifican cuáles son las necesidades de seguridad informática. Debido a esto, el primer contacto será con el personal a cargo del departamento de riesgos o el de tecnologías de la información y comunicación ya que, no es lo mismo un banco con grandes captaciones de dinero comparado con una cooperativa de ahorro y crédito puesto que, su estructura de seguridad y enfoque hacia plataformas virtuales son totalmente diferentes. Posterior a la identificación de cada entidad, el departamento encargado de la seguridad informática de la entidad financiera realiza el contacto con el experto o Ingeniero SIEM, con esto se realiza un análisis previo para recomendar el servicio al cliente.

El experto asesorará de manera inmediata que servicio va acorde a la circunstancia presentada. El área comercial cotizará y elaborará un presupuesto para que el cliente tenga claro cuál es el costo del servicio para controlar y monitorear sus sistemas propensos a ataques informáticos. Además, se mencionará que este servicio posee un análisis global, el cual incluye la detección y aviso oportuno del incidente. También, se

recomienda al cliente optimizar sus sistemas de seguridad para impedir ataques informáticos externos.

5.2.3 Entorno físico (imagen de la marca)

Para la presentación del local físico e imagen del personal de “Owl SOC”, la oficina en la cual va a operar, en su exterior se presenta el logo de la empresa. En su interior se encuentra las divisiones para cada área operativa. En las paredes se muestran los certificados y títulos obtenidos que avalan las habilidades de los expertos en seguridad de la información y certificaciones ISO, así como, la misión, visión, objetivos y valores de la entidad. Por último, el consultor entregará cartas de presentación con el logo y contactos de “Owl SOC” (2015, pág. 26).

5.2.4 Servicio (producto)

El servicio se enfoca principalmente en el control y monitoreo de incidentes informáticos las veinticuatro horas del día, los siete días de la semana de las entidades financieras, las cuales con permiso de las mismas y en base a contratos rigurosos de confidencialidad, permiten a Owl SOC manejar remotamente los servidores que albergan información como: cuentas bancarias, correos corporativos, banca virtual y otros sistemas sujetos a vulnerabilidades informáticas que el cliente desee monitorear para impedir accesos no permitidos. También se encuentran los avisos oportunos y recomendaciones para que la entidad financiera no sea víctima de ataques maliciosos.

5.2.4.1 Branding

Para la prestación de este servicio son importantes tres aspectos. El primero corresponde al posicionamiento del servicio. En segundo lugar, se encuentra el concepto del servicio y, por último, el entorno físico o imagen de la marca.

5.2.4.2 Concepto de la marca:

El nombre para la empresa va a ser “Owl SOC”, nombre compuesto por el servicio principal en abreviatura en idioma ingles (Security Operation Center), y por el nombre de un animal salvaje en idioma inglés, el búho (Owl).

El búho se utiliza debido a que es un animal capaz de mantenerse atento todo el tiempo, descansa por el día y se mantiene activo toda la noche. Con esto, se quiere mostrar que la marca posee la habilidad de mantenerse continuo en el monitoreo y control de incidentes informáticos, así como lo hace el búho. Además, por sus habilidades y sigilo en sus movimientos, es caracterizado como una de las aves más inteligentes que existen en el mundo. Tienen una visión excepcional dándoles la capacidad de ser muy buenos cazadores. Son animales pequeños, muy hábiles al momento de cazar, defenderse de sus depredadores y muy territoriales (Buhopedia, s.f.). Con esto se quiere mostrar fortaleza por las características y capacidades de competir y proteger al cliente, también se desea mostrar que este servicio se mantiene activo todo el tiempo. Además, el logo hace referencia al contenido de seguridad informática y contenidos de información colgadas en la internet.

Para el diseño del logotipo se usaron colores como el azul, negro y blanco. El azul es el indicado para promocionar servicios o productos con altas prestaciones tecnológicas. El blanco representa seguridad, positivismo, y simplicidad para servicios de tecnología o similares. Por último, el negro muestra poder, elegancia, formalidad, autoridad y fortaleza (Wbusable, s.f.).

Figura 1: Logotipo de Owl SOC.

Según el libro de Marketing de servicios, personal, tecnología y estrategia, menciona que existen tres tipos de atributos de un servicio (Wirtz, 2015, pág. 84)

5.2.4.3 Atributos del servicio

Tabla 1: Atributos del servicio

Atributos del Servicio		
Producto básico	**Servicios complementarios**	**Procesos de entrega**
Identificar vulnerabilidades en los sistemas informáticos	Posterior al análisis de agentes maliciosos, corregir los errores y vulnerabilidades con el uso de otro tipo de software y hardware.	Business to Business (B2B) con el cliente que tiene el poder de adquisición del servicio
Monitorear y controlar los sistemas informáticos, los cuales pueden arrojar alarmas inmediatas de intrusión de malware.	Capacitación al personal encargado de los sistemas de seguridad informático de la entidad financiera.	Según el análisis de riesgo por parte de la entidad financiera, se elabora el servicio especifico que vaya acorde a la vulnerabilidad detectada

Adaptado de Wirtz, J., & Lovelock, C. (2015). Marketing de servicios: personal, tecnología y estrategia.

5.2.5 Promoción

Es importante mencionar que la atención al cliente es un factor intangible pero importante al momento de tratar directamente con él. La promoción del servicio se basó principalmente en el cliente, con lo cual se establecen los siguientes medios estratégicos para impulsar la marca:

- Página web

El contenido de la página web debe resaltar y enmarcar la misión, visión, objetivos y valores de la empresa. Además, mencionar cuales son los servicios que ofrece, certificados que avalan la calidad y efectividad del experto en seguridad informática. También, publicaciones sobre tendencias tecnológicas con respecto a fraudes electrónicos y otro tipo de ataques informáticos. En adición, en la página se publicarán eventos relevantes relacionados a seguridad de la información. Asimismo, es importante mostrar la ubicación de la oficina y los contactos de la empresa. El costo para la elaboración de la página web para Owl SOC bordea los $500 anuales.

- Revista especializada

La revista para promocionar el servicio de este plan de negocio será IT Ahora. Revista reconocida a nivel nacional. IT Ahora publica 3.000 ejemplares cada bimestre, siendo el 39% de los lectores de esta revista de la ciudad de Quito. Los perfiles de lectores son de: CIO (Chief Information Officer), responsables de la TI de medianas y grandes empresas, encargados de las TICs, universidades y segmentos como actualidad, emprendimiento y otros relacionados con temas de tecnología. Esta revista tiene dos

segmentos específicos para el lanzamiento de productos o servicios relacionados con la industria de tecnología llamado “Actualidad IT” y “Emprendimiento” (IT Ahora la revista del lider de Tecnología, 2016). El costo de la publicación en esta revista es de $2.700 por tres publicaciones bimestrales pasando cuatro meses para cada una.

- Mails corporativos (mailing)

Para focalizar la promoción del servicio a través de las entidades financieras, se va a utilizar el método de mail masivo o llamado mailing, el cual tiene el propósito de centralizar la información sobre la prestación y efectividad del servicio. El costo anual de este software es de dos centavos por cada mail enviado, esta herramienta posee diseños automatizados los cuales no requieren de un diseñador de por medio para elaborar los mails. Además, esta herramienta permite pagar paquetes de mails mensuales o anuales. Como iniciativa para medir la aceptación con este método se comprará mil mails dando como total $19,99 al mes por este paquete (Mailify, 2016).

- Cartas de presentación

Se van a realizar cartas de presentación las cuales serán entregadas en cada visita a la entidad financiera. Además, estas cartas de presentación las tendrán el personal de la empresa para entregar en cualquier momento al cliente. Estas cartas contienen los contactos de Owl SOC, ubicación y direcciones web como mails corporativos y pagina web de la empresa. Esto tiene un costo de $150 por 300 cartas de presentación.

5.2.5.1 Promoción de ventas

Para todas las instituciones financieras que adquieran el servicio y desean tener un SOC, pueden acceder a un descuento del 10% al inicio del mes que lo adquieran. El precio tiene un descuento de $1.400 para el primer mes de operación del SOC con el cliente.

5.2.5.1.1 Eventos y convenciones

Cada año se participará en el campus party en Ecuador, como cede principal se encuentra la ciudad de Quito. Campus Party, es un evento tecnológico que se realiza cada año, en el cual se presentan expositores con grandes conocimientos tecnológicos. En su segmento llamado Start-up 360 & Makers Camp ellos dan cabida a 40 emprendimientos que se exhibirán durante los seis días del evento. Esto no tiene ningún costo, pero es requisito llenar el formulario para poder participar en este segmento. El costo para entrar al Campus Party es de $100 (sin acampar) y $130 (acampar), estos precios son para los seis días del programa. También, en este evento se encuentran grandes empresas que buscan invertir en proyectos innovadores. El objetivo de participar en esto es encontrar nuevos talentos y lo más importante tener apoyo de inversionistas para incrementar el valor de Owl SOC.

5.2.5.2 Relaciones públicas

Para fomentar las relaciones públicas se utilizará mails corporativos y la página web oficial de la empresa, con lo cual se busca focalizar las sugerencias, peticiones y necesidades en cuanto al requerimiento para expandir o reducir el servicio. Con respecto a las redes sociales, mediante el uso de Twitter se busca seguir a personas influyentes o empresas que tengan cuenta en esta red social. Con esto se busca escribir tweets periódicos que contengan información acerca de las tendencias e información sobre contenido de seguridad informática o eventos de tecnología. Por último, la red social no tiene como objetivo ser un canal de contacto directo con el cliente, sino un medio por el cual se informe acerca de los beneficios de tener un SOC. Esta red social no aplica ningún costo de publicación.

5.2.5.3 Fuerza de ventas y Marketing Directo.

El Ingeniero SIEM es el principal enlace entre la empresa y el cliente, el cual tiene el objetivo de demostrar las ventajas de poseer un SOC externo, una de ellas se encuentra en el manejo focalizado por una empresa especialista en incidentes informáticos. Además, no incurrir en una gran inversión en equipos avanzados en seguridad de la información, sino que ese costo lo asume Owl SOC. También, se encuentra el área comercial encargada de mantener contacto periódico con los clientes para facilitar información sobre el servicio. Por otro lado, la página web oficial, que tiene como objetivo actuar como fuerza de ventas mediante la técnica AIDA (atención, interés, deseo y acción) (Gestiopolis, 2011).

5.2.6 Punto de distribución

En el caso del punto de distribución para este servicio de seguridad informática el término de B2B Business to Business por sus siglas en inglés, es el más conveniente. Se relaciona al contexto del giro de negocio para este proyecto. La utilización de tecnología para seguridad informática por temas de protocolos que usan los bancos llamados HTTPS, para la transferencia de datos mediante el uso de canales cifrados condiciona el servicio a mantener parámetros de seguridad óptimos. Por lo tanto, esta metodología permite abaratar costos de desplazamiento de personal. También, permite dar mayor seguridad con mejor desempeño en el control y monitoreo del servicio (Master Magazine, 2016). La oficina en la cual va a operar Owl SOC, se encuentra en el centro norte de Quito en la Av. Naciones Unidas e Iñaquito en el edificio Metropolitan, este lugar es propicio por la presencia de grandes instituciones financieras.

5.2.7 Precio

Para establecer el precio del servicio se usó información de empresas comparables que ya brindan servicios de seguridad informática a instituciones financieras, empresas privadas y públicas en el Ecuador.

Mediante el uso de Benchmarking, se obtuvo precios aproximados de SOC´s de la competencia. La primera empresa Digiware con 17 años de experiencia en el mercado nacional e internacional, países como: Colombia, Perú y Ecuador. El experto Pablo Sosa, ex CEO de Digiware menciona que un SOC puede ir desde $12.000 a $20.000 mensuales. Por otro lado, Ramiro Pulgar menciona que Radical, Secure Soft, Level 3 y Cloud Sec, tienen precios para servicios de control y monitoreo de incidentes mediante el uso de un SOC que rodean los $16.000 mensuales. Por efectos de confidencialidad, los encargados de estas empresas solo mencionaron precios aproximados, los cuales se acercan a la realidad. No se obtuvo específicamente el precio detallado de un SOC. Por lo cual, estos precios corresponden al montaje de un SOC con las mejores prestaciones de calidad y eficiencia operacional. Por ende, se realizó un promedio entre los precios de la competencia, con lo cual se obtuvo un precio promedio de $14.000, este va a ser el precio que va a cobrar Owl SOC a sus clientes.

5.2.7.1 Benchmarking

Los parámetros comparables son los siguientes:

- Sistemas de Help Desk. Incluye el personal que está al frente del sistema de control (SOC). Ese personal se encuentra en tres turnos rotativos de ocho horas diarias los siete días de la semana para cumplir con el ciclo de veinticuatro horas y siete días semanales. Además, se encargan de visualizar y alertar las anomalías que generan el software que evalúa los servidores que se encuentran vinculados al SOC.
- Sistemas de correlación y administración de bitácoras. El software y hardware que se encarga de recibir los logs, estos son registros de actividad de un sistema, este guarda en un fichero de texto y se añaden líneas a medida que se realizan más acciones en el mismo (Desarrollaweb.com, 2016). Con esto se

quiere identificar cuáles son actividades normales y cuáles pueden ser comportamientos anómalos que pueden generar daños a los sistemas informáticos de la entidad financiera y al proveedor del servicio.

- Instalaciones físicas. Corresponden a la parte física del centro de control, el cual debe abastecer de espacio y recursos para el personal de Help Desk.

Tabla 2: Benchmarking

Benchmarking						
Empresas	**Digiware**	**Level 3**	**Secure Soft**	**Radical**	**CloudSec**	**precio promedio**
Precios comparables	$13.000,00	$ 12.000,00	$ 15.000,00	$ 16.000,00	$ 14.000,00	**$ 14.000,00**

Según los precios que cobran las empresas comparables para el montaje de un SOC para instituciones financieras fluctúa entre los doce mil y dieciséis mil dólares mensuales. Por esta razón según la estrategia de más por lo mismo se pone el precio de catorce mil dólares mensuales. El servicio incluye el control y monitoreo las veinticuatro horas del día, los siete días de la semana. Además, incluyen recomendaciones y avisos en tiempo real para que el cliente tenga conocimiento de las vulnerabilidades de sus sistemas informáticos.

5.3 Presupuesto de las 7 Ps

5.3.1 Personas

Para el presupuesto del personal de Owl SOC, se tomó en cuenta que, por los cambios tecnológicos y las nuevas tendencias del mercado es oportuno impartir capacitaciones trimestrales para mantener a la vanguardia al personal que se encuentra detrás del servicio de seguridad informática.

Tabla 3: Presupuesto de las Siete Ps (Personas).

Presupuesto de las 7 ps			
Personas	**cantidad**	**precio unitario**	**total**
Capacitacion a Help Desk	9,00	2.000,00	72.000,00
Capacitacion a Especialistas	2,00	2.500,00	20.000,00
TOTAL	11,00	4.500,00	92.000,00

5.3.2 Entorno físico

Tabla 4: Presupuesto de las Siete Ps (entorno físico).

Presupuesto de las 7 ps			
Entorno físico	**cantidad**	**precio unitario**	**total**
Cuadros para misión, visión, valores, objetivos	4,00	35,00	140,00
Cartas de presentación	300,00	0,50	150,00
Logo	1,00	10,00	10,00
TOTAL	305,00	45,50	300,00

5.3.3 Promoción

La revista especializada ITAhora accedió a promocionar este plan de negocio por motivos de emprendimiento. Las publicaciones son bimensuales, por lo cual, para la campaña de promoción del servicio para entidades financieras se lo va a realizar cada cuatro meses durante un año. Se pretende colocar información del plan de negocio en marcha a partir de su operación del primer año. La página web, tiene como propósito mejorar su diseño al transcurso del tiempo, por esta razón el precio del mismo se encuentra en la media del costo.

Tabla 5: Presupuesto de las Siete Ps (promoción).

Presupuesto de las 7 ps			
Promoción	**cantidad**	**precio unitario**	**total**
Mail masivo (mailing)	1.000,00	0,02	19,99
Revista especializada (ITAhora)	3,00	900,00	2.700,00
Página web	1,00	500,00	500,00
TOTAL	1.004,00	1.400,02	3.219,99
Costo entrada campus party (CP)	**cantidad**	**precio unitario**	**total**
Entrada simple seis dias	2,00	100,00	200,00
Entrada con derecho a acampar seis dias	2,00	130,00	260,00
TOTAL	4,00	230,00	460,00

5.4 Presupuesto 7ps proyectado.

Para la proyección de las siete Ps, se tomó en cuenta el crecimiento de la inflación en los últimos 15 años. Según los datos entregados por el Banco mundial, Ecuador presenta una inflación promedio entre los años 2002 – 2015 de 4,85% (Banco Mundial, 2016). No se consideró la inflación del año 2016 por que los precios ya se encuentran con la inflación del año en curso. A partir del primer año el gasto en las siete Ps crece de acuerdo a la inflación proyectada en base al crecimiento promedio de la inflación.

Tabla 6: Tabla de la inflación.

Inflacion proyectada					
2016	**2017**	**2018**	**2019**	**2020**	**2021**
4,34%	4,34%	4,75%	5,19%	5,67%	6,21%

Tabla 7: Presupuesto siete ps proyectado

Presupuesto 7 ps Proyectado						
Detalle	**AÑOS PROYECTADOS**					
	2016	**2017**	**2018**	**2019**	**2020**	**2021**
Cartas de presentación	153,00	159,64	167,22	175,90	185,88	197,41
Mail masivo (mailing)	20,39	21,27	22,28	23,44	24,77	26,31
Revista especializada (ITAhora)	2.754,00	2.873,55	3.009,95	3.166,17	3.345,85	3.553,47
Costo total presupuestado entrada con acampada CP	265,20	276,71	289,85	304,89	322,19	342,19
Página web	500,00	521,71	546,47	574,83	607,45	645,15
Capacitacion a Help Desk	72.000,00	75.125,61	78.691,58	82.775,76	87.473,27	92.901,12
Capacitacion a Especialistas	20.000,00	20.868,22	21.858,77	22.993,27	24.298,13	25.805,87

5.5 Proyección del precio.

Tabla 8: Proyección precio

Proyección precio						
Precio	**Años**					
	2016	**2017**	**2018**	**2019**	**2020**	**2021**
14.000,00	14.000,00	14.000,00	14.000,00	14.000,00	14.000,00	14.000,00

Para la proyección del precio, se mantuvo constante para que vaya acorde a la estrategia de más por lo mismo. Con lo cual, este precio se mantiene para la proyección de los seis años de este proyecto. Se desea mantener niveles de competitividad altos, ya que la competencia tiene conocimiento del mercado, y por ende se desea entrar con un precio promedio de la industria.

Capítulo VI: Propuesta de filosofía y estructura organizacional

6.1 Misión, visión y objetivos de la organización

6.1.1 Misión

Somos una empresa líder en seguridad informática, que brinda a nuestros clientes calidad, eficiencia y confidencialidad de la información para el control y monitoreo

constante de incidentes informáticos las veinticuatro horas del día, los siete días de la semana.

6.1.2 Visión

Owl SOC en cinco años quiere ser una empresa reconocida en las instituciones financieras del Ecuador. Además, expandir su línea de negocios hacia el área comercial y de servicios complementarios para brindar capacitaciones a personas que deseen obtener conocimientos sobre seguridad informática.

6.1.3 Objetivos

6.1.3.1 Mediano plazo

- Aumentar la frecuencia trimestral de capacitaciones del personal de Owl SOC a periodos bimensuales con el objetivo de incrementar la eficiencia de los mismos.
- Incrementar el número de clientes en 20% trimestralmente hasta el año tres.

6.1.3.2 Largo plazo

- Con el objetivo de reclutar perfiles potenciales se realizará eventos anuales a partir del quinto año en universidades técnicas como: la Politécnica Nacional, Politécnica del Ejercito y otras que tengan altos índices de estudiantes que estudien ingenierías afines al tema de seguridad informática,
- Realizar alianzas estratégicas con empresas similares que presten servicios de seguridad informática ya sean públicas o privadas al cabo del quinto año, con el objetivo de mejorar la imagen de la marca y el reconocimiento por parte de los competidores directos. Estas asociaciones deben representar el 5% de las empresas competidoras dentro de la industria.

6.2 Plan de Operaciones

6.2.1 Arquitectura de un SOC

Esta estructura de operación del SOC abarca ocho etapas (Security Operation Center "Colombia", 2008).

- Dimensionamiento

Esta etapa pretende delimitar el alcance al cual se quiere llegar. La limitación objetiva enfoca estrategias para que exista mayor eficiencia en la captura de tráfico informático o los llamados logs. Esta etapa el Ingeniero especialista muestra el alcance del servicio para dar opiniones sobre que plataformas pueden estar bajo el control del SOC.

- Métricas y afinamiento

Esta etapa en conjunto con el dimensionamiento pretende conocer en términos cualitativos los activos que deben implementare para el control y monitoreo que vayan acorde al perfil de riesgo del cliente. Los Ingenieros SIEM y los administradores de incidentes evalúan cuales son las herramientas como software y hardware que se deben emplear en el servicio.

- Recolección

El objetivo es conocer previo a un análisis el máximo de incidentes informáticos con carácter de importantes proveniente del flujo de internet. En esta etapa se instalan herramientas informáticas para la detección oportuna de incidentes informáticos. Es importante mencionar que un evento, es una situación que puede ser ocasional en un período corto de tiempo. Por otro lado, un incidente es un evento que tiene la característica de dañino, el cual ha vulnerado las políticas y los protocolos de la entidad. El personal de Help Desk, los cuales están en permanente monitoreo de los sistemas de seguridad, son los que evalúan los elementos correlacionados por el software. Ellos poseen escalas o niveles los cuales se califican en tres categorías, leve, moderado y grave.

- Detección

La entidad financiera menciona cuales de sus plataformas virtuales pueden ser vulneradas y son posibles objetivos de intrusos como: banca virtual, mails corporativos, depósitos o trasferencias electrónicas y otros sistemas que se encuentran vinculados a la red de internet, pueden estar comprometidos y vulnerados. Con este análisis se muestra cuáles de ellos tienen mayor índice de riesgo para la entidad financiera. En la detección, el personal de Help Desk debe reportar a los especialistas para tomar decisiones, como intervenir o acudir directamente con el cliente para informar el nivel de riesgo que puede ser víctima.

- Análisis

En esta etapa se realizan las correlaciones cruzadas de todos los eventos recolectados en la etapa tres. Este análisis tiene la característica de poseer niveles, los cuales escalan de acuerdo al nivel de riesgo del incidente encontrado. El primer nivel, se encarga Help Desk de correlaciones que pueden solucionar sin intervención del especialista. Por otro lado, el segundo nivel, comprende acciones que pueden ser manejadas por los operadores encargados del monitoreo pero que tienen la probabilidad de ser graves, por ende, puede ascender al nivel de los especialistas. El tercer nivel reporta al encargado principal del SOC o Ingeniero SIEM, el cual es el que toma la decisión de categorizar al incidente informático de acuerdo a su nivel de riesgo. Este nivel va de leve, moderado y grave. En el anexo 4 se muestra un ejemplo de análisis de eventos presentados en un periodo de tiempo. Además, se muestra un bosquejo de cómo funciona un SOC en los varios niveles operativos del mismo.

- Acción

Los sistemas del SOC y los operadores del mismo observan la evaluación del evento presentado. Con esto se toman acciones de informar, contrarrestar o eliminar la amenaza presentada. Help Desk y los especialistas deben tomar las mejores decisiones para eliminar el incidente informático.

- Respuesta

En base a la etapa de acción, la respuesta tiene el objetivo de tomar decisiones oportunas y claras para mitigar el riesgo. Esta respuesta puede ser de carácter drástico o permisivo, en el cual el permisivo depende de la decisión del cliente en cuanto a las normativas que aplica la entidad financiera. En este caso, los especialistas y el Ingeniero SIEM, presentan las estadísticas del sistema para plantear posibles mejoras en los sistemas informáticos del cliente.

- Mantenimiento

La última etapa tiene el objetivo de corregir y detectar posibles falencias que se presentaron en el primer instante del control y monitoreo del SOC. Además, comprende las sugerencias por parte del proveedor, en el cual incluyen mejoras de las políticas de seguridad internas del cliente. El gerente general pide reportes sobre las acciones que se tomaron por parte de los especialistas y el Ingeniero SIEM, con el objetivo de establecer mejoras en los sistemas de seguridad del servicio y del cliente.

En el anexo 2 se muestra la cadena de valor de Owl SOC.

6.3 Estructura Organizacional

6.3.1 Estructura legal

Owl SOC se constituirá como sociedad anónima. Debido a que este tipo de negocios necesita grandes aportes de capital, lo cual genera un alto riesgo para los socios, el alcance de la responsabilidad de los mismos se limita al capital aportado. Además, esta figura legal permite aumentar aportes de capital, lo cual crea mayor capitalización

de la empresa. Para la constitución de la empresa el capital mínimo es ochocientos dólares americanos, esto corresponde al capital aportado por los socios.

6.3.2 Diseño organizacional

Debido a que el giro de negocio trata sobre la prestación de un servicio de seguridad informática que opera las veinticuatro horas del día, los siete días de la semana, la estructura organizacional es de carácter funcional. Además, cada área tiene asignado tareas especializadas. A la vez, la escala es jerárquica con tendencia vertical. Esto responde al nivel de riesgo que se presente. El área administrativa, se enfoca en la operación en cuanto a contacto con futuros clientes, gastos administrativos y otros.

6.3.2.1 Gerencia

Junta de accionistas: tienen como función:

- La integrarán los socios que aportan capital en la empresa. Pueden ser, empresas que deseen trabajar en sociedad o capitales que apoyen emprendimientos tecnológicos. Adicionalmente, tomarán decisiones con respecto a expansión de capital y autorizarán el pago de dividendos o a la vez retener las ganancias para aumentar la capitalización de la empresa. Además, nombrarán y ratificarán a la gerencia general.

Gerente General: tiene como funciones:

- Tomará decisiones estratégicas para la optimización de recursos económicos, con el objetivo de presentar a los accionistas los resultados dados en el periodo. Informará a la junta de accionistas acerca de los estados financieros. Además, tomará decisiones estratégicas correspondientes a adquisición y renovación de equipos, licencias y otros. También, contactará y creará vínculos con empresas similares para trabajar en conjunto. También, buscará y reclutará personal especializado en seguridad informática.
- Es la persona que se encargará de los asuntos legales de la empresa en otras palabras es el representante legal de la compañía.

6.3.2.2 Área administrativa

Jefe comercial: tiene como funciones:

- Buscará nuevos clientes con el objetivo de aumentar las relaciones con entidades financieras y Elaborará proformas y cotizaciones acordes al servicio que el cliente requiera. Por último, se encargará de gestionar las promociones y publicidad de la empresa.

Contador: tiene como funciones:

- Facturará y cobrará los servicios prestados. Además, evaluará los costos que la empresa genera en cuanto a costos fijos y variables. Además, Determinará la viabilidad de prestar el servicio al cliente en cuanto a costo beneficio de brindar el mismo. Por último, se encargará de administrar los ingresos y egresos que se generen en la empresa.

6.3.2.3 Área operativa

Administrador de incidentes: tiene como funciones:

- Gestionará el contacto con el encargado de seguridad informática del cliente y comunicará con la brevedad posible incidentes informáticos de carácter de alto riesgo. Además, tomará estrategias para la mitigación y el control eficiente de incidentes informáticos y analizará a profundidad los riesgos presentados a diario en los sistemas de detección de intrusos (IDS) por sus siglas en inglés y malware.

- Como perfil profesional, es un ingeniero en sistemas con certificaciones internacionales en análisis forense y gestión de riesgos operacionales.

Analistas de nivel uno y dos: tienen como funciones:

- Encargados de monitorear el flujo de datos que se generan en la red e Identificar las correlaciones de incidentes que pueden escalar a un riesgo más alto. Asimismo, comunicarán al superior o al ingeniero encargado de gestionar las alertas de seguridad SIEM o Security Information and Event Manager es el que realiza análisis de los datos que se crean en tiempo real, gestiona las alertas de seguridad generados por el hardware y software de la red (Seguridad X, 2013). Además, deberán brindar el soporte constante a los clientes y a las herramientas de hardware y software que se encargan de la parte de automatización del manejo de eventos e incidentes informáticos que se realizan en el flujo de la red.
- Como perfil profesional son ingenieros en sistemas o afines, los cuales posean conocimientos sobre seguridad informática, también, conocimientos de hackeo ético, para operar directamente con las herramientas de seguridad.

Ingeniero (SIEM): tiene como función:

- Analizará los datos proporcionados por los analistas del nivel uno y dos y gestionará las alarmas cuando se presenten casos de riesgo considerable para el cliente. Además, Comunicará al administrador de incidentes los análisis correspondientes a eventos que pueden generar daños al cliente y autorizará inspecciones o mantenimientos a los sistemas de seguridad y equipos del SOC.
- Como perfil profesional es un ingeniero en sistemas o afines con conocimientos específicos en gestión de riesgo operacional, análisis forense, hackeo ético y certificados que avalen el conocimiento sobre seguridad de la información.

En el anexo 3 se presenta el flujograma de operación de Owl SOC.

Capítulo VII: Evaluación financiera

7.1 Proyección de estados de resultados, situación financiera, estado de flujo de efectivo y flujo de caja

7.1.1 Estado de resultados

Para la proyección del estado de resultados, Owl SOC empezará con un cliente durante los primeros seis meses de operación. Según el experto Pablo Sosa, las empresas netamente focalizadas en este tipo de servicios empiezan con pocos clientes debido al desconocimiento y credibilidad en el mismo. Además, menciona que las empresas nacionales que brindan servicios de seguridad mediante un SOC pueden tener más de veinte clientes en su cartera. Por otro lado, señala que el crecimiento en la adquisición de nuevos clientes depende del marketing y calidad del servicio. Con lo cual se modeló una curva gradual de ingresos que sigue la tendencia del margen de ganancias de empresas comparables. Los activos intangibles, especialmente el software de seguridad informática que sobrepasa los cien mil dólares con vigencia anual, para el primer año corresponde cerca del 22.39% de los gastos. Además, debido al nivel de personal capacitado con amplios conocimientos en seguridad informática los salarios administrativos corresponden el 57.13% de las ganancias netas del primer año. También, se espera para el tercer año ganancias en la empresa y para los años posteriores al mismo, cuando las ventas se estabilicen, va haber un crecimiento promedio de 48% en los últimos tres años proyectados (Anexo 5). Así mismo, Para el tercer año de operación de la empresa se va a invertir capital para expandir el número de personas, con el objetivo de duplicar la cantidad de especialistas, analistas de nivel uno y dos o los llamados Help Desk e ingenieros SIEM. Esto se debe al crecimiento pronosticado de clientes para el año 2018 con 10

instituciones financieras en cartera. Por último, se utilizó la curva de adopción de nuevos productos para la proyección del crecimiento de la empresa.

7.1.2 Estado de situación

Los supuestos para los estados de situación se explican con más detalle en el anexo 5. Debido, al riesgo que representa adquirir préstamos para este giro de negocio, los expertos mencionaron que los niveles de apalancamiento corresponden a mayores aportes de capital. Según los estándares de la industria las cuentas por cobrar tienen como política de cobro 30 días debido a que es un servicio mensual con ventas al contado de 60% y crédito de 40%. En el caso de los activos no corrientes, como propiedad, planta y equipo; el primer año tienen una participación del 11.02% del total de activos de ese periodo, incluso este porcentaje se incrementa a medida que la empresa expande su personal en el periodo 3 de la proyección del estado de situación. (Anexo 6)

7.1.3 Flujo de efectivo

El flujo de efectivo se realizó con el método indirecto. Debido a la gran inversión en equipos, licencias y personal, se inyectó $400.000,00 dólares para el primer año. Según Pablo Sosa, en la entrevista mencionó que las empresas que brindan seguridad informática establecen rondas de capital semestrales o anuales y que en promedio se introduce entre medio millón a más de un millón de dólares para el primer año de operación. Por ende, las rondas de capital para el flujo de efectivo del proyecto alcanzaron $ 680.000,00 para los seis años proyectados. (Anexo 7)

7.1.4 Flujo de caja

Para el método de flujo de caja libre o FCF por sus siglas en ingles. Se usó el método de Aswath Damodaran. También, para el cálculo del valor terminal se realizó una perpetuidad creciente tomando como tasa el promedio de la inflación de los últimos diez años con 4,23%. Así mismo, la beta no apalancada se tomó del sector de servicios informáticos de Estados Unidos con 0,94 (Damodaran, 2016). Además, para la prima de mercado se usó la tasa de 12,6%, esta corresponde a la prima promedio de Ecuador (Fernandez, Ortiz, & Acín, 2016). Adicionalmente, para la tasa libre de riesgo se tomó de los bonos americanos a treinta años, con un valor de 2,45% (Yahoo Finance, 2016). Con lo mencionado anteriormente, se obtuvo un VPN de $ $3.177.002,80 (Anexo 7)

7.2 Inversión inicial, capital de trabajo y estructura de capital

7.2.1 Inversión inicial

Para la inversión inicial del proyecto se necesita $178.900,00, esta comprende los gastos pre-operacionales, las dos licencias de software para hacer pruebas operativas, muebles de oficina y equipos de computación (Anexo 7).

7.2.2 Capital de trabajo

Las rondas de capital para asumir las pérdidas ascienden a los $ 680.000,00. La primera corresponde a una ronda de $400.000,00. Así mismo, la segunda es en el año siguiente por un valor de $150.000,00. Por último, en el tercer periodo se inyecta $130.000,00 (Anexo 7).

7.2.3 Estructura de capital

Para la estructura deuda capital se usó una razón 33% deuda y 67% capital. Con el objetivo de soportar la inversión inicial la deuda ayudaría como escudo fiscal. Además, se desea mantener cierto nivel de deuda, el cual en el quinto año se asume completamente el pago de la misma. (Anexo 7).

7.3 Estado y evaluación financiera del proyecto

Según la valoración realizada en el flujo de caja libre, el Valor Presente Neto o VPN es de $3.177.002,80. Además, es importante mencionar que para el cálculo de la perpetuidad la tasa de crecimiento es el promedio de los últimos diez años históricos del comportamiento de la inflación con un g de 4.23% para los seis años proyectados. De esta forma, la Tasa Interna de Retorno o TIR tiene una tasa de 68%. Así mismo, el Índice de Rentabilidad o IR, por cada dólar invertido se obtiene $18.76. Por último, el periodo de recuperación contable se ubica en el quinto año del proyecto. El plan de negocios tiene perspectivas positivas debido a la viabilidad optimista del VAN, la TIR y el índice de rentabilidad (Anexo5).

7.4 Indicadores financieros

Para los indicadores de liquidez no pueden ser comparables, ya el proyecto no tiene pasivos corrientes. Además, los indicadores de solvencia o endeudamiento promedio de Owl SOC se encuentra muy por debajo de la industria, la misma usa 88,61% de razón D/E y el proyecto mantiene un endeudamiento promedio de 14,25%. Esto quiere decir, que la empresa en su mayoría no tiene endeudamiento, sino mayores aportes de capital accionario. Por otro lado, los indicadores de rentabilidad ROE y ROA, con 58,69% y 21,90% respectivamente, sobrepasan la industria (ROE industria, 19,80 y ROA industria 9,99%). Sin embargo, los indicadores de actividad o rotación están por debajo de la industria debido a que el giro de negocio por poseer un precio alto con grandes prestaciones tendrá mayor margen, pero menor rotación de activos, lo cual se compensa por un margen neto más amplio. Con lo cual, se obtiene una rotación de cartera promedio de 25,63 veces comparado con las 43,98 veces de la industria. Además, la rotación de ventas está muy por debajo de la industria con 3,59 veces comparado con las 13,73 veces de la misma.

Capítulo VIII: Conclusiones Generales

- Las leyes gubernamentales y de las entidades reguladoras como: la Superintendencia de Bancos, la Asociación de Bancos privados del Ecuador y el Código Orgánico Integral penal, son los principales factores los cuales sustentan la viabilidad de emprender este plan de negocio.
- La entidad reguladora por sus parámetros en cuanto a requerimientos para adquirir servicios de seguridad informática para todas las instituciones financieras del país hace propicio el ofrecimiento de un servicio de seguridad de la información focalizado al control y monitoreo de incidentes informáticos los trescientos sesenta días del año.
- Los cambios tecnológicos y por ende la globalización, son factores en contra de las entidades financieras debido a que son vulnerables a los ataques de hackers que quieren sacar ventaja en un país que desconoce este tipo de delitos informáticos. Con lo cual, es beneficioso para emprender el proyecto debido a la escasa oferta en el mercado nacional de empresas focalizadas en seguridad informática.
- Según los expertos en seguridad de la información, la fuerte competencia es una amenaza importante en esta industria debido a que las empresas constituidas poseen líneas de negocio que sustentan la amplia inversión para poder operar con equipos tecnológicos que soporten las exigencias del cliente.
- Amenazas como los cambios gubernamentales, los altos costos en equipos y licencias especializadas hacen que este plan de negocio necesite una amplia inversión en capital de trabajo y propiedad planta y equipos.
- La crisis que atraviesa el país vulnera la estabilidad económica de los bancos y de los nuevos emprendimientos.
- Las estrategias de marketing como: la estrategia de especialización y desarrollo del producto permiten focalizar y personalizar el servicio hacia las instituciones financieras. Además, competir con los precios del mercado mediante la estrategia

de más por lo mismo tiene como objetivo desplazar a empresas competidoras que manejan precios por encima de lo que el cliente y la crisis nacional lo permite.

- Los costos operacionales, salarios, capacitaciones, adquisición de licencias y equipos especializados en seguridad informática son factores en contra que vulneran la viabilidad del plan de negocio.
- La falta de información y los aspectos de confidencialidad de las personas e instituciones que aportaron con su tiempo para la realización de este proyecto no proporcionaron aspectos detallados sobre costos, precios y aspectos operativos, lo cual hace que este plan de negocio obtenga estimaciones aproximadas a la realidad.
- La parte financiera en este plan de negocio, la viabilidad de la misma depende en su mayoría de los aportes de capital de empresas inversoras que deseen entrar en un nicho de mercado, la ventaja de esta industria es la etapa en la que se encuentra la misma, esta corresponde a una etapa en crecimiento debido a las tendencias tecnológicas que el país está presenciando.
- En general este plan de negocio tiene un aspecto positivo a mediano plazo, se espera un auge exponencial de delitos informáticos debido a las crisis políticas que presentan todos los países en el mundo.

REFERENCIAS

Asamblea Nacional del Ecuador. (12 de Septiembre de 2014). *Código Orgánico Monterario y Financiero*. Recuperado el 16 de Marzo de 2016, de www.sbs.gob.ec/.../codigo_organico_monetario_financiero_sept_14.doc

Banco Mundial. (2016). *Datos*. Recuperado el 2 de Mayo de 2016, de http://datos.bancomundial.org/pais/ecuador#cp_fin

Batrankov, D. (3 de Octubre de 2016). *Building Security Operation Center*. Recuperado el 10 de Junio de 2016, de http://www.slideshare.net/CERT-GOV-MD/awal-sioc-batrankov

BBVA. (1 de Octubre de 2015). *Skimming: la estafa de la clonación de tarjetas*. Recuperado el 16 de Marzo de 2016, de https://info.bbva.com/es/noticias/asuntos-sociales/gente/skimming-la-estafa-la-clonacion-tarjetas/

BBVA. (1 de Octubre de 2015). *Skimming: la estafa de la clonaciòn de tarjetas*. Recuperado el 10 de Abril de 2016, de https://info.bbva.com/es/noticias/asuntos-sociales/gente/skimming-la-estafa-la-clonacion-tarjetas/

Buhopedia. (s.f.). *Características del Búho*. Recuperado el 21 de Abril de 2016, de http://www.buhopedia.com/caracteristicas-buho/#libro-as

Curso Hacker.es. (8 de Enero de 2014). *Ingenieria social informática*. Recuperado el 16 de Marzo de 2016, de http://cursohacker.es/ingenieria-social-informatica

Damodaran. (Enero de 2016). *Betas por sector (US)*. Recuperado el 9 de Junio de 2016, de http://pages.stern.nyu.edu/~adamodar/New_Home_Page/datafile/Betas.html

Desarrollaweb.com. (2016). *Los Logs*. Recuperado el 1 de Mayo de 2016, de http://www.desarrolloweb.com/faq/408.php

Expreso.ec. (25 de Febrero de 2016). *Los menores ingresos presionaron un ajuste.* Recuperado el 27 de Mayo de 2016, de http://expreso.ec/economia/los-menores-ingresos-presionaron-un-ajuste-IE83708

Fernandez, P., Ortiz, A., & Acín, I. (2016). *Market Risk Premium used in 71 countries in 2016: a survey with 6,932 answers.* 9: Mayo. Recuperado el 9 de Junio de 2016

Gestiopolis. (22 de Marzo de 2011). *Técnica de ventas AIDA. Atención, interés, deseo y acción.* Recuperado el 26 de Abril de 2016, de http://www.gestiopolis.com/tecnica-de-ventas-aida-atencion-interes-deseo-accion/

Grupo Banco Mundial. (2016). *Doing Business*. Recuperado el 17 de Marzo de 2016, de Doing Business, facilidad para hacer negocios: http://espanol.doingbusiness.org/data/exploreeconomies/ecuador/

Info Spyware. (3 de Noviembre de 2008). *¿Què es el Pishing?* Recuperado el 10 de Abril de 2016, de https://www.infospyware.com/articulos/que-es-el-phishing/

Info Spyware. (19 de Marzo de 2009). *¿Què son los Malwares*. Recuperado el 10 de Abril de 2016, de https://www.infospyware.com/articulos/que-son-los-malwares/

Instituto Nacional de Estadística y Censos. (2010). *Resultados del censo 2010 de la población y vivienda en el Ecuador*. Recuperado el 17 de Marzo de 2016, de http://www.ecuadorencifras.gob.ec/wp-content/descargas/Manu-lateral/Resultados-provinciales/pichincha.pdf

IT Ahora la revista del lider de Tecnología. (2016). *Publicidad*. Recuperado el 26 de Abril de 2016, de http://www.itahora.com/documentos/PUBLICIDAD-ITahora-web.pdf

JC Magazine. (26 de Mayo de 2015). *Las personas no saben identificar los correos phishing*. Recuperado el Marzo de 15 de 2016, de http://www.jcmagazine.com/las-personas-no-saben-identificar-los-correos-phishing/

Lambin, J.-J. C. (2009). *Dirección de marketing gestión estratégica y operativa del mercado.* Mexico DF, Mexico: McGraw Hill.

M2 Commerce LATAM news. (30 de Julio de 2015). *Noticias de comercio, pagos y banca móvil*. Recuperado el 17 de Marzo de 2016, de Ecuador: más de 45 mil cuentas activas de dinero electrónico: http://noticias.mobilemoneylatam.com/2015/07/30/ecuador-mas-de-45-mil-cuentas-activas-de-dinero-electronico/

Mailify. (2016). *Emailing*. Recuperado el 25 de Abril de 2016, de https://es.mailify.com/tienda.asp

Master Magazine. (2016). *Definición de B2B*. Recuperado el 27 de Abril de 2016, de http://www.mastermagazine.info/termino/3984.php

Ministerio de Justicia, Derechos Humanos y Cultos. (2014). *Código Orgánico Integral Penal*. Recuperado el 17 de Marzo de 2016, de http://www.justicia.gob.ec/wp-content/uploads/2014/05/c%C3%B3digo_org%C3%A1nico_integral_penal_-_coip_ed._sdn-mjdhc.pdf

Porter, M. E. (2008). The Five Competitive Forces that Shape Strategy. *Harvard Business Review*. Recuperado el 17 de Marzo de 2016

Privacidad del internauta y delitos informáticos. (2016). *Ciberataques y Ciberamenazas*. Recuperado el 27 de Mayo de 2016, de http://www.gitsinformatica.com/ciberataques.html

Reglamento a la Ley de Comercio Electrónico, firmas electrónicas y mensajes de datos. (31 de Diciembre de 2002). *Reglamento a la Ley de Comercio Electrónico*. Recuperado el 17 de Marzo de 2016, de https://plataformamunicipal.ame.gob.ec/recursos/descarga/FacturacionElectronica/baseLegal/9.%20Reglamento%20a%20la%20Ley%20de%20Comercio%20Electr%C3%B3nico,%20Firmas%20Electr%C3%B3nicas%20y%20Mensajes%20de%20Datos.pdf

SBS. (04 de 2016). *Superintendencia de bancos*. Recuperado el 6 de 4 de 2016, de Superintendencia de bancos: www.sbs.gob.ec

SC. (9 de Junio de 2016). *Datos de la industria*. Recuperado el 9 de Junio de 2016, de http://181.198.3.71/portal/cgi-bin/cognos.cgi?b_action=cognosViewer&ui.action=run&ui.object=%2fcontent%2ffolder[%40name%3d%27Societario%27]%2ffolder[%40name%3d%27Reportes%27]%2freport[%40name%3d%27ind_finan_x_rama%27]&ui.name=ind_finan_x_rama&run.outputFo

Security Operation Center "Colombia". (2008). *Arquitectura de un SOC.* Recuperado el 10 de Mayo de 2016, de http://www.soccolombia.com/documentos/documento1.pdf

Security Standards Council. (2016). Recuperado el 8 de Abril de 2016, de Securing the future of payments together: https://www.pcisecuritystandards.org/pci_security/why_security_matters

Seguridad X. (18 de Enero de 2013). *Que es un SIEM.* Recuperado el 10 de Mayo de 2016, de http://www.seguridadx.com/que-es-un-siem-que-es-prelude-siem/

Seguridad, cultura de prevención para TI. (4 de Mayo de 2011). *Ingeniería Social: corrompiendo la mente humana*. Recuperado el 27 de Mayo de 2016, de http://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana

Superintendencia de Bancos. (2015). *Estudios y análisis técnicos.* Recuperado el 27 de Mayo de 2016, de Análisis financiero: Bancos privados.: http://www.superbancos.gob.ec/medios/PORTALDOCS/downloads/articulos_financieros/Estudios%20Tecnicos/2015/AT7_2015.pdf

Superintendencia de Bancos del Ecuador. (2016). *Superintendencia de Bancos del Ecuador*. Recuperado el 17 de Marzo de 2016, de http://www.superbancos.gob.ec/practg/p_index?

Superintendencia de Bancos y Seguros del Ecuador. (26 de Abril de 2012). *Resolución JB-2012-2148*. Obtenido de http://www.sbs.gob.ec/medios/PORTALDOCS/downloads/normativa/2012/resol_JB-2012-2148.pdf

SVT Cloud Security Services. (26 de Agosto de 2010). *Hacking ètico*. Recuperado el 10 de Abril de 2016, de Hablemos de Spoofing: http://hacking-etico.com/2010/08/26/hablemos-de-spoofing/

Wbusable. (s.f.). *El significado de los colores*. Recuperado el 21 de Abril de 2016, de http://www.webusable.com/coloursMean.htm

Wirtz, C. L. (2015). *Marketing de servicios: personal, tecnología y estrategia.* Mexico DF: Pearson.

Yahoo Finance. (2016). *Yahoo Fianance/bonds*. Recuperado el 9 de Junio de 2016, de http://finance.yahoo.com/bonds

ANEXOS

Anexo 1

Tabla 9 Clasificación Industrial Uniforme (CIIU)

Clasificación internacional industrial uniforme (CIIU 4.0)		
Actividad económica nivel 1	J	Información y comunicación
Actividad económica nivel 2	J62	Programación informática, consultoría de informática y actividades convexas
Actividad económica nivel 3	J620	Actividades de programación informática y de consultoría de informática y actividades convexas
Actividad económica nivel 4	J6201	Actividades de programación informática
Actividad económica nivel 5	J6201.0	Actividades de programación informática
Actividad económica nivel 6	J6201.02	Adaptación de programas informáticos a las necesidades de los clientes, es decir, modificación y configuración de una aplicación existente para que pueda funcionar adecuadamente con los sistemas de información de que dispone el cliente.

Adaptado de la Superintendencia de Compañías

Tabla 10 Matriz de Evaluación de Factores Externos

Matriz EFE				
Oportunidades		**Ponderación**	**Calificación**	**Peso ponderado**
1	Leyes y resoluciones que les exigen a las instituciones financieras adquirir sistemas de seguridad informáticos optimos y eficientes.	0,20	4	0,8
2	Tendencias tecnologicas en crecimiento, mayor uso de Smart phones para ingresar a bancos.	0,08	3	0,2
3	Auge de fraudes bancarios y ciberataques a nivel mundial	0,20	3	0,6
4	Las instituciones financieras desconocen o no han experimentado ataques informáticos considerables, pero conocen que son vulnerables ante ello.	0,10	4	0,4
5	Pocas empresas que brindan servicios de seguridad informática.	0,08	2	0,2
Amenazas		**Ponderación**	**Calificación**	**Peso ponderado**
1	Cambios estructurales dentro del gobierno que minimicen la adquisición de sistemas seguridad informáticos para controlar ciberataques.	0,07	4	0,3
2	Duración de la crisis nacional, menor captación de depósitos para las instituciones financieras.	0,03	3	0,1
3	Fortalecimiento de leyes tributarias y legales con respecto a la contratación de especialistas extranjeros en el tema de seguridad informática.	0,07	3	0,2
4	Competencia fuerte dentro de esta industria, debido a que tienen experiencia en el tema.	0,08	2	0,2
5	Licencias costosas para adquirir sistemas informáticos actualizados	0,10	1	0,1
Total		1,00		3,02

Tabla 11 Matriz de Análisis de la Industria

Matriz de Análisis de la Industria									
		Nada atractivo	Poco atractivo	Neutral	Atractivo	Muy atractivo		Calificación	Promedio de calificación
Barreras de Entrada									
Economias de escala	Poco						Mucho	1	
Diferenciación de producto	Poco						Alto	4	
Identificación de marcas	Bajo						Alto	3	*3,0*
Requerimiento de capital	Bajo						Alto	2	
Experiencia	Sin Importancia						Importante	5	
Barreras de Salida									
Especialización de activos	Alto						Bajo	2	
Costo de salida	Alto						Bajo	3	*2,3*
Estrategia interelacionadas	Alto						Bajo	2	
Rivalidad entre competidores									
Cantidad de competidores	Muchos						Pocos	3	
Crecimiento de la Industria	Lento						Rápido	2	
Costos fijos	Altos						Bajo	3	
Características del producto	Commodities						Especializados	5	*3,2*
Incrementos de Capacidad	Altos Incrementos						Bajos Incrementos	3	
Diversidad de Competidores	Alto						Bajo	3	
Capacidad de negociación Compradores									
Número de clientes	Pocos						Muchos	4	
Producto sustitutos	Varios						Pocos	4	*4,0*
Switching Cost	Bajo						Alto	3	
Influencia de la calidad	Bajo						Alto	5	
Capacidad de negociación proveedores									
Cantidad de proveedores	Pocos						Varios	1	
Productos sustitutos	Bajo						Alto	4	*2,8*
Switching Costs	Alto						Bajo	3	
Capacidad de convertirse en competenci	Alto						Bajo	3	
Total Análisis Industria									
Barreras de entrada	Bajo						Alto	3,0	
Barreras de salida	Alto						Bajo	2,3	
Rivalidad entre competidores	Alto						Bajo	3,2	
capacidad de negociación Compradores	Alto						Bajo	4,0	*3,2*
capacidad de negociación proveedores	Alto						Bajo	2,8	
Viabilidad de sustitutos	Algunos						Poco	4	

Anexo 2

Pishing

"El estafador, conocido como phisher, se vale de técnicas de ingeniería social, haciéndose pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo general un correo electrónico, o algún sistema de mensajería instantánea, redes sociales SMS/MMS, a raíz de un malware o incluso utilizando también llamadas telefónicas" (Info Spyware, 2008).

Skimming

"El Skimmer es un aparato que utiliza la tecnología usada por los cajeros automáticos para leer la banda magnética de las tarjetas. Se realiza la lectura pasándola por una pequeña ranura y los datos quedan almacenados para transferirlos posteriormente a un ordenador" (BBVA, 2015).

Spoffing

"uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación. Un atacante falsea el origen de los paquetes haciendo que la víctima piense que estos son de un host de confianza o autorizado para evitar la víctima lo detecte" (SVT Cloud Security Services, 2010).

Datos de los cuatro entrevistados

Tabla 12: Patricio Vivero

Primer entrevistado	
NOMBRE	Patricio Vivero
OCUPACION	Gerente de riesgo en Diners Club Ecuador, Coordinador de la carrerra de Economía en la Universidad de las Américas.
PERFIL PROFESIONAL	Gestion en riesgo organizacional, Master en finanzas en la Universidad de Illinois
ENTIDAD	Universidad de las Américas

Tabla 13: Ramiro Pulgar M.

Segundo entrevistado	
NOMBRE	Ramiro Pulgar M.
OCUPACION	Gerente general de Blue Hat Consultores Cia.Ltda.
PERFIL PROFESIONAL	Experto en seguridad informatica, posee certificados en seguridad informatica reconocidos internacionalmente. EC-Council - Circle of Excellence Instructor 2014 http://www.eccouncil.org/Support/pressroom/ec-council-events/ec-council-global-awards - Circle of Excellence Instructor 2013 http://www.eccouncil.org/Support/pressroom/ec-council-events/ec-council-global-awards
ENTIDAD	Blue hat Consultores Cia.Ltda.

Tabla 14: tercer entrevistado (carta de confidencialidad)

Tercer entrevistado	
NOMBRE	Confidencial
OCUPACION	Confidencial
PERFIL PROFESIONAL	Confidencial
ENTIDAD	Entidad Reguladora
Se anexa la carta del acuerdo de confidencailidad por las partes, en la cual consta la participacion y colaboracion del entrevistado.	

Tabla 15: Pablo Sosa.

Cuarto entrevistado	
NOMBRE	Pablo Sosa
OCUPACION	Commercial Director SAPHIRTEK, Information Security and Commercial manager helping companies to improve security.
PERFIL PROFESIONAL	Experto en tecnologias de información, seguirdad informática y en sistemas de seguridad para instituciones financieras y empresas en general.
ENTIDAD	Saphirtek

Cadena de valor

Cadena de valor de "Owl SOC"				
Infraestructura de la empresa (aportes de capital de los inversionistas; Gobierno corporativo con lineamientos operacionales y administrativos; Transparencia en el manejo de información con los inversores y clientes)				
Gestión de Recursos Humanos (Reclutamiento de personal con amplio conocimiento en seguridad de la información; capacitaciones periódicas; plan de selección y promoción del personal)				
Desarrollo de Tecnología (Inversión en investigación y desarrollo de nuevos sistemas de seguridad informática; alianzas estratégicas con empresas relacionadas con el giro de negocio; análisis periódico de las necesidades del cliente y de nuevas amenazas informáticas)				
Compras (políticas alineadas al manejo adecuado de los sistemas de seguridad adquiridos para el servicio; relación estratégica con los proveedores del servicio)				
Logística interna	**Operaciones**	**Logística externa**	**Marketing y ventas**	**Servicio post venta**
Recepción de pedidos de compra e información sobre el servicio por parte del cliente. Gestionar y facilitar información técnica de las ventajas y desventajas del mismo.	Montaje del centro de operaciones de seguridad (SOC) en las instalaciones del cliente. Pruebas y mantenimiento de los mismos para monitorear y controlar los servidores integrados al sistema de seguridad.	Gestión de los pedidos de adquisición del servicio para el montaje del mismo.	Estrategias de promoción del servicio mediante los canales de: pagina web, revistas y mailing (o correo personalizado)	Soporte continuo al cliente para la resolución oportuna de incidentes informáticos en tiempo real. Recomendaciones y quejas por parte del cliente.

Actividades de Soporte

MARGEN

MARGEN

Actividades Primarias

Certificado de Confidencialidad

Quito, 2 de Abril de 2016

SEÑORES
UNIVERSIDAD DE LAS AMÉRICAS

CERTIFICACIÓN Y ACUERDO DE CONFIDENCIALIDAD

Yo, Marcia Myreya Topón Figueroa, portadora de la cédula de identidad número 1711906790, certifico que he accedido a la entrevista propuesta por el señor Renato Pulgar, estudiante de la FACEA de la Universidad de las Américas; la información es proporcionada exclusivamente para fines académicos, por lo que se solicita se mantenga la confidencialidad de mi identidad así como de la institución en la que trabajo y al mismo tiempo aclaro que los criterios vertidos en la entrevista no constituyen el criterio del organismo de control.

El señor Pulgar por medio del presente se compromete a guardar la confidencialidad de la identidad de la persona entrevistada así como de su lugar de trabajo.

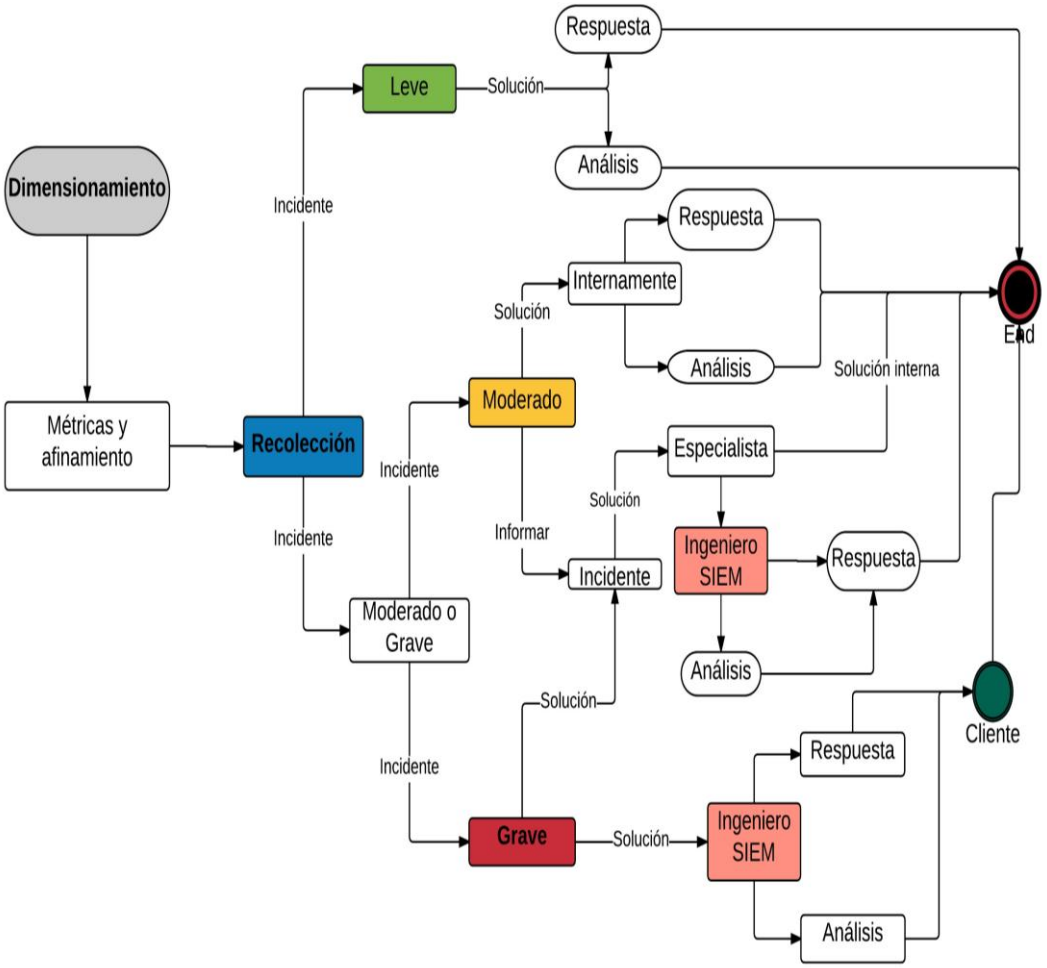
Con un cordial saludo,

Ing. Marcia Topón Figueroa
Directora Nacional de Riesgos (e)
Superintendencia de Bancos
CI: 1711906790
Cel: 0982446175

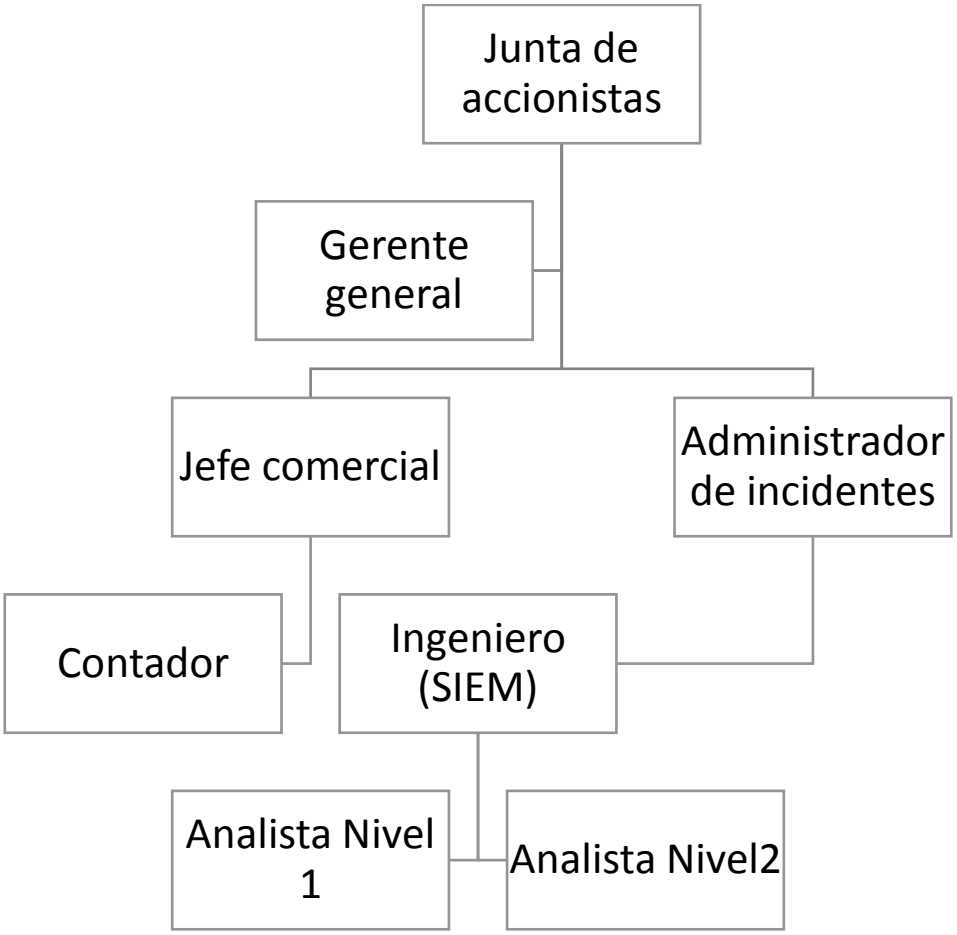
Sr. Renato Pulgar
Estudiante de la FACEA
Universidad de las Américas
CI: 1716070808

Anexo 3

Flujo grama de Owl SOC



Estructura Organizacional



Anexo 4

Tabla 16: Modelación de incidente informático

Modelación de incidente		
	10 millones	Eventos totales recibidos en un dia
	1 millon	Eventos analizados
	50000	Total eventos correlacionados de interes
	1000	Eventos correlacionados de amplio interes
	10	Casos abiertos
	5	Casos criticos

En esta tabla 16, los incidentes son filtrados de acuerdo al nivel de importancia, el cual puede clasificarse como incidentes leves, moderados y graves. Estos últimos, son considerados casos críticos, los cuales son de suma importancia solucionarlos ya sea a nivel interno con los expertos o informar al cliente para tomar decisiones en conjunto.

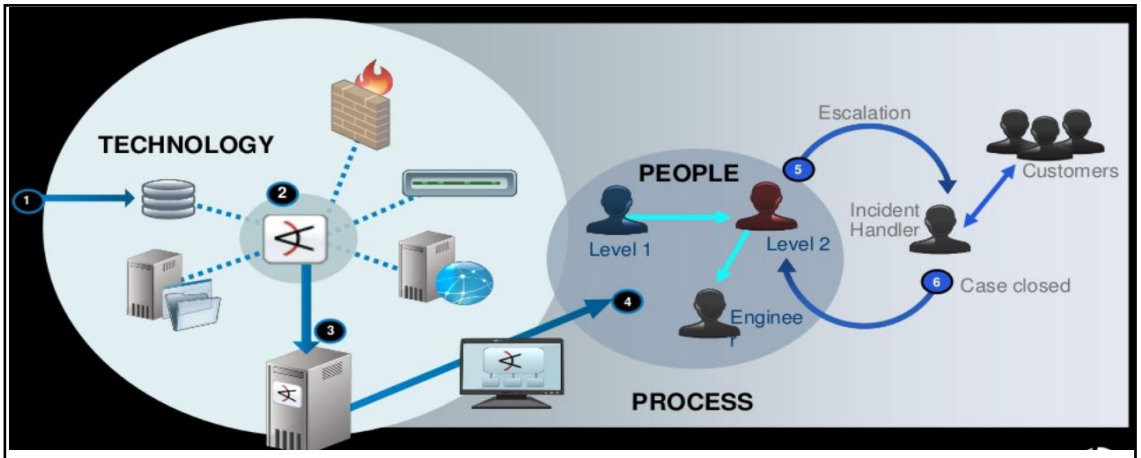


Figura 3: Funcionamiento de un SOC, Batrankov, D. (3 de octubre de 2016). Building Security Operation Center.

Anexo 5: Estado de Resultados

Estado de resultados	Inicial	2016	2017	2018	2019	2020	2021
Ingresos	-	252.000,00	770.000,00	1.666.000,00	2.254.000,00	2.590.000,00	2.828.000,00
Descuentos	-	4.200,00	32.200,00	43.400,00	37.800,00	43.400,00	23.800,00
Ingresos netos	-	247.800,00	737.800,00	1.622.600,00	2.216.200,00	2.546.600,00	2.804.200,00
Gastos relacionados con el cliente	-	388.229,40	431.470,66	903.902,35	950.815,94	1.004.774,60	1.067.123,87
Help desk L-V Nivel 1 y Nivel 2	-	190.666,80	212.085,60	444.305,24	467.365,20	493.888,10	524.536,10
Help desk S-D Nivel 1 y Nivel2	-	81.871,20	91.057,50	190.759,40	200.660,04	212.047,46	225.205,33
Especialista incidentes (12 h L-V)	-	77.930,40	86.319,82	180.834,29	190.219,81	201.014,75	213.488,02
Ingeniero SIEM L-V 8h	-	37.761,00	42.007,74	88.003,41	92.570,89	97.824,28	103.894,42
Suministros de oficina relacionado con el giro de negocio	-	4.496,40	-	1.237,08	-	-	-
Utilidad Bruta	-	-144.925,80	306.329,34	717.460,58	1.265.384,06	1.541.825,40	1.737.076,13
Gastos de constitución	-	1.818,00	-	-	-	-	-
Gastos pre operacionales	-	48.560,00	-	-	-	-	-
Gastos sueldos administrativos	-	57.964,00	64.652,26	67.721,10	71.235,90	75.278,53	79.949,67
Gastos	-	129.992,59	135.635,73	211.837,22	222.831,82	235.477,50	250.089,23
Honorarios profesionales outsourcing	-	6.600,00	6.886,51	7.213,39	7.587,78	8.018,38	8.515,94
Servicios basicos	-	4.680,00	4.883,16	5.114,95	5.380,42	5.685,76	6.038,57
Arriendo	-	18.240,00	19.031,82	19.935,20	20.969,86	22.159,90	23.534,95
Mantenimiento y reparaciones	-	2.040,00	2.128,56	2.229,59	2.345,31	2.478,41	2.632,20
Suministros, materiales y repuestos	-	840,00	876,47	918,07	965,72	1.020,52	1.083,85
Seguros	-	2.400,00	2.504,19	2.623,05	2.759,19	2.915,78	3.096,70
Capacitacion personal	-	92.000,00	95.993,83	170.313,66	179.153,13	189.320,05	201.067,64
Publicidad	-	3.192,59	3.331,18	3.489,30	3.670,40	3.878,70	4.119,38
Depreciación	-	7.686,67	7.686,67	14.947,42	31.870,40	31.870,40	33.120,31
Amortización	-	151.500,00	151.500,00	151.500,00	151.500,00	151.500,00	151.500,00
Provisión cuentas por cobrar	-	991,20	2.951,20	6.490,40	8.864,80	10.186,40	11.216,80
Utilidad antes de intereses e impuestos	-	-673.430,85	-191.732,24	53.127,21	556.249,32	802.035,09	961.110,89
Intereses	-	6.142,65	5.039,90	3.808,43	2.433,23	897,53	-
Utilidad antes de participación de trabajadores	-	-679.573,50	-196.772,14	49.318,78	553.816,08	801.137,55	961.110,89
15% participación trabajadores	-	-101.936,03	-29.515,82	7.397,82	83.072,41	120.170,63	144.166,63
Utilidad antes de impuestos	-	-577.637,48	-167.256,32	41.920,96	470.743,67	680.966,92	816.944,26
22% Impuesto a la renta	-	-127.080,24	-36.796,39	9.222,61	103.563,61	149.812,72	179.727,74
Utilidad Neta	-	$ -450.557,23	$ -130.459,93	$ 32.698,35	$ 367.180,06	$ 531.154,20	$ 637.216,52

Supuestos de los estados financieros

Estado de resultados

- Los descuentos se implementan a la entrada de cada cliente el primer mes de la contratación del servicio.
- Los gastos relacionados con el cliente, es el personal que interactúa directamente con el mismo. Esto se aplicó debido a que el proyecto no tiene costo de ventas, pero si tiene personal que posee altos costos como: capacitación y salarios mensuales de niveles considerables. El personal corresponde a los analistas de nivel uno y dos de todas las jornadas, también los especialistas y los ingenieros SIEM, con esto se pretende transferir el peso de los gastos generados por estas personas hacia el costo que asume el cliente.
- Los suministros relacionados con el giro de negocio corresponden a equipos como: monitores, cpu´s, mouse, teclados, Reuters, cables de red, cámaras de seguridad, acceso biométrico, extintores y otros artículos de pequeñas proporciones.
- El gasto pre operacional según las nuevas normas este gasto se lo incluye en el primer mes del primer año del plan de negocio.
- El 15% de3 participación de los trabajadores y el 22% del impuesto a la renta no aplica en el caso que la suma del año de ganancias negativas. En el modelo financiero se aplicó una restricción en la formula, la cual tiene como objetivo descartar este supuesto. No se considera como crédito tributario, sino como perdidas del ejercicio
- Se espera un aumento de personal en año 2018 por lo cual existe una inversión importante en personal y equipos de cómputo para ese año, debido al crecimiento de clientes que se proyecta obtener

Estado de Situación

- Para la depreciación se tomó en cuenta el límite de los años depreciables, los cuales corresponden a: equipos de oficina y cómputo 3 años, muebles y enseres 10 años. Además, las licencias son amortizables anualmente, debido a que la adquisición y vencimiento de las mismas son de un año.
- No se considera tener pasivos corrientes debido a que no se manejan cuentas por pagar.
- Las ventas a contado o cuentas por cobrar son de 30 días, con un supuesto de 60% ventas al contado y 40% a crédito, esto para dar flexibilidad al cliente para la adquisición del servicio.
- El capital social son rondas de capital con lapsos anuales, para que la razón deuda capital sea 67% capital 33% deuda.

Flujo de caja libre o FCF

- Se usa el método de Damodaran para apalancar la beta.
- La tasa libre de riesgo se obtuvo de los bonos americanos a 30 años de los Estados Unidos.

Indicadores financieros

- Los datos de la industria se tomaron de la superintendencia de compañías, estos corresponden a la Rama J in formación y comunicación, año 2014 según las NIIF (Datos de la industria, 2016).

Datos de la valoración: Valor presente, VP; Inversión inicial; Valor Presente Neto, VPN; Tasa Interna de retorno, TIR; Índice de rentabilidad, IR y Periodo de recuperación.

Valoración	$ 3.355.902,80
Inversión inicial	($ 178.900,00)
VPN	$ 3.177.002,80
TIR	68%
Índice de rentabilidad	18,76

Periodo de recuperación		**5**
Inicial	**Entrante**	**Final**
-178.900,00	-298.385,98	-477.285,98
-477.285,98	-148.260,61	-625.546,60
-625.546,60	-594,38	-626.140,97
-626.140,97	317.606,77	-308.534,21
-308.534,21	552.531,66	243.997,45
243.997,45	7.270.236,53	7.514.233,98

Anexo 6: Estado de situación

Estado de situación	Inicial	2016	2017	2018	2019	2020	2021
Activos							
Activos corrientes	-	152.164,80	232.528,21	291.903,87	605.827,62	1.154.158,73	1.799.979,99
Efectivo	-	141.076,80	192.611,41	225.375,87	528.211,62	1.065.454,73	1.705.731,99
Cuentas por cobrar	-	11.200,00	40.320,00	67.200,00	78.400,00	89.600,00	95.200,00
Provisión cuentas por cobrar	-	112,00	403,20	672,00	784,00	896,00	952,00
Neto cuentas por cobrar	-	11.088,00	39.916,80	66.528,00	77.616,00	88.704,00	94.248,00
Activos No corrientes	178.900,00	19.713,33	12.026,67	21.233,19	61.331,72	29.461,32	20.856,58
Equipos	21.200,00	14.133,33	7.066,67	13.843,89	54.901,23	23.989,64	16.343,72
Computador pc desktop	11.000,00	11.000,00	11.000,00	17.011,16	29.657,46	29.657,46	36.754,07
Depreciación acumulada	-	3.666,67	7.333,33	13.003,72	19.222,87	25.442,03	32.023,00
Neto	11.000,00	7.333,33	3.666,67	4.007,44	10.434,59	4.215,43	4.731,08
Monitores	3.000,00	3.000,00	3.000,00	4.639,41	39.129,31	39.129,31	41.064,75
Depreciación acumulada	-	1.000,00	2.000,00	3.546,47	15.589,57	27.632,68	39.774,46
Neto	3.000,00	2.000,00	1.000,00	1.092,94	23.539,74	11.496,63	1.290,29
Televisor	4.500,00	4.500,00	4.500,00	12.697,04	28.217,49	28.217,49	37.894,70
Depreciación acumulada	-	1.500,00	3.000,00	7.232,35	15.138,18	23.044,01	31.443,23
Neto	4.500,00	3.000,00	1.500,00	5.464,69	13.079,32	5.173,49	6.451,47
Impresora	2.700,00	2.700,00	2.700,00	7.618,22	16.930,50	16.930,50	22.736,82
Depreciación acumulada	-	900,00	1.800,00	4.339,41	9.082,91	13.826,41	18.865,94
Neto	2.700,00	1.800,00	900,00	3.278,82	7.847,59	3.104,09	3.870,88
Muebles y enseres	6.200,00	5.580,00	4.960,00	7.389,30	6.430,49	5.471,68	4.512,87
Mesas	5.000,00	5.000,00	5.000,00	7.732,35	7.732,35	7.732,35	7.732,35
Depreciación acumulada	-	500,00	1.000,00	1.773,23	2.546,47	3.319,70	4.092,94
Neto	5.000,00	4.500,00	4.000,00	5.959,11	5.185,88	4.412,64	3.639,41
Sillas	1.200,00	1.200,00	1.200,00	1.855,76	1.855,76	1.855,76	1.855,76
Depreciación acumulada	-	120,00	240,00	425,58	611,15	796,73	982,31
Neto	1.200,00	1.080,00	960,00	1.430,19	1.244,61	1.059,03	873,46
Intangibles	151.500,00	-	-	-	-	-	-
Licenciamiento de SW Open Source (DETECTOR DE INCIDENTES Y	150.000,00	150.000,00	300.000,00	450.000,00	600.000,00	750.000,00	900.000,00
Amortización acumulada	-	150.000,00	300.000,00	450.000,00	600.000,00	750.000,00	900.000,00
Neto	150.000,00	-	-	-	-	-	-
Amazon Web Services AWS (servidores en la nube)	1.500,00	1.500,00	3.000,00	4.500,00	6.000,00	7.500,00	9.000,00
Amortización acumulada	-	1.500,00	3.000,00	4.500,00	6.000,00	7.500,00	9.000,00
Neto	1.500,00	-	-	-	-	-	-
-	-	-	-	-	-	-	-
Total Activos	178.900,00	171.878,14	244.554,88	313.137,05	667.159,34	1.183.620,05	1.820.836,57
Pasivos	-	-	-	-	-	-	-
Corrientes	-	-	-	-	-	-	-
No corriente	59.633,33	50.184,97	39.633,85	27.851,27	14.693,48	-0,00	-
Deuda a largo plazo	59.633,33	50.184,97	39.633,85	27.851,27	14.693,48	-0,00	-
Total Pasivo	59.633,33	50.184,97	39.633,85	27.851,27	14.693,48	-0,00	-
Patrimonio	119.266,67	121.693,17	204.921,03	285.285,79	652.465,85	1.183.620,05	1.820.836,57
Capital social	119.266,67	801.266,67	1.081.266,67	1.152.866,67	1.152.866,67	1.152.866,67	1.152.866,67
Utilidad Neta	-	-679.573,50	-876.345,64	-867.580,88	-500.400,81	30.753,38	667.969,91
Total Pasivo mas Patrimonio	$ 178.900,00	$ 171.878,14	$ 244.554,88	$ 313.137,05	$ 667.159,34	$ 1.183.620,05	$ 1.820.836,57

Anexo 7: Estado de flujo de efectivo

Estado de flujo de efectivo	Inicial	2016	2017	2018	2019	2020	2021
Actividades de operación	-	-531.474,83	-66.414,27	148.600,98	539.462,46	703.436,59	816.292,83
Utilidad Neta	-	-679.573,50	-196.772,14	8.764,76	367.180,06	531.154,20	637.216,52
Depreciación	-	7.686,67	7.686,67	14.947,42	31.870,40	31.870,40	33.120,31
Amortización	-	151.500,00	151.500,00	151.500,00	151.500,00	151.500,00	151.500,00
Incremento de cuentas por cobrar	-	-11.088,00	-28.828,80	-26.611,20	-11.088,00	-11.088,00	-5.544,00
Incremento de cuentas por pagar	-	-	-	-	-	-	-
	-	-	-	-	-	-	-
Actividad Inversión	-178.900,00	-	-151.500,00	-175.653,94	-223.468,93	-151.500,00	-176.015,57
Capex	-178.900,00	-	-151.500,00	-175.653,94	-223.468,93	-151.500,00	-176.015,57
	-	-	-	-	-	-	-
Actividad Financiamiento	178.900,00	672.551,64	269.448,88	59.817,41	-13.157,78	-14.693,48	0,00
	-	-	-	-	-	-	-
Deuda a Largo Plazo	59.633,33	-9.448,36	-10.551,12	-11.782,59	-13.157,78	-14.693,48	0,00
Aportes de Capital	119.266,67	682.000,00	280.000,00	71.600,00	-	-	-
	-	-	-	-	-	-	-
Flujo de efectivo inicial	-	-	141.076,80	192.611,41	225.375,87	528.211,62	1.065.454,73
Efectivo resultante	-	141.076,80	51.534,61	32.764,46	302.835,75	537.243,11	640.277,26
Flujo de efectivo final	$ -	$ 141.076,80	$ 192.611,41	$ 225.375,87	$ 528.211,62	$ 1.065.454,73	$ 1.705.731,99

Valoración: método Flujo de caja libre o FCF

Flujo libre de Caja							
	inicial	**2016**	**2017**	**2018**	**2019**	**2020**	**2021**
NOPAT		($ 446.484,65)	($ 127.118,48)	$ 35.223,34	$ 368.793,30	$ 531.749,26	$ 637.216,52
Depreciación		$ 7.686,67	$ 7.686,67	$ 14.947,42	$ 31.870,40	$ 31.870,40	$ 33.120,31
Amortización		$ 151.500,00	$ 151.500,00	$ 151.500,00	$ 151.500,00	$ 151.500,00	$ 151.500,00
FEO		($ 287.297,98)	$ 32.068,19	$ 201.670,76	$ 552.163,70	$ 715.119,66	$ 821.836,83
Capital de Trabajo		($ 11.088,00)	($ 28.828,80)	($ 26.611,20)	($ 11.088,00)	($ 11.088,00)	($ 5.544,00)
Gastos de Capital	($ 178.900,00)	$ 0,00	($ 151.500,00)	($ 175.653,94)	($ 223.468,93)	($ 151.500,00)	($ 176.015,57)
FCF	($ 178.900,00)	($ 298.385,98)	($ 148.260,61)	($ 594,38)	$ 317.606,77	$ 552.531,66	$ 640.277,26
T	33,7%	33,7%	33,7%	33,7%	33,7%	33,7%	33,7%
g	4,23%	4,23%	4,23%	4,23%	4,23%	4,23%	4,23%
Bu	0,94	0,94	0,94	0,94	0,94	0,94	0,94
rf bonos a 30 años USA	2,45%	2,45%	2,45%	2,45%	2,45%	2,45%	2,45%
Prima de mercado	12,60%	12,60%	12,60%	12,60%	12,60%	12,60%	12,60%
Bl	0,95	0,95	0,95	0,94	0,94	0,94	0,94
Ke	14,44%	14,39%	14,36%	14,33%	14,31%	14,29%	14,29%
Kd	10,30%	10,04%	9,61%	8,74%	6,11%	0,00%	0,00%
D/E	1,81%	1,23%	0,82%	0,50%	0,24%	0,00%	0,00%
WACC	14,30%	14,30%	14,29%	14,29%	14,29%	14,294%	14,29%
E+D	**$ 3.355.902,80**	**$ 4.134.212,88**	**$ 4.873.526,70**	**$ 5.570.714,99**	**$ 6.049.205,43**	**$ 6.360.995,79**	**$ 6.629.959,27**