DISEÑO DEL BUSINESS MODEL CANVAS PARA LA NUEVA LÍNEA DE NEGOCIO "U.E.S – UNIDAD ESTRATÉGICA DE SEGURIDAD" DE PCM S.A.S

Camilo Santamaria Martinez

Uniempresarial – Cámara de Comercio de Bogotá

Facultad de Postgrados

Especialización en Alta Gerencia

Bogotá, 2019

TABLA DE CONTENIDO

1. Formulación del Problema

Actualmente la compañía PCM S.A.S es una compañía dedicada a la prestación de servicios y soluciones de TI para organizaciones del sector público y del sector privado. Este año cumplió ya 36 años en el mercado consolidándose como una empresa de trayectoria y que va evolucionando a medida que las necesidades del mercado van cambiando. La compañía inicio sus actividades con la prestación de servicios de mantenimiento preventivo y correctivo para servidores, computadores, impresoras, escáner y demás componentes electrónicos como Discos duros, unidades de diskettes, memorias, boards, etc. Para los próximos años la empresa siguió con la prestación de este tipo de servicios e incursiono en la venta de equipos de cómputo ensamblados por la misma compañía. A estos equipos se les llamaban “CLONES” ya que no eran equipos de marca como lo eran “Compaq” y “Acer" entre otros los cuales tenían un precio muy superior al de los clones, permitiendo márgenes bastante buenos de hasta el 40%. Hoy en día por la amplia diversidad de productos y fabricantes estos márgenes son entre el 8% y 15% según el jefe de compras de la compañía Iván Cepeda. Hacia el año 2002 la empresa decide incursionar en servicios de seguridad informática desarrollando una importante alianza con uno de los fabricantes líderes en el mundo que es McAfee. Esta alianza comenzó con la comercialización e implementación de soluciones de antivirus para las estaciones de trabajo, soluciones de Firewall, soluciones de protección de la web y el correo electrónico. Esta alianza permitió a PCM ser uno de los partners más representativos en Colombia. Desde esa fecha hasta el año 2015 la compañía no distribuía ni comercializaba ninguna solución de seguridad diferente a las de este fabricante.

Debido al crecimiento exponencial de amenazas informáticas avanzadas, PCM decide ampliar su portafolio de soluciones con otros fabricantes de seguridad como lo son Sophos, Cisco, Forcepoint, Kod Latam Security entre otros. Estas amenazas informáticas, afectan tanto a personas como a compañías en cuento a pérdida y/o robo de información, lo cual representan millones de dólares en pérdidas para las empresas.

Según un informe realizado por (SYMANTEC, 2017), uno de los fabricantes líderes de seguridad, nos muestra que “las amenazas a la seguridad digital pueden provenir de fuentes nuevas e inesperadas. Con cada año que pasa, no solo se ha incrementado el volumen de amenazas, sino que el panorama de amenazas se ha vuelto más diverso, con los

atacantes trabajando más arduamente para descubrir nuevas vías de ataque y cubrir sus huellas al hacerlo.” Este informe muestra cifras como las siguientes:

- Aumento del 92% en nuevas variantes de descarga.
- El 55% de los correos son Spam, 2% más que en 2016.
- 600% de aumento en los ataques contra dispositivos de IoT (Internet de las cosas).

Estas son solo algunas de muchas de las cifras que hoy tienen con preocupación tanto a fabricantes como a compañías. Ante este panorama de amenazas, las compañías pueden encontrar en el mercado una amplia variedad de soluciones de TI para administrar, gestionar y asegurar sus infraestructuras de TI. En este mismo sentido hay muchos canales y/o empresas que comercializan las soluciones que venden estos fabricantes ya que, en un amplio porcentaje, los fabricantes nunca llegan directo a cliente o usuario final, tienen un ecosistema de "partners” para la distribución de sus productos y soluciones. Hoy en día muchas compañías cuentan con infraestructuras de TI muy robustas, ya consolidadas y con un mix de soluciones de varios fabricantes, las cuales cumplen con una necesidad específica y que según esa especificidad existen empresas como Gartner y NSSLAB, que hacen estudios año a año con los clientes, evaluando y calificando bajo determinados criterios, los diferentes tipos de soluciones existentes en el mercado. Muchas de estas compañías toman estas evaluaciones como uno de los factores determinantes para escoger una determinada solución. Esta es una tendencia que las compañías desarrollan y que vienen trabajando muchos años de la mano con ciertos fabricantes y/o canales, consolidando así una base de proveedores en sus infraestructuras tecnológicas, y además de esto les resulta complejo realizar un cambio de solución, ya que dicho cambio puede generar un alto impacto en la organización.

Dada esta situación los clientes generan muchas barreras a nuevos proveedores que vienen con soluciones similares sin poder llegar a que conozcan los beneficios que estas pueden llegar a ofrecer igual o mejor, haciendo del mercado bastante cerrado y competido. Ante esta alta competencia del mercado y el amplio número de empresas (locales y extranjeros), PCM encuentra una fuerte barrera para entrar a estos mercados donde la

competencia ya tiene una amplia porción del mercado con las soluciones de seguridad que actualmente cuenta en su portafolio.

PCM es un canal que comercializa desde hace varios años, diferentes soluciones de seguridad y cuenta con importantes alianzas con diferentes fabricantes de seguridad como lo son McAfee, Sophos, Cisco Forcepoint. Kod entre otros y compite fuertemente con bastantes canales que también comercializan las soluciones de estos fabricantes y de otros como Kaspersky, Symantec, Eset, Cylance entre otros. De acuerdo con la experiencia y el conocimiento con el que cuenta el área de ingeniería de PCM se evidencia que una compañía que cuenta con las mejores soluciones y que estén bien administradas, actualizadas y parametrizadas no garantizan que su infraestructura de TI 100% segura. Según un informe del centro cibernético policial (Policial, 2017) en Colombia las amenazas están pasando del ciudadano común a las grandes empresas del sector público-privado. Las amenazas al ciudadano común pasaron de un 92% en 2014 a un 57% en 2016, mientras que los incidentes reportados en el sector empresarial aumentaron de un 5% a un 28% en los mismos años.

Ante esta perspectiva el mercado está demandando cada vez más mejores servicios y soluciones que respalden y aseguren la operación del negocio la cual se apalanca en la tecnología en un gran porcentaje. Y en la misma medida que el mercado va evolucionando es necesario para PCM dar un salto en su modelo de negocios dejando de ofrecer las soluciones tradicionales a servicios de ciberseguridad que permitirán a los clientes estar mejor preparados ante esas nuevas amenazas. Para esto la compañía decide crear la “UES – Unidad Estrategica de Seguridad”. Dada esta premisa se revisa la literatura para la generación de modelos de negocio la cual nos lleva a centrarnos en el Business Model Canvas. Se propone el enfoque de esta nueva línea de negocio en el Bussines Model Canvas ya que es una forma práctica y simple de describir un modelo de negocio y que a su vez ayudara a interiorizar el nuevo modelo de negocio en la organización. Para ver el gran potencial que tiene la organización al implementar este nuevo modelo de negocios veremos algunas cifras que pueden ilustrar mejor dicho potencial:

Según el MinTic en alianza con la Federación Colombiana de la Industria de Software y Tecnologías Informáticas (Fedesoft) en 2017 indicaron que las ventas del sector de TI pasaron de facturar de $9,6 billones en 2015 a $13,5 billones en 2016, lo que

representa un crecimiento de 40,7% y para este 2018 se espera llegar a 17,7 billones. Adicional Estas cifras encontramos que las entidades gubernamentales están comprometidas con la ciberseguridad de las personas y las empresas a través de decretos y regulaciones que a obliga a las empresas a cumplir e implementar procesos que garanticen la confidencialidad y seguridad de los datos en el ciberespacio. Teniendo esto en cuenta PCM debe explorar otras perspectivas, dejando un poco el foco de venta del esquema tradicional de trabajar con fabricantes y soluciones, a uno mucho más consultivo y estratégico, con un personal altamente especializado y certificado, aplicando diferentes metodologías que ayudan a prevenir y detener a los atacantes y amenazas que día a día van evolucionando y son más inteligentes vulnerando cualquier solución existente.

Estos factores mencionados anteriormente nos muestran el gran potencial de mercado que tiene PCM el cual se debe abordar de una manera estratégica e innovadora y de fácil comprensión al interior de la organización determinando: ¿Que vender? ¿A quiénes le voy a vender? ¿A través de que canales les voy a comunicar? ¿Cuáles son los recursos y actividades clave? ¿Qué asociaciones debe desarrollar? ¿Cómo se va a dar esa relación con los clientes? Y ¿Cómo va hacer mi estructura de costos e ingresos? Todos estos interrogantes nos llevan a formular la siguiente pregunta de investigación: **¿Cómo sería el diseño del Business Model Canvas para la nueva línea de negocio "UES – Unidad Estratégica de Seguridad"?**

2. Justificación

Ante el panorama de amenazas avanzadas y el gran potencial del mercado que se planteó anteriormente PCM ha decidido desarrollar una línea de servicios la cual denomino "Unidad Estratégica de Seguridad – UES". El desarrollo de esta nueva línea de servicios supone un gran reto para la empresa ya que se requiere un profundo conocimiento tanto de los servicios a prestar en esta nueva línea de negocios, como del mercado al cual se van a ofertar dichos servicios. Históricamente la participación de las ventas actuales de PCM están en mayor proporción en el sector estatal que en el sector público que en el sector privado o corporativo y hoy en día es un objetivo de la empresa dar vuelta a esta balanza, donde el sector corporativo sea la principal fuente de ingresos y no el sector estatal donde los procesos de licitación son cada vez menos regulados, procesos licitatorios que ya están sesgados a un proponente especifico. Subastas donde otras empresas sacrifican

significativamente su utilidad, con tal de ganarse el cliente y muchos otros factores que hacen que se deba dar un giro en la estrategia de negocio de la empresa.

Este giro estratégico supone para la empresa un entendimiento de las necesidades cambiantes del mercado corporativo y como se les entrega valor. Es claro que desde la etapa de entender las necesidades del mercado hasta la generación de valor son muchas las fases y procesos que la empresa debe desarrollar y articular para que eso de materialice. Si bien es cierto que la compañía ya ha trabajado con clientes de este sector, esto no se ha dado por la implementación de una estrategia clara de la compañía. Para la implementación de esta estrategia, supone un reto importante para PCM desarrollar con éxito esta nueva línea de negocio la cual debe ir acompañada de innovación, pero que pueda ser aplicada de una manera práctica y simple en todas las áreas de la organización.

Con base en esto, se plantea desarrollar un plan estratégico para la "UES" basado en la implementación del Business Model Canvas o generación de modelos de negocio El modelo Canvas fue escrito y diseñado por Alex Osterwalder y Yves Pigneur en 2010, el cual fue creado para describir de la mejor manera un modelo de negocio, dividido en nueve módulos básicos que reflejen la lógica que sigue la empresa para conseguir nuevos ingresos. Estos nueve módulos cubren las cuatro áreas principales de un negocio: clientes, oferta, infraestructura y viabilidad económica (Osterwalder, Pigneur, 2010).

Los nueve módulos del modelo Canvas son los siguientes:

1. Segmentos de mercado
2. Propuesta de Valor
3. Canales
4. Relaciones con los clientes
5. Fuentes de Ingresos
6. Recursos clave
7. Actividades clave
8. Asociaciones clave
9. Estructura de costes

La escogencia de este modelo para el desarrollo de este plan estratégico se da principalmente por su simplicidad y fácil aplicabilidad con el fin de que todos los colaboradores al interior de la organización lo comprendan fácilmente y se pueda aplicar rápidamente. También se consideró pertinente dado que este concepto se ha aplicado y probado a nivel internacional y principalmente con empresas de tecnológica como Amazon, IBM, Ericcson y Deloitte, compañías que ya lo están utilizando. A lo largo de este trabajo analizaremos que factores claves llevaron a una de exitosa implementación de estos modelos de negocio y que serán un insumo fundamental para el diseño de modelo de negocio de la U.E.S en PCM.

La pertinencia del desarrollo de este trabajo de grado permitirá determinar la viabilidad y aplicabilidad de la creación de la nueva línea de negocio y será la hoja de ruta para su posterior implementación en caso de que así lo considere la empresa. Así mismo poder comprobar la teoría del modelo con la aplicación en un escenario real

3. Objetivos

3.1 Objetivo General

Diseñar el Business Model Canvas para la nueva línea de negocio “UES - Unidad Estratégica de Seguridad” de PCM S.A.S.

3.2 Objetivos Específicos

- Diseñar los componentes de clientes del Business Model Canvas teniendo en cuenta los módulos de segmentos de mercado, canales y relaciones con los clientes.
- Diseñar el módulo de propuesta de valor del Business Model Canvas.
- Diseñar los componentes de la infraestructura del Business Model Canvas teniendo en cuenta los módulos de recursos, actividades y asociaciones claves.
- Diseñar los componentes de viabilidad económica del Business Model Canvas teniendo en cuenta los módulos de fuentes de ingresos y estructura de costos.

4. Marco Teórico (Referencial)

4.1 Marco Contextual

PCM es una compañía con más de 35 años de experiencia en el mercado de TI 100% colombiana, enfocada en la Seguridad, Administración y Gestión de Soluciones de TI, a través de la prestación de servicios acreditados. Son servicios acreditados ya que la compañía cuenta con la certificación ISO 20000, norma que acredita la prestación de servicios de TI.

Actualmente cuenta con 3 líneas de negocio definidas:

- PCM Mesa de Servicios TI
- PCM Seguridad TI
- PCM Plataforma TI

La línea Mesa de servicios TI fue la línea con la que inició y creció la compañía la cual estaba enfocada a la prestación de servicios de mantenimiento preventivo y correctivo de servidores equipos de cómputo. Dada la experiencia y conocimiento de su fundador el ingeniero electrónico Jaime Santamaria Sánchez sobre la tecnología que en ese entonces se manejaba le permitió darse a conocer y llegar ofrecer estos servicios a muchas empresas que usaban y demandaban servidores y equipos de cómputo. Años más tarde la empresa incursiona en la venta de computadores de marca y equipos clon principalmente, que eran equipos ensamblados y comercializados por PCM. Para la comercialización de estos equipos en el año de 1995, la empresa creó una marca ante la Superintendencia de industria y comercio llamada “PCM LA PC PERFECTA”. Estos equipos tenían una alta demanda por parte de los clientes y se vendían a muy buenos márgenes (entre el 25 y 40%) ya que los equipos de marca como lo eran “Compaq” y “Acer” entre otros los superaban casi en el doble de precio.

Ya hacia el año 2002 PCM decide incursionar al mercado de la seguridad informática y lo hace realizando una importante alianza con uno de los fabricantes líderes en seguridad a nivel mundial “McAfee”. Desde ese año y por varios años más, la compañía creció a través de la venta de contratos de soporte que incluían el licenciamiento de antivirus para estaciones de trabajo. PCM como estrategia de negocio decidió apostar a por una relación exclusiva con este fabricante por el posicionamiento de sus soluciones a nivel

mundial, pero para el año 2015 la compañía decide abrirse más a un espectro más amplio de fabricantes.

Hoy en día PCM cuenta con algún tipo de alianza con más de 10 fabricantes en sus 3 diferentes líneas de negocio en la venta e implementación de soluciones de TI. Para esta nueva línea de negocio que se desea desarrollar no se requiere ningún tipo de alianza con fabricantes. Se requiere de profesionales expertos y con amplia experiencia en seguridad informática aplicando distintas herramientas y metodologías que permitan frenar las acciones de los hackers que son los que penetran y vulneran las diferentes soluciones de seguridad que usan las organizaciones para proteger sus sistemas.

4.2 Marco Teórico Preliminar

Para ahondar sobre el Bussines Model Canvas es necesario remitirse en primera instancia a sus creadores (Osterwalder, Pigneur, 2010). Alexander Osterwalder es un teórico, autor, consultor y emprendedor, nacido en San Galo Suiza en 1974. (EAE BUSINESS SCHOOL, 2015) Es conocido por su trabajo en modelado de negocios y el desarrollo del lienzo de modelo de negocio que también es desarrollado en compañía de Ives Pigneur. Pigneur nacido en Bélgica en el año 1954 es un informático y profesor de Sistemas de Información de Gestión en la Universidad de Lausana desde 1984. Al ver el perfil de estos dos autores se percibe que fueron una gran conjugación entre marketing y tecnología, elementos clave en la generación del Business Model Canvas.

Para arrancar con la explicación del modelo, se iniciará con la definición Modelo de negocio. De entrada, se podría pensar que el origen de los modelos de negocio es de décadas recientes con el boom del internet, los sistemas de información y las nuevas tecnologías, donde encontramos ejemplos claros como UBER, AIRBNB y NETFLIX entre los más exitosos. El modelo de negocio data de 1954 con Peter Druker que introduce el término de “estrategia” en el mundo de los negocios, cuando esta palabra pertenecía exclusivamente al ámbito militar (Drucker, 1954, 1979, 1994). La estrategia en el ámbito empresarial se refiere al desempeño de la empresa en un entorno competitivo (Porter, 1991). Teniendo en cuenta estas definiciones es preciso definir la diferencia entre modelo de negocio y estrategia, ya que, aunque son complementarios tienen enfoques diferentes. El modelo de negocio se enfoca en la forma de entregar valor a los clientes, hacer dinero y es

estático mientras que la estrategia se centra en el factor diferenciador, es dinámica y reflexiva viendo de manera integral todos los componentes del modelo de negocio (Vicedo, 2015). El modelo de negocio viene siendo una especie de anteproyecto de una estrategia, es decir, permitirá contar con una radiografía clara y concisa que pueda ser comprendida e interiorizada en todos los niveles de una organización para poner en marcha la estrategia organizacional. Ahondando por ahora en la estrategia es necesario remitirse a la definición de Mintzberg, el cual la especifica en desarrollar la capacidad al interior de la organización para dar "Respuesta emergente a circunstancias no previstas". (Mintzberg, 1978, pág. 935), a partir de "un modelo en una corriente de decisiones o acciones" (Mintzberg, 1978, P935), sin que tenga que estar en todo el fundador de la empresa. Teniendo presente esta definición es imprescindible que la empresa cuente con una estrategia sólida y perdurable en el tiempo, que tenga en cuenta todas las variables del mercado y que pueda responder de manera rápida ante diferentes situaciones no previstas como lo menciono Mintzberg y es por esta razón que la estrategia es parte fundamental en la generación de un modelo de negocio.

Ahondando ya en los creadores del Business Model Canvas, para Osterwalder y Pigneur el modelo de negocio describe las bases sobre las que una empresa crea, proporciona y capta valor. (Osterwalder, Pigneur, 2010). Teniendo en cuenta esta definición se puede inferir que en la creación de un modelo de negocio se define el qué, a quiénes y cómo entrega valor y para seguir con esta lógica los autores plantearon su modelo dividiéndolo en nueve módulos básicos que reflejan la lógica que sigue una empresa para conseguir ingresos. Estos nueve módulos cubren las 4 áreas principales del negocio que son: clientes, oferta, infraestructura y viabilidad económica. (Osterwalder, Pigneur, 2010).

A continuación, se describirán los nueve módulos que compone el modelo basados en el libro de Generación de modelos de negocio

- Modulo Segmentos de Mercado: Este módulo define los diferentes sectores o entidades a los que se dirige la empresa. La empresa puede agrupar en uno o varios segmentos de clientes y a su vez los que no tendrá en cuenta. Teniendo esto definido ya se puede diseñar un modelo de negocio basado en un amplio conocimiento de las necesidades específicas del cliente objetivo. Este es de los primeros módulos que hay que definir, puesto que la oferta de valor puede variar dependido de cada segmento de clientes definido por la organización.

Los clientes pertenecen a segmentos diferentes si:

- Sus necesidades requieren o justifican una oferta diferente
- Son necesarios diferentes canales de distribución para llegar a ellos
- Requieren un tipo de relación diferente
- Están dispuestos a pagar por diferentes aspectos de la oferta

- Modulo Propuesta de Valor: En este se describen el conjunto de productos y/o servicios que crean valor para un segmento de mercado especifico. Es el factor que hace que un cliente se incline por una empresa u otra. La finalidad de esta es solucionar un problema y satisfacer una necesidad del cliente. Por ello hay que identificar claramente cuál es esa necesidad a satisfacer y cuál es el dolor del cliente en sus actividades *core* de negocio.

Una propuesta de valor crea valor para un segmento de mercado gracias a una mezcla especifica de elementos adecuados a las necesidades de dicho segmento. Los valores pueden ser cuantitativos (precios, velocidad del servicio) o cualitativos (diseño, experiencia del cliente). La combinación de estos elementos serán clave para diferenciarse muy bien de la competencia. Su éxito también dependerá de la definición e implementación de los demás módulos del modelo que interrelacionados puedan materializar dicha propuesta de valor.

- Módulo Canales: Este es el modo en que una empresa se comunica con los diferentes segmentos de mercado para llegar a ellos y proporcionarles una propuesta de valor. Los canales tienen 5 fases distintas, aunque no necesariamente se abarcan todas. Se pueden distinguir entre canales directos e indirectos, así como canales propios y canales de socios comerciales. A la hora de llevar la propuesta de valor a los diferentes segmentos, es necesario acertar la combinación exacta de canales para aproximarse a los clientes del modo adecuado.
- Módulo Relaciones con los Clientes: En este módulo se describen los diferentes tipos de relaciones que establece la empresa con determinados segmentos de mercado. Estas relaciones se pueden dar en distintos momentos como lo son la captación de clientes, la fidelización de clientes y la estimulación de las ventas. El tipo de relación que exige el modelo de negocio de una empresa repercute en gran medida en la experiencia global del cliente y en la medida que dicha experiencia sea positiva permitirá a la empresa fidelizar sus clientes.

- Módulo Fuentes de Ingresos: Este módulo se refiere al flujo de caja que genera una empresa en los diferentes segmentos de mercado. Acá lo crucial es determinar el valor que estaría dispuesto a pagar cada segmento de mercado. Aunque es evidente que los 9 módulos se interrelacionan entre sí, la fuente de ingresos tiene una fuerte relación con la propuesta de valor y lo clara que es esta para el cliente.
- Módulo de Recursos clave: Este módulo describe los activos más importantes par que el modelo de negocio funcione. Dentro de estos podemos encontrar recursos Físicos, Intelectuales, Humanos y Económicos. La clave está en articularlos muy bien para desarrollar la propuesta de valor.

Este módulo es de los más importantes a tener en cuenta para la generación de modelos de negocio. Hoy en día ya que en muchos modelos exitosos que han llegado al mercado, su éxito se basa en la infraestructura tecnológica, aunque esto se debe entrelazar con un recurso humano altamente capacitado y enfocado en la atención y fidelización de clientes.

- Módulo de Actividades clave: este módulo describe las acciones más importantes que debe emprender una empresa para que su modelo de negocio funcione. Las actividades principales de un modelo de negocio están determinadas por la forma en que la propuesta de valor resuelve la necesidad. Un factor clave de éxito se basa en el adecuado diseño del servicio para que una vez implementado contribuya a entregar esa propuesta de valor y satisfacer la necesidad de forma rápida y eficaz ya que con la evolución de las tecnologías los clientes viven en un ritmo de inmediatez que no espera.
- Módulo de Asociaciones clave: Este módulo describe la red de proveedores y socios que contribuyen al funcionamiento de un modelo de negocio. Hoy en día se habla de cuatro tipos de asociaciones: a) Alianzas estratégicas, b) Coopetición que es desarrollada entre competidores, c) Joint Ventures (empresas conjuntas) y d) Relaciones Cliente-proveedor
- Módulo de estructura de Costes: Este módulo describe todos los costes que implica la puesta en marcha de un modelo de negocio. Estos costes pueden variar dependiendo el modelo de negocio y la composición de cada uno de los demás módulos del modelo.

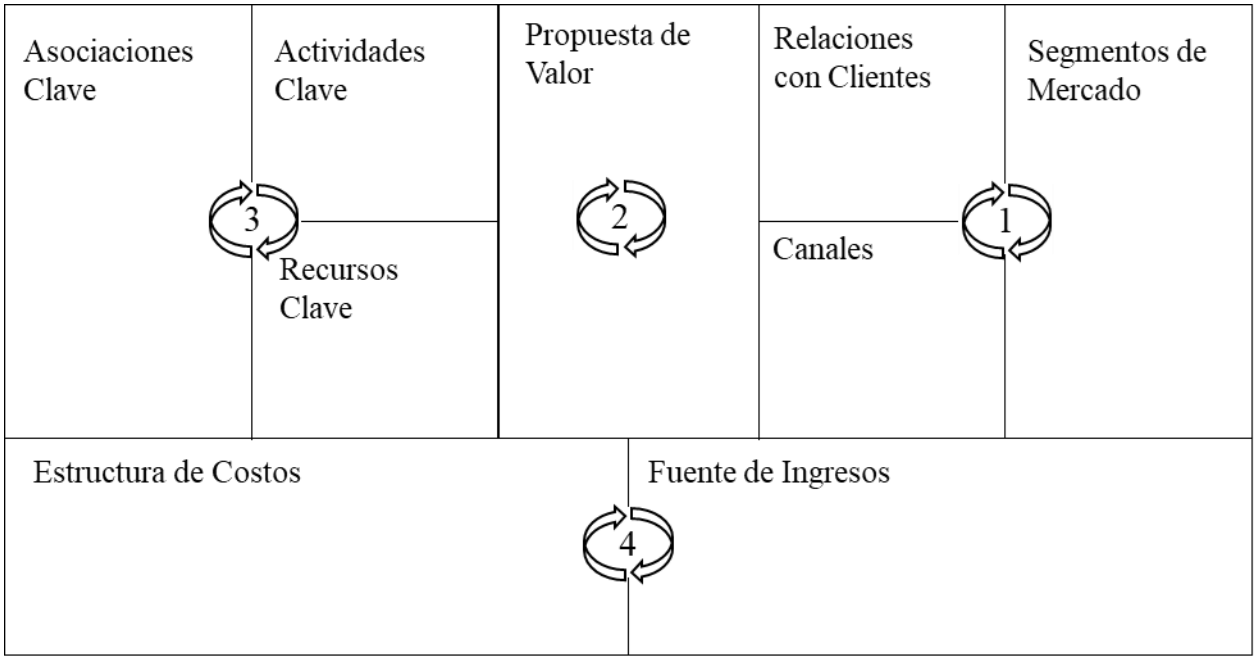

Figura 1. Tomado del libro Generación de Modelos de Negocio (Osterwalder, Pigneur, 2010). El área de clientes (1) cuenta con los módulos de Segmentos de Mercado, Relaciones con los Clientes y Canales. El área de oferta (2) corresponde al módulo de propuesta de valor. El área de infraestructura (3) corresponde a los módulos de Recursos Clave, Actividades Clave y Asociaciones Clave. El área de viabilidad económica (4) corresponde a los módulos de Estructura de Costes y fuentes de Ingresos.

4.2.1 Diseño del Business Model Canvas:

Para el diseño del Business Model Canvas los autores (Osterwalder, Pigneur, 2010), definieron 6 técnicas que son: aportaciones de clientes, ideación, pensamiento visual, creación de prototipos, narración de historias y escenarios

Aportaciones de clientes: este es un principio fundamental a la hora de construir el modelo de negocio ya que son ellos a los que vamos a entregar la propuesta de valor. Aunque también son muy buena fuente de información para definir los módulos de canales de distribución, relaciones con los clientes y fuentes de ingresos. Solo ellos saben muy bien cuál es su necesidad y como desean que sea satisfecha.

- Ideación: La ideación de modelos de negocio pueden tener varios epicentros. Puede ser basadas en recursos, en la oferta, en los clientes, en las finanzas o puede ser una combinación de varias. Para ello una de las técnicas más utilizadas es la de brainstorming o lluvia de ideas, la cual se debe basar en un equipo heterogéneo ya que no

se puede dejar en manos de personas con talento creativo, sino que debe ser una construcción conjunta de todo el equipo.

- Pensamiento visual: Esta técnica permite comprender mejor las diferentes interrelaciones de cada uno de los módulos y una mejor construcción del debate, en torno a la creación del modelo de negocio. En esta los autores destacan 4 procesos que el pensamiento visual ayuda a mejorar: comprensión, dialogo, exploración y comunicación.
- Creación de prototipos: la creación de prototipos va más enfocada hacia, productos, arquitectura y diseño. No es tan habitual usar esta técnica en el ámbito empresarial. La creación de prototipos se puede visualizar en diferentes escalas que son: Dibujo en una servilleta, Lienzo elaborado, Plan de negocio, Prueba de campo.
- Narración de historias: esta técnica permite a los interlocutores a abrir la mente a nuevas posibilidades donde es preciso realizar una narración esquemática y detallada. Además, permite implicar a los empleados para que se familiaricen con la creación del modelo de negocio y hagan sus aportaciones.
- Escenarios: Su función principal es aportar al desarrollo del modelo un contexto de diseño detallado y específico, donde se describen todos los aspectos relacionados con el cliente.

La aplicación de estas seis técnicas de diseño del Business Model Canvas se pueden desarrollar tanto de manera independiente como combinada, la elección de las técnicas a utilizar dependerá del enfoque del modelo de negocio y de los resultados que se quieran obtener.

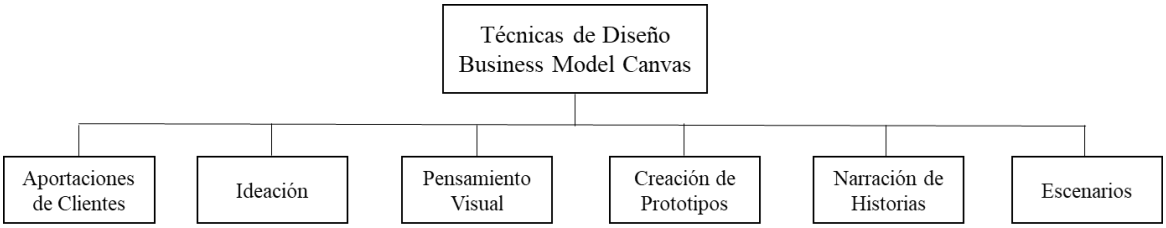

Figura 2. Técnicas de Diseño del Business Model Canvas

4.2.2 Proceso de diseño de modelos de negocio:

Para el proceso del diseño del modelo de negocios los autores (Osterwalder, Pigneur, 2010) lo definieron en 5 fases:

- Movilización: esta fase consiste en la preparación del escenario, contando con todos los elementos necesarios y describiendo la motivación que se tiene para desarrollarlo y contar con una idea común dentro del equipo.
- Comprensión: En esta fase se realiza la investigación de los elementos necesarios para el diseño del modelo, es decir lo necesario para cada módulo del modelo.
- Diseño: convierte la información y las ideas en prototipos de modelo de negocio con el fin de explorar y comprobar el mejor diseño que cumpla las expectativas.
- Aplicación: Esta fase hace referencia a la aplicación efectiva del prototipo.
- Gestión: Permite la modificación del modelo de acuerdo a la reacción del mercado.

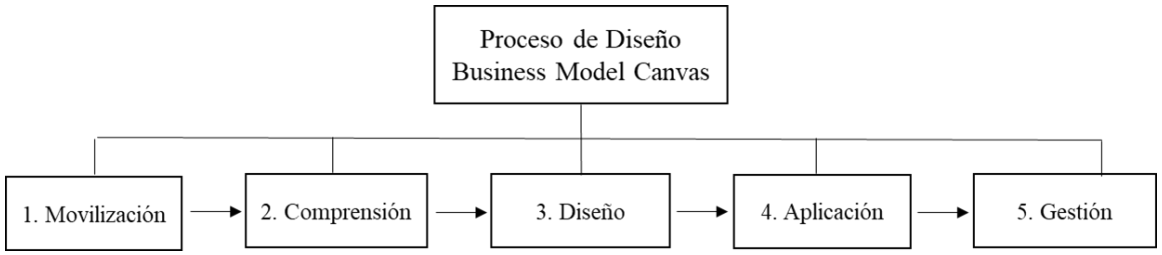

Figura 3. Proceso de Diseño del Business Model Canvas

4.3 Marco Legal

El inminente crecimiento de ataques informáticos ocurridos en los últimos años, representa un aumento de los riesgos cibernéticos a nivel mundial y evidencia la importancia de la ciberseguridad para todos los usuarios del ecosistema digital (personas, empresas e instituciones gubernamentales); los sistemas de telecomunicaciones son siempre un objetivo lucrativo para los ciberdelincuentes, porque representan la columna vertebral necesaria para el intercambio de información como voz, vídeo, datos, conectividad a Internet y almacenan gran cantidad de datos personales y empresariales (SYMANTEC, 2017). La información robada, en cualquier empresa, podría tener serias implicaciones como la interrupción de servicios esenciales, robo de identidad, acceso no autorizado a sistemas, pérdidas económicas y de clientes, que pueden derivar en pérdida de la reputación o daño a la marca de una empresa y afectar su valoración financiera.

Dado el interés de prestar servicios especializados en Ciberseguridad, es necesario para el desarrollo del diseño, conocer cuáles son las leyes, normas y tratados que

penalicen cualquier conducta ilícita en el ciberespacio y que afecta tanto a los ciudadanos como a las empresas y entidades gubernamentales. Para ello se analizarán las leyes y marcos regulatorios desde el ámbito internacional a las que se aplican y rigen en Colombia. Así mismo se analizará el estándar técnico que se creó para la gestión de la seguridad de la información y la ciberseguridad.

4.3.1 Convenio de Budapest (Ciberdelincuencia)

En primera instancia se toma como El Convenio de Budapest, sobre la Ciberdelincuencia (CONSEJO DE ESTADOS DE EUROPA, 2001) ya que es el primer tratado internacional que busca hacer frente a los delitos informáticos y los delitos de internet. Mediante la armonización de leyes nacionales, mejora de las técnicas de investigación y cooperación entre las naciones. El convenio tiene cuatro capítulos, en los que además de definirse una serie de terminologías en común, se establecen tres ejes esenciales para hacer frente a los delitos informáticos:

En el primer eje se aborda el tema de los delitos informáticos, y tiene como objetivo establecer un catálogo de figuras dedicadas a penar las modalidades de criminalidad informática. Es decir, en este capítulo se definen los delitos y se los clasifica en 4 categorías:

- Delitos que tienen a la tecnología como fin: que atentan contra la confidencialidad, integridad o disponibilidad de la información. Por ejemplo, el daño informático o el acceso ilícito a un sistema.
- Delitos que tienen a la tecnología como medio: se refiere a delitos ya conocidos, que se cometen a través de un sistema informático. Son delitos comunes, que ya se encuentran tipificados en la mayoría de las legislaciones, ampliados a los medios digitales. Por ejemplo, el fraude informático o la falsificación de datos digitales.
- Delitos relacionados con el contenido: establece como delitos diversos aspectos de la producción, posesión y distribución electrónica de pornografía infantil.
- Delitos relacionados con infracciones a la propiedad intelectual: se refiere a la reproducción y difusión en Internet de contenido protegido por derechos de autor, sin la debida autorización. Por ejemplo: infracciones a la propiedad intelectual, piratería.

En el segundo eje se abarcan las normas procesales: aquí se establecen los procedimientos para salvaguardar la evidencia digital, así como también las herramientas

relacionadas con la manipulación de esta evidencia. El alcance de esta sección va más allá de los delitos definidos en el punto anterior, ya que aplica a cualquier delito cometido por un medio informático o cualquier tipo de evidencia en formato electrónico. Entre otras cosas determina la obtención y conservación de datos digitales para ser utilizados como pruebas.

El tercer eje contiene las normas de cooperación internacional, que son reglas de cooperación para investigar cualquier delito que involucre evidencia digital, ya sean delitos tradicionales o informáticos. Incluye, entre otras, disposiciones acerca de la localización de sospechosos, recolección o envío de evidencia digital, e incluso lo referente a extradición. Es de resaltar que en el congreso de Colombia se radico un proyecto de ley para adherirse al convenio mostrando un serio compromiso en la lucha contra los ciberdelincuentes.

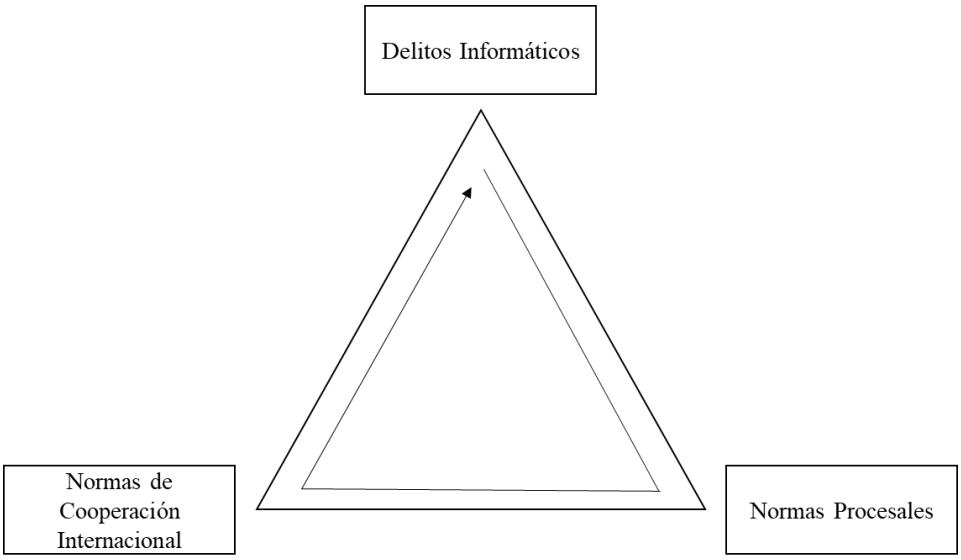

Figura 3. 3 ejes del convenio de Budapest (Ciberdelincuencia)

4.3.2 Leyes en Colombia

A nivel Colombia se resaltan las siguientes leyes:

4.3.2.1 Ley 1273 de 2009:

Esta ley hace referencia a los delitos penales relacionados con delitos informáticos y la protección de la información. Se modifica el Código Penal, con la creación de un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones. En ella se destacan los siguientes artículos:

- ART 269A: Acceso abusivo a un sistema informático
- ART 269B: Obstaculización ilegitima de sistema informático o red de telecomunicaciones
- ART 269C: Interceptación de datos informáticos
- ART 269D: Daño informático
- ART 269E: Uso de software malicioso
- ART 269F: Violación de Datos Personales
- ART 269G: Suplantación de sitio web para capturar datos personales
- ART 269H: Agrega agravantes en algunos aspectos de la pena impuesta
- ART 269I: Hurto por medio informático y semejante
- ART 269J: Transferencia no consentida de activos.

Esta Ley es un paso muy importante en la lucha contra los delitos informáticos en Colombia y la preparación de cómo enfrentar los retos legales que plantea el avance tecnológico. Las empresas se deben adecuar y crear los mecanismos idóneos para la protección de uno de sus activos más importantes como lo es la información.

4.3.2.2 CONPES 1701 (Consejo Nacional de Política Económica y Social):

Fue creado por la Ley 19 de 1958. Representa la máxima autoridad nacional de planeación y desempeña el rol de asesor en todos los aspectos relacionados con el desarrollo económico y social del país. Mediante el CONPES, Colombia se convierte en el primer país de Latinoamérica en incorporar plenamente las recomendaciones y prácticas internacionales en seguridad de riesgos de seguridad digital; por medio del cual se ha emitido los siguientes documentos en materia de Seguridad informática:

- CONPES 3701 DE 2011 que habla de los Lineamientos de Política para Seguridad y Ciberdefensa, que busca fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético (ciberseguridad y ciberdefensa), creando el ambiente y las condiciones necesarias para brindar protección al ciberespacio.
- CONPES 3854 DE 2016 que es el modelo de Riesgos de Seguridad Digital, que se enfoca en modernizar al país y reaccionar oportunamente ante los riesgos de

posibles peligros, en cuanto a infraestructura e información digital y que tiene como objetivo:

> Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país. (Mintic, 2017)

4.3.2.3 Circular Externa 007 de 2018:

En el 2018 la Superintendencia Financiera de Colombia emitió la "CIRCULAR EXTERNA 007 DE 2018" de junio 05 de 2018, donde Imparte instrucciones relacionadas con los requerimientos mínimos para la gestión del riesgo de ciberseguridad en las entidades vigiladas y estándares de seguridad con el objetivo de fortalecer la protección de la información de los consumidores financieros. Fue expedida teniendo en cuenta el auge de la digitalización de los servicios financieros y la masificación de los canales electrónicos que aumenta la administración de los riesgos operativos y la seguridad de la información.

Adicionalmente, establece a las entidades vigiladas la inclusión del plan de continuidad del negocio, la respuesta, recuperación, reanudación de la operación en momento de una contingencia y la restauración de los procesos ante la materialización de un ataque cibernético y pérdida de información.

Uno de los requerimientos que deberán cumplir las entidades vigiladas en materia de ciberseguridad está en la conformación de una unidad que gestione los riesgos de seguridad de la información y la ciberseguridad. Adicionalmente, informar a los consumidores financieros sobre los incidentes cibernéticos que se presenten y que puedan afectar la confidencialidad o integridad de su información y las medidas adoptadas para solventar la situación. Esto supone para las entidades contar con las tecnologías y los procesos adecuados para tener una total visibilidad de las amenazas ya sean propias o de proveedores de servicios.

Es de destacar que es imperativo para las organizaciones adoptar controles y procesos de ciberseguridad no solo por el riesgo mismo de las amenazas sino también en el mismo sentido cumplir con normas y reglamentaciones para garantizar y salvaguardar la tanto la información de la compañía como la información que manejan de sus clientes ya que por la pérdida de estas les pueden acarrear sanciones económicas muy significativas.

4.3.3 Norma ISO 27032 "Gestión de la Ciberseguridad"

Como es conocido a nivel mundial, La Organización Internacional de Normalización, promueve el uso de estándares, que facilita la creación de productos y servicios. A nivel de la ciberseguridad no se podía quedar a través y es por eso que en 2005 se publicó la primera versión de este estándar y donde actualmente la última revisión fue publicada en 2013.

Esta norma facilita la colaboración segura y fiable para proteger la privacidad de las personas en todo el mundo. De esta manera, puede ayudar a prepararse, detectar, monitorizar y responder a los ataques. La organización espera que ISO/IEC 27032 permita luchar contra ataques de ingeniería social, hackers, malware, spyware y otros tipos de software no deseado. Utilizando los puntos técnicos y estratégicos más importantes para esa actividad y los que están relacionados con: La seguridad en las redes, seguridad en internet, seguridad de la información y seguridad de las aplicaciones.

Dentro de su alcance, la definición de Activos en el Ciberespacio, considera como tales aquellos que entregan valor a la organización, así como información, software, hardware, servicios, personas con sus habilidades y experiencias, y los activos intangibles, como la reputación y la imagen ante los clientes. Así mismo define los controles técnicos, un aspecto relevante de la Norma como los ataques de ingeniería social, hacking, software malicioso, spyware y otros programas no deseados.

El desarrollo de un ciclo de revisión y mejora continua a estos controles permitirá apoyar los lineamientos establecidos en la norma y tener un panorama claro de las amenazas, vulnerabilidades, zonas de riesgos y criterios de aceptación, que permitan optimizar la inversión en seguridad y priorizar la implementación de controles y salvaguardas. Por último, destacar la Concientización y Capacitación a los empleados en los

riesgos existentes a nivel de seguridad informática como un punto importante a desarrollar dentro las Organizaciones.

Por lo anteriormente mencionado se ve la importancia y la necesidad de las organizaciones contar un estándar que sirve como hoja de ruta para implementar y gestionar los controles necesarios para evitar ser víctimas de los ciberdelincuentes. Si bien es cierto que ya se encuentra con unos lineamientos a nivel de ciberseguridad es necesario que las organizaciones cuenten con el apoyo de consultores expertos que los asesoren y los orienten ya que la curva de aprendizaje para una organización es lenta y compleja.

5. Metodología

El desarrollo del diseño del Business Model Canvas se llevó a cabo bajo dos métodos: Uno bajo una perspectiva de investigación Teórica la cual se desarrolló a lo largo del marco teórico y donde se puntualizó cada uno de los módulos del Business Model Canvas y que será el input para el desarrollo del otro método. El otro método se basó en la construcción de una metodología desarrollada en 4 fases las cuales se desarrollaran según lo planteado por los autores en el proceso del diseño del Business Model Canvas:

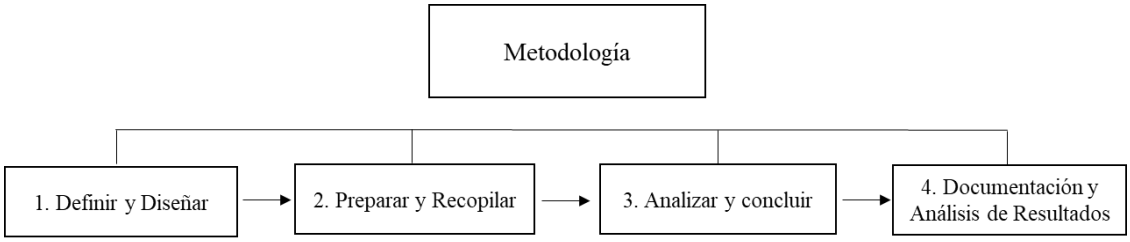

Figura 4. Metodologia.

5.1 Definir y diseñar: Para el diseño del Business Model Canvas como se mencionó anteriormente en el marco teórico los autores Alexander Osterwalder e Yves Pigneur plantearon 6 instrumentos para la fase de diseño que son: 1) Aportaciones de clientes. 2) Ideación. 3) Pensamiento visual. 4) Creación de prototipos. 5) Narración de historias. 6) Escenarios

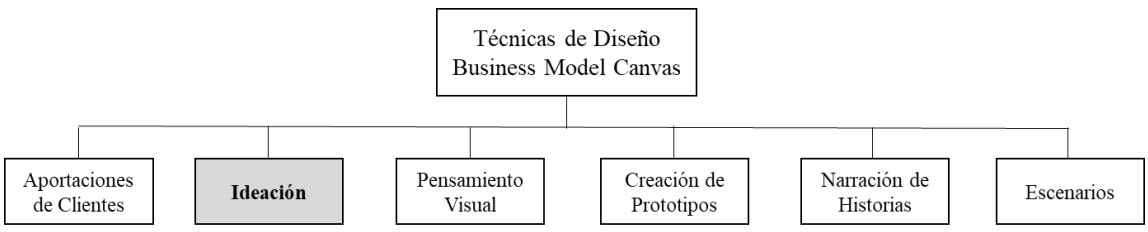

Figura 5. Selección técnica de Diseño Business Model Canvas

Para el diseño del Business Model Canvas de la "UES – Unidad estratégica de Seguridad" se centró en "Ideación" el cual se concentrará en una sesión de Brainstorming o lluvia de ideas.

Adicional al diseño también es importante y relevante tener en cuenta el proceso. Para el proceso los autores definieron 5 fases que son: 1) Movilización. 2) Compresión. 3) Diseño. 4) Aplicación. 5) Gestión.

Para pertinencia del presente proyecto de grado se enfocó en las 3 primeras fases del proceso las cuales concluirán con la proposición del Business Model Canvas para la "UES – Unidad Estratégica de Seguridad". Las fases 4. Aplicación y 5. Gestión no se aplicarán ya que estas fases son posteriores al enfoque del proyecto de grado que es el Diseño del Business Model Canvas.

Para la realización del brainstorming se desarrolló con los siguientes directivos de la compañía:

- Jaime Santamaria – Gerente general.
- Maria Fernanda Torres – Gerente de negocios y operaciones.
- William Botonero – Director de ingeniería y preventa.
- Jeny Santamaria – Directora de Calidad y gestión de servicios de TI
- Julian Martinez – Especialista de Seguridad informática.

De acuerdo con (Osterwalder, Pigneur, 2010) es importante para el proceso contar con un equipo heterogéneo e interdisciplinario ya que esto contribuye a la generación, discusión y selección de ideas y que este proceso no se debe dejar exclusivamente a personas que se consideren creativas.

Para el desarrollo del brainstorming se contó con un lienzo impreso grande del Business Model Canvas donde cada uno coloco "post it" con las ideas que surgieron de cada uno de los 9 módulos del Business Model Canvas.

Adicional se llevaron las siguientes preguntas planteadas por los autores por cada uno de los módulos. Esto permitió facilitar el desarrollo de la sesión (ver Tabla 1.)

TABLA 1.
Preguntas guía para el desarrollo de los módulos del modelo Canvas.

Segmentos de mercado	¿Para quienes creamos valor? ¿Cuáles son nuestros clientes más importantes? ¿En qué segmentos o grupos de clientes nos vamos a enfocar? ¿Cómo vamos a agrupar esos segmentos de clientes?
Canales	¿Qué canales prefieren nuestros segmentos? ¿Cómo establecemos actualmente el contacto con los clientes? ¿Cómo se conjugan nuestros canales? ¿Cuáles tienen mejores resultados? ¿Cuáles son los canales más rentables? Fases del Canal 1. Información: ¿Cómo damos a conocer los productos y servicios de PCM? 2. Evaluación: ¿Cómo ayudamos al cliente a evaluar nuestra propuesta de valor? 3. Compra: ¿Cómo pueden comprar nuestros clientes nuestros productos y servicios? 4. Entrega: ¿Cómo entregamos a los clientes nuestra propuesta de valor? 5. Postventa: ¿Qué servicio de atención postventa ofrecemos? ¿Cómo va a ser esa comunicación una vez sean nuestros clientes? ¿Cómo será su fidelización?
Relaciones con los clientes	¿Qué tipo de relación esperan los diferentes segmentos de mercado? ¿Qué tipos de relaciones hemos establecido? ¿Cómo se integran en nuestro modelo de negocio? ¿Cuál es nuestro cliente más antiguo? ¿Qué hemos hecho bien para tener este cliente por varios años?
Propuesta de Valor	¿Qué valor proporcionamos a nuestros clientes? ¿Qué problemas de nuestros clientes ayudamos a solucionar? ¿Qué necesidades de los clientes ayudamos a solucionar? ¿Qué paquetes de productos o servicios ofrecemos a cada segmento de mercado? ¿Cómo podemos diferenciar nuestra oferta de valor de la de la competencia? ¿Cuál será la variable que predomine en nuestra oferta de valor? (Precio, personalización, Rapidez, reducción de riesgos)

Recursos Clave	¿Qué recursos clave requieren nuestras propuestas de valor, canales de distribución, relaciones con clientes, y fuentes de ingresos? ¿Cuál es la infraestructura ideal con la que debemos contar para entregar nuestra propuesta e valor? ¿Cuáles son los perfiles con los que debe contar nuestra área de ingeniería en especial la Unidad estratégica de Seguridad? ¿Cuál es el plan de formación que debe tener nuestros ingenieros?
Actividades Clave	¿Qué actividades clave requieren nuestras propuestas de valor, canales de distribución, relaciones con los clientes y fuentes de ingresos? ¿Cómo vamos a atraer a nuestros segmentos de mercado? ¿Cómo se van a resolver los problemas de los clientes de una manera rápida y oportuna? ¿Cuáles serán nuestros tiempos de respuesta?
Asociaciones clave	¿Quiénes son nuestros socios clave? ¿Quiénes son nuestros proveedores clave? ¿Qué recursos clave adquirimos a nuestros socios? ¿Qué actividades clave realizan nuestros socios?
Fuentes de ingresos	¿Qué valor están dispuestos a pagar nuestros clientes? ¿Por qué pagan actualmente? ¿Cómo pagan actualmente? ¿Cuánto podría reportar en ingresos la "UES – Unidad estratégica de Seguridad" frente al total de ingresos?
Estructura de costos	¿Cuáles son los costos más importantes e inherentes a nuestro modelo de negocio? ¿Cuáles son los recursos clave más costosos? ¿Cuáles son las actividades clave más caras?

5.2 Preparar y recopilar: Una vez se realizó el proceso de brainstorming con el equipo directivo de PCM SAS, se procedió a recopilar las ideas y factores clave de cada uno de los nueve módulos del Business Model Canvas. En primera instancia se empezó por los módulos de propuesta de valor y actividades clave que fueron los que por consenso se dieron para iniciar y después se fueron desarrollando los siguientes módulos.

5.3 Analizar y concluir: Luego de haber realizado el brainstorming se precedió a la selección de las ideas más relevantes para cada uno de los 9 módulos y donde se definió el Business Model Canvas para la UES de PCM SAS en un lienzo.

5.4 Documentación y discusión de resultados: Luego de haber realizado la recopilación de la información y haber definido las ideas para cada uno de los módulos se analizó la viabilidad económica a través una proyección de ingresos y costos teniendo presente lo que se definió en cada uno de los módulos del Business Model Canvas.

6. Resultados

De acuerdo a la generación, selección y definición de los aspectos más relevantes encontrados en el brainstorming, a continuación, se presenta el Business Model Canvas propuesto para la UES en el siguiente lienzo:

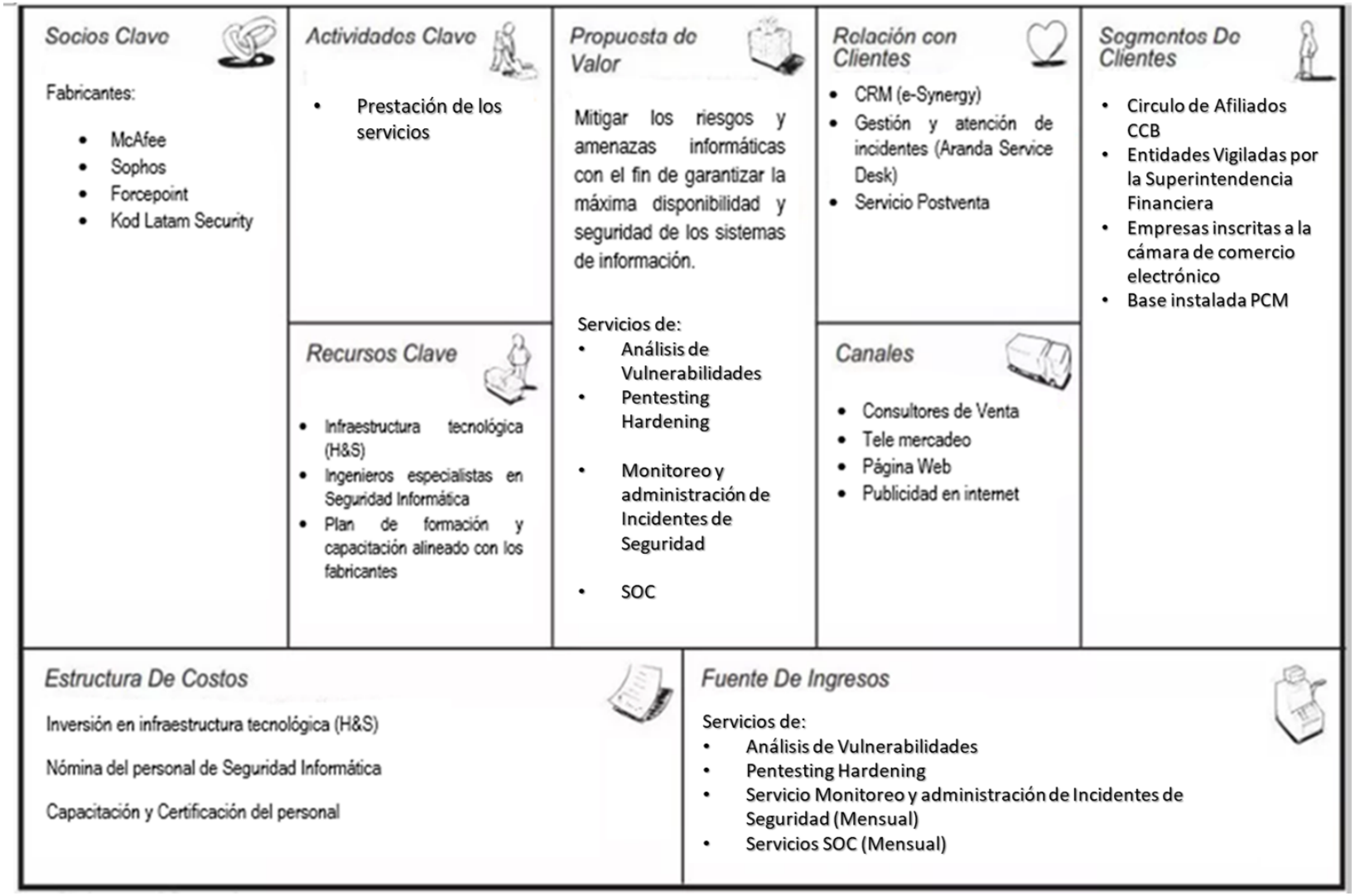

Figura X. Resultado Business Model Canvas UES

Una vez plasmado el Business Model Canvas se desagregaron cada uno de los 9 módulos, basándonos en las 4 áreas principales del negocio (clientes, oferta, infraestructura y viabilidad económica), como lo plantearon los autores.

6.1 CLIENTES

Para el componente de clientes del Business Model Canvas (segmentos de mercado, canales y relaciones con los clientes) se concluyó lo siguiente:

6.1.1 Segmentos de mercado: Hacia el 2002 cuando la compañía inició la venta de soluciones de seguridad con el fabricante McAfee se determinó un perfil de cliente de empresas que tuvieran como mínimo 150 computadores en su infraestructura ya que el modelo de servicio para empresas con una cantidad menor a estos computadores requería de un mayor desgaste operativo y una menor rentabilidad para la empresa. Por esta razón la empresa se enfocaba en empresas medianas y grandes principalmente.

Para los servicios de la UES el espectro de clientes potenciales se amplía a cualquier tipo de empresa y abarca desde empresas pequeñas que cuenten con una infraestructura tecnológica básica hasta infraestructuras tecnológicas muy robustas y complejas de administrar. Todas estas empresas se encuentran expuestas a cualquier tipo de amenaza y tienen la necesidad de asegurar tanto sus infraestructuras tecnológicas como su información.

En función de esto, se propusieron los siguientes segmentos de clientes para la prestación de los servicios de la UES:

• Base instalada de clientes y prospectos de PCM: Desde el año 2006 la empresa cuenta con un CRM (E-SYNERGY) en el cual se encuentra alojada toda la información de clientes y prospectos en los que durante estos años ha mantenido relaciones comerciales. Actualmente se encuentra la información de alrededor de 2400 cuentas donde se excluyeron alrededor de 800 que son cuentas de gobierno, aunque cabe aclarar que no es que las cuentas de gobierno no se puedan atender, sino que la empresa se concentrará en empresas del sector corporativo. De estas 1600 se realizó un filtro quedando alrededor de 1000 cuentas potenciales entre clientes actuales, algunos que fueron clientes en el pasado y prospectos que también se contactaron y se tuvo alguna relación

• Empresas vigiladas por la Superintendencia Financiera de Colombia: Como se mencionó en el marco legal a través de la circular 007, las empresas que son vigiladas por este ente deben cumplir con una normatividad y contar con procesos establecidos para

manejo de los riesgos de ciberseguridad. Se logró determinar en la página de la superintendencia financiera que el total de empresas vigiladas por este ente son 409, donde se excluyeron entidades bancarias por motivos de barreras de entrada de este sector a nuevos proveedores, quedando un total de 265 empresas.

• Empresas afiliadas a la cámara de colombiana de comercio electrónico: Este tipo de empresas son un segmento bastante atractivo, ya que deben garantizar ciertos protocolos de seguridad tanto a las empresas que venden productos por internet como a los usuarios que realizan compras seguras a través de internet. En la página de la cámara de comercio electrónico (www.ccce.org.co) se encuentran alrededor de 300 afiliados dentro de los cuales se encuentran empresas que venden a través de internet, bancos y pasarelas de pago. Dentro de esa base se descartaron los bancos y algunas multinacionales que gestionan todos sus servicios desde casa matriz. Basados en estas exclusiones se cuentan con alrededor de unas 180 empresas que son potenciales para los servicios de la UES.

Según el banco de la república en el 2017 las ventas de e-commerce por valor de $17.850 millones de dólares y se proyecta para 2021 ventas por $ 21.073 millones de dólares con un incremento del 18%.

De acuerdo con la cámara colombiana de comercio electrónico, en Colombia existen un poco más de 97 pasarelas de pago al cierre del 2018 dentro de las que se destacan PAGOS EN LINEA, PAGOS INTELIGENTES, EPAYCO, INTERPAGOS, PAGO DIGITAL, RECAUDO EXPRESS, EV1ENLINEA, DICMAX, SHOPIFY, KUSHKI y MERCADO LIBRE entre otras**.**

• Empresas pequeñas y medianas que necesitan gestionar y administrar las amenazas e incidentes de seguridad y que no cuentan con los recursos ni las capacidades para gestionarlas y solo desean enfocarse en la operación Core de su negocio. PCM cuenta con la base de datos del círculo de afiliados de la cámara de comercio de Bogotá donde se encuentran 12.182 empresas las cuales se excluyeron 2745 empresas teniendo en cuenta las siguientes variables según la pertinencia de la empresa:

▪ Excepción de las personas naturales

- Excepción de empresas ubicadas fuera de Bogotá, pero con la inclusión de Cajicá, chía, Soacha y cota ya que en estas se encuentran una gran cantidad de empresas potenciales

- Ingresos superiores a $ 500 millones de pesos

- Utilidades superiores a $ 100 millones de pesos

- Que cuenten con más de 50 empleados

Realizando estos filtros el potencial de empresas del círculo de afiliados de la cámara quedaron 9.437 empresas, que tienen como características comunes el manejo y la seguridad de la información sensible que necesita ser protegida en primera instancia y en segunda instancia que cuente con algún respaldo (Back up de la información) de la misma ya sea localmente o en la nube.

Cabe resaltar que a medida que se gestione la base de datos, la empresa tendrá en cuenta otros filtros como lo son sector, y personal ocupado. Teniendo estos diferentes segmentos de mercado a continuación se muestra el tamaño de los diferentes segmentos de mercado potenciales propuestos para la UES (ver Tabla 2)

TABLA 2.
Segmentos de mercado

Cantidad de empresas	Segmento de mercado
1000	CRM (SYNERGY)
265	Vigiladas por la supe financiera
180	Afiliados Cámara de Comercio Electrónico
9437	Círculo de afiliados CCB
10882	**Total**

Aunque se definieron estos segmentos a atacar también la compañía seguirá en la búsqueda de otros segmentos más específicos ya que se están creando normativas y cumplimientos para las empresas para mitigar los riesgos de ciberseguridad, perdida de información y manejo adecuado de datos de sus clientes. Adicionalmente en PCM se está

explorando la incursión de otros mercados en ciudades intermedias como Tunja, Bucaramanga, Manizales y Pereira entre otras que también son mercados potenciales para la prestación de los servicios de la UES.

6.1.1 Canales: En la parte de canales se deben contemplar de dos tipos. El primero es referente a la captación de clientes y el segundo referente a la atención de los clientes de la empresa. Para la captación de clientes se identificaron los siguientes canales:

- Fuerza de Ventas: Históricamente PCM ha contado en promedio su fuerza de ventas como mínimo con 3 consultores o ejecutivos de venta. Este número se basa en el histórico de ventas que año a año tiene la empresa y por la cantidad de oportunidades y cuentas a gestionar por parte de la empresa mensualmente para abarcar tanto sus clientes actuales como sus prospectos, los cuales venden de manera transversal todo el portafolio de productos y servicios de la compañía. Para los servicios de la UES se realizará la contratación de un perfil específico para atender la demanda que se va generando a través de la gestión de este y de los demás canales dispuestos para generar demanda. Aunque se contratará este perfil especifico se debe desarrollar un proceso de formación y capacitación a los demás consultores para que también detecten oportunidades de negocio para esta nueva línea. A medida que va creciendo el número de prospectos se contemplará la contratación de un segundo consultor para el 4 mes con el fin de no dejar desatendida la nueva demanda que se va generando.

A nivel de costos se tendrá el salario de consultor que será de $ 1.800.000 de salario base más comisiones de acuerdo con lo determinado por la gerencia comercial. Las comisiones para esta línea serán del 8% de la facturación.

- Tele mercadeo: Para esta actividad la empresa decide subcontratar con una empresa especializada que permita generar contactos con prospectos potenciales. En esta labor se contará con una persona enfocada en la promoción de los servicios de la UES. Con esta empresa se acordó de un valor mensual de 3 millones de pesos donde la persona estará dedicada a contactar a todos los prospectos que se definieron en el módulo de segmentos de mercado. Adicional en esta labor la empresa generará reportes diarios de gestión que le permitirá a la empresa generar métricas de cumplimiento de la gestión y generar oportunidades para que sean desarrolladas y gestionadas por el consultor comercial.

Esta labor será contratada en principio por 3 meses donde se evaluará la continuación o no con base en los resultados obtenidos

- Página Web: Se contratará una empresa especializada en el diseño de un sitio web que trabaje con procesos de optimización SEO o búsqueda orgánica que permita a los clientes encontrar nuestros servicios de una manera fácil y además de esto debe tener un componente de fácil administración para personas que no cuentan con conocimiento de programación web. Este sitio web será diseñado bajo una herramienta de fácil administración y actualización para que cualquier persona que no tenga conocimientos técnicos en sitios web la pueda modificar sin necesidad de contratar nuevamente a un experto, por ende, la administración será ejecutada por la persona de marketing de la compañía, lo cual no generara una contratación adicional para la empresa.

Para la contratación del sitio web PCM recibió varias propuestas donde oscilan entre $ 1.500.000 y $ 2.500.000. Los diferentes precios varían en función del alcance del diseño y la optimización SEO y se seleccionó al proveedor que cumplía con ambos requerimientos e igualmente por el valor económico como segundo factor de decisión.

A nivel de contenido el proveedor deberá realizar dicha optimización SEO, que es posicionar el sitio web de manera orgánica para que los posibles clientes que están interesados en contratar cualquiera de los servicios de la compañía encuentre en los 3 primeros resultados de búsqueda el sitio web. Adicional a esto se debe contar con un contenido claro y conciso de los servicios que la empresa, así como todos los posibles mecanismos de contacto (Teléfono, mail, formulario de contacto).

- Publicidad por internet: Dado que el segmento de mercado definido por la compañía es un mercado corporativo se descartó la publicidad a través de las redes sociales ya que estas van enfocadas más a un consumo masivo. Se contratarán campañas directamente con GOOGLE, a través de anuncios pagos con la aplicación de Google Adwords. Estos anuncios les aparecen a los usuarios de internet cuando realizan búsquedas con las palabras clave que previamente se definieron y que tienen que ver con los servicios de la compañía. Esta publicidad es complementaria al diseño y optimización del sitio web de la compañía. Este canal también es administrado y gestionado por el personal actual de mercadeo de la empresa. La inversión en anuncios será en promedio de $ 600.000 mensuales

de acuerdo con el histórico de la compañía, las cuales serán administradas por el encargado de mercadeo de la empresa.

- Redes sociales: Como complemento a la página y publicidad se debe contar con una estrategia de redes sociales, pero más como un mecanismo de posicionamiento de marca de la compañía que para la consecución de nuevos clientes ya que el segmento de clientes que atiende la empresa no son personas naturales sino jurídicas. Estas serán administradas por la persona de mercadeo actual de la compañía
- Mail marketing: se generarán envió de campañas a través del correo electrónico. La empresa viene utilizando la herramienta vía web de envíos de correo (MAILCHIMP, s.f.) la cual se viene utilizando la versión free ya que el envío de correos de la compañía no supera los 12.000 correos al mes permitidos en la versión gratuita. Se tiene contemplado el envío de 2 campañas al mes.

6.1.2 Relaciones con los clientes: PCM cuenta con una solución de CRM (E-SYNERGY) que permite gestionar y llevar una trazabilidad de las interacciones con prospectos como con los clientes.

A nivel de relaciones con los clientes se gestionará a través de un procedimiento de atención de incidentes a través de la mesa de ayuda, el cual tendrá definidos unos tiempos de respuesta que van en función de las categorías de alertas. Todo esto se almacenará y se gestionará a través de la consola Aranda Service Desk con que cuenta PCM, la cual permite llevar la trazabilidad de todos casos creados por los clientes. Adicional a esto los clientes de la UES se incluirán en el proceso de encuestas de satisfacción de los clientes que la empresa lleva con todos sus clientes para evaluar la calidad del servicio y las oportunidades de mejora.

Como inicialmente se tiene contemplado la prestación de servicios de consultoría en ethical hacking y análisis de vulnerabilidades para la UES, como incentivo para los clientes se ofrecerá un Health check sin costo, que es un diagnóstico que se realiza a la infraestructura del cliente el cual nos arroja una serie de recomendaciones para mejorar y optimizar las infraestructuras de TI. Este Health Check contribuirá a que los clientes pueden ver la calidad de los servicios y se generen más oportunidades de negocio.

6.2 OFERTA

En el componente de oferta del Business Model Canvas (propuesta de valor) se propuso lo siguiente:

- **Propuesta de valor:** Para la propuesta de valor se inició por determinar cuál es la necesidad que se estaría satisfaciendo y se llegó a la siguiente declaración:

"Mitigar los riesgos y amenazas informáticas con el fin de garantizar la máxima disponibilidad y seguridad de los sistemas de información."

Esta propuesta de valor busca apoyar a todas las empresas a tener una visibilidad y un control sobre las amenazas informáticas que como lo mencionamos tienen un crecimiento exponencial, mostrando en Latinoamérica un aumento del 60% en 2018 respecto del año anterior según un reporte de KASPERSKY LAB; y que día a día son más avanzados vulnerando las soluciones tradicionales con las que cuentan los clientes y que para llegar a mitigar dichas amenazas por si mismos requieren altas inversiones e implementación de procesos en la organización que pueden ser bastante prolongados.

Para cumplir con dicha propuesta de valor se tiene como objetivo principal la implementación de un SOC "Security Operation Center" el cual de acuerdo a los objetivos planteados por la compañía se implementará en tres fases:

- Fase I: Implementación de los servicios de Análisis de Vulnerabilidades, Ethical Hacking (Pentesting) y aseguramiento de la infraestructura (Hardening) para enero de 2019.
- Fase II: Implementación de un centro de Monitoreo y administración para las soluciones de seguridad de los clientes para julio de 2019.
- Fase III: Implementación del SOC para julio de 2020.

Se plantaron estas diferentes fases debido a su complejidad, ya que dicha implementación, representará a la organización una reestructuración en los procesos, en el modelo de servicio, inversiones en adecuación física e infraestructura tecnológica y la contratación y/o capacitación de ingenieros especializados y certificados en seguridad informática.

- Fase I: En esta primera fase se propone iniciar con la prestación de servicios de análisis de vulnerabilidades, consultoría en ethical hacking (pentesting) y aseguramiento de la infraestructura tecnológica en los clientes (Hardening). Estos servicios

se realizan a través de la implementación de herramientas y metodologías que en primera instancia intentan penetrar sistemáticamente los sistemas informáticos, redes, aplicaciones u otros recursos con el consentimiento del cliente y así detectar las diferentes vulnerabilidades existentes, para posteriormente si es posible o no el acceso no autorizado u otras actividades maliciosas. De acuerdo a lo revisado con el Especialista en Seguridad Julian Martinez se describen cada uno de estos servicios:

- Análisis de Vulnerabilidades: Por medio de herramientas especializadas, se realiza un análisis a los dispositivos del cliente con el fin de identificar riesgos sobre las aplicaciones y servicios que soportan estas.
- Ethical Hacking (Pentesting): Las pruebas de Ethical Hacking identifican los riesgos asociados a los servicios de la organización desde una perspectiva interna o externa al negocio con el fin de solucionar vulnerabilidades técnicas.
- Hardening: Consiste en el proceso de asegurar un sistema interno reduciendo las vulnerabilidades o huecos de seguridad, fortaleciendo el hardware y software de la empresa y eliminando los elementos innecesarios que puedan afectar el sistema. Estos servicios los prestará un ingeniero certificado CEH (Certified Ethical Hacker).

- Fase II: Para la segunda fase propone la implementación de un modelo de servicio de “Administración y monitoreo de incidentes de seguridad”. Este servicio será prestado por ingenieros y/o técnicos analistas que monitorearan de manera remota las alertas y amenazas para determinar si las mismas se pueden convertir en un incidente de seguridad o si son falsos positivos. Esto se ejecutará en un esquema de servicio de 5x8.

Tal como se propuso en la propuesta de valor, esta fase se dará inicio hacia julio del 2019 ya contando con una base de clientes a los cuales se les prestaron los servicios de consultoría en ethical hacking y análisis de vulnerabilidades.

Este servicio aplica para las soluciones tradicionales con las que cuentan hoy en día los clientes y que hoy en día PCM ofrece dentro de su portafolio actual con un esquema de implementación, soporte y visitas programadas que se agendad mensual o bimensualmente de acuerdo a lo acordado con cada cliente. Dentro de las soluciones actuales se encuentran soluciones de firewall y antivirus principalmente. De entrada, el modelo de servicio parece inviable ya que para cubrir el salario y que la compañía tenga margen del servicio, se requerirán al menos de 5 clientes de entrada que se les ofrecerá un

valor mensual muy bajo y que pueda cubrir el salario de este ingeniero para llegar al punto de equilibrio.

Lo que se plantea desde el área de ingeniería es que la prestación de este servicio inicialmente se va a soportar con los recursos que la compañía tiene actualmente para soportar sus proyectos actuales, mientras se va dando la consecución de clientes con este modelo de servicio.

En el módulo de fuentes de ingresos se ahondará más a profundidad sobre este modelo de servicio. Inicialmente se determinaron los siguientes recursos necesarios para la implementación de este modelo que son: 2 televisores de 42" pulgadas, 2 equipos de cómputo de alta capacidad con 4 monitores para los analistas que realizaran el soporte y las actividades de monitoreo. Esta infraestructura se tendrá contemplada en la estructura de costos.

- Fase III: Siendo el SOC el objetivo último para la UES se debe tener clara su definición y para qué sirve. Un SOC es una unidad orientada a proteger la confidencialidad, integridad y disponibilidad en las redes y servicios. Está dedicado exclusivamente a detectar cualquier actividad maliciosa y realiza labores orientadas al monitoreo, aseguramiento y defensa de los activos de información por medio de equipos tecnológicos y personal especializado que monitorean en tiempo real los eventos generados en la infraestructura tecnológica durante 24 horas al día y los 7 días de la semana. (SOCCOLOMBIA, s.f.)

Un SOC está compuesto por tres pilares fundamentales que son la tecnología, los procesos y las personas, donde para cada uno se debe considerar como mínimo (ver Tabla 3).

TABLA 3.
Pilares básicos para la implementación de un SOC

PERSONA	Entrenamiento formal
	Entrenamiento interno
	Experiencia laboral
	Entrenamiento con Proveedor específico
PROCESO	Procesos de gestión de incidentes:
	Identificación
	Contención
	Erradicación
	Recuperación

	Lecciones aprendidas Preparación
TECNOLOGÍA	Flujo de red Monitoreo de red Amenaza inteligente Forense Incidente detección y administración Endpoint

Para los módulos subsiguientes se tendrán en cuenta estos pilares básicos del SOC según su pertinencia dependiendo del módulo al que apliquen, aunque se resalta que el componente de viabilidad económica en su fase III, dependerá en gran medida de la implementación de las fases I y II, ya que estas determinarán la tecnología, los recursos, los servicios y las necesidades del cliente que se deberán analizar para la implementación del SOC.

6.3 INFRAESTRUCTURA

En los componentes de infraestructura del Business Model Canvas (Actividades clave, recursos clave y asociaciones clave) se propuso lo siguiente:

6.3.1 Actividades clave:

- Prestación del Servicio: La prestación del servicio es una de las actividades clave que la empresa debe ejecutar eficazmente ya que una ejecución optima del servicio garantizara la satisfacción de los clientes que tendrán en cuenta los servicios de la compañía en necesidades y requerimientos futuros. Para la prestación de los servicios de la Fase I se determinaron las siguientes 6 etapas las cuáles se definieron con el especialista en Seguridad Julian Martinez:

1. Reconocimiento: Consiste en la utilización de herramientas que permitan realizar un monitoreo, descubrimiento y recopilación de información útil de los dispositivos, servicios, activos, targets o blancos de TI a simular a ataques.
2. Escaneo: Consiste en la utilización de herramientas que permitan detectar puntos de entrada como puertos abiertos, host accesibles, localización de routers, etc. Sobre cada uno de objetivos o targets detectados en la etapa anterior. En esta etapa se realizarán: Escaneo de puertos y escaneo de red.

3. Análisis de Vulnerabilidades: Consiste en la utilización de herramientas que permitan realizar la detección de vulnerabilidades a los diferentes activos detectados en las dos etapas anteriores.

4. Presentación Plan de explotación: En esta etapa se entregará un informe detallado de las vulnerabilidades encontradas y los activos susceptibles de ataques a fin de acordar entre las partes sobre cuales realizar la explotación de dichas vulnerabilidades garantizando que no se presenten impactos sobre la plataforma de producción.

5. Explotación –Hacking Ético: Consiste en la ejecución de herramientas, técnicas y actividades necesarias que permitan explotar las vulnerabilidades encontradas y por lo tanto lograr acceso a los diferentes sistemas de información, activos de TI, bases de datos y en general a la infraestructura de la entidad según lo acordado entre las partes en la presentación del plan de explotación.

6. Documentación y Entregables: La presente propuesta contempla la entrega de los siguientes informes y reportes:

- Informe Ejecutivo: Este informe contendrá el resultado de las pruebas de manera concisa y abreviada y el cual estará compuesto por la siguiente información:

  - Descripción de los segmentos de red analizados
  - Descripción de fecha y hora de la ejecución y duración de los escaneos
  - Observaciones importantes respecto de los hallazgos que puedan poner en riesgo la seguridad de la organización y que deben corregirse de manera inmediata.
  - Gráficas de equipos intervenidos
  - Conclusiones

- Informe Técnico de Seguridad: Este informe contendrá el resultado detallado de las vulnerabilidades identificadas con los siguientes campos o columnas:

  - Elemento evaluado
  - Servicios habilitados
  - Listado de vulnerabilidades encontradas
  - Descripción de la vulnerabilidad
  - Nivel de criticidad de la vulnerabilidad
  - Evidencias y hallazgos de los accesos e intrusiones alcanzadas.

- Matriz de Remediación: Este reporte contendrá:

  - Recomendaciones técnicas

- Plan de ajustes técnicos
- Plan de ajustes operativos
- Riesgo asociado e impacto
- Recomendaciones para llevar a cabo las remediaciones
- Código CVE asociado

En la prestación del servicio es importante resaltar que a nivel interno la interacción y comunicación entre el consultor comercial y especialista debe ser constante en pro de la óptima ejecución del servicio y la misma comunicación con el cliente.

Proceso del SOC: Para la implementación del SOC es importante la parametrización de los procesos a ejecutar, ya que son relevantes para su funcionamiento y estructura. Con ellos se busca identificar, mitigar, contener y eliminar las amenazas sobre la infraestructura de la organización, dándole una mayor visibilidad y control a la superficie de seguridad.

Los procesos centrales del SOC son: **monitoreo, reporte, cumplimiento y actualizaciones** los cuales se aplican a los diferentes productos con los que los clientes pueden contar a nivel de infraestructura y seguridad. Esto se puede ver resumido en la Tabla 4:

TABLA 4.
Descripción de los procesos centrales del SOC

		ACCIÓN			
	EJEMPLO	**MONITOREO**	**REPORTE**	**CUMPLIMIENTO**	**ACTUALIZAR**
COMPONENTE	**RED**	SOC	SOC	Administrador de Red	Administrador Infraestructura
	ANTIVIRUS	SOC	SOC	SOC	Administrador Infraestructura
	FIREWALL	Administrador FW	Administrador FW	SOC	Administrador FW
	EQUIPOS	SOC	SOC	SOC	Administrador Infraestructura
	TELCO	Administrador Infraestructura	Administrador Infraestructura	Auditoría Interna	Administrador Infraestructura
	CORREO	Administrador Infraestructura	Administrador Infraestructura	SOC	SOC
	WEB	SOC	SOC	SOC	SOC

Adicional a esto, estos procesos se categorizan en diferentes niveles de alertas dependiendo de la complejidad de las amenazas (ver tabla 5):

TABLA 5.
Niveles de alertas del *SOC*

NIVELES	***DESCRIPCIÓN***
NIVEL 1	Análisis y escalamiento de amenazas
NIVEL 2	Contención y mitigación de amenazas
NIVEL 3	Búsqueda y contención de amenazas desconocidas

-

Al analizar los diferentes procesos, se puede inferir que todas estas variables determinaran en gran medida la estructura y los costos para la implementación del SOC.

6.3.2 Recursos clave: Teniendo en cuenta los tres pilares fundamentales del SOC, se destacan dos fundamentales a nivel de recursos que son las personas y la tecnología. A nivel de personas se tienen definidos 4 perfiles para la administración y monitoreo del SOC: Nivel 1: Analista de alertas. Nivel 2: Respuesta a incidentes. Nivel 3: Experto/Cazador. Administrador del SOC (ver Tabla 6).

TABLA 6.
Descripción de perfiles UES

SOC - RESPONSABILIDADES Y FORMACIÓN

Perfil	**Responsabilidades**	**Formación**
Nivel 1 Analista de alerta	• Monitorear continuamente la cola alerta • Clasificar las alertas de seguridad. • Monitorear el estado de sensores de seguridad y criterios de valoración. • Recoger los datos y el contexto necesario para iniciar el trabajo de nivel 2.	• Conocimiento y experiencia en procedimientos de triage alerta; detección de intrusos; red, información de seguridad y gestión de eventos (SIEM) y formación investigativa hostbased; y otras específicas de la herramienta. Certificaciones: • SANS SEC401: Security Essentials Bootcamp Style • CEH,CHIF
Nivel 2 Respuesta a incidentes	• Realizar análisis de incidentes de buceo profundo por correlacionar datos de diversas fuentes. • Determinar si un sistema o conjunto de datos se ha visto afectado.	• Conocimiento y experiencia en análisis forenses, forenses basadas en host. • Conocimiento y experiencia en procedimientos de respuesta a incidentes, sesión comentarios,

	• Asesorar en restauración. • Proveer soporte para nuevos métodos analíticos para la detección de amenazas.	evaluación básica malware, network forensics y amenaza de inteligencia. Certificaciones: • SANS SEC501: Advanced Security Essentials - Defensor de la empresa. • SANS SEC503: Intrusion Detection In-Depth. • SANS SEC504: Hacker Tools, Techniques, Exploits and Incident Handling. • CEH, CHIF.
Nivel 3 Experto / Cazador	• Poseer un profundo conocimiento en la red, extremo, información sobre amenazas, análisis forense y malware inversa ingeniería, así como el funcionamiento de aplicaciones específicas o subyacentes, infraestructura; actúa como un incidente "hunter" no espera incidentes escalados; estrechamente en el desarrollo, adaptación e implementación de análisis de detección de amenazas.	• Entrenamiento avanzado en detección de anomalías. • Conocimiento y experiencia en herramientas para agregación de datos y análisis de amenaza inteligentes. Certificaciones: • SEC503: Intrusion Detection In-Depth. • SANS SEC504: Hacker Tools, Techniques, Exploits and Incident Handling. • SANS SEC561: Intense Hands-on Pen Testing Skill Development. • SANS FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques. • CEH, CHIF, APT, LPT.
Administrador del SOC	• Gestionar recursos; personal, presupuesto, programación de cambio y tecnología. • Establecer las estrategias para cumplir con los SLA’s. • Comunicarse con la alta gerencia; sirve como punto de organización para incidentes críticos para el negocio. • Proporcionar la dirección general para la entrada a la estrategia de seguridad global y SOC.	• Gestión de proyectos, formación en gestión de incidentes, habilidades para la administración general de personas. Certificaciones: • CISSP, CISA, CISM y CGEIT.

▪ Tecnología: El éxito de la implementación de un SOC depende, de la recopilación de datos que realicen de los equipos de TIC de la organización, por ejemplo: EndPoint, Servidores, Switch Core, Firewall, Sanbox y NGIPS. Todos estos datos serán enviados a un SIEM (Security Information and Event Management) que permite tener una visión holística de los eventos para su análisis y procesamiento. Los servicios prestados por el SOC les permiten a los clientes tener visibilidad y gestión de los incidentes de seguridad ya que con el alto flujo de amenazas y alertas se le es casi imposible gestionar por sí mismo al área de TI interna ese gran volumen de información.

A nivel de tecnología el SOC debe contar con los siguientes recursos:

▪ SIEM (Security Information and Event Management): Es un software o sistema de gestión de eventos de seguridad, también conocido como correlacionador de eventos, capaz de detectar, responder y neutralizar las amenazas informáticas generados en los diferentes dispositivos y servidores que componen la plataforma tecnológica.

Al momento de seleccionar una solución SIEM, existe una amplia variedad de opciones con diferentes fabricantes como McAfee, IBM, Alient Vault, Symantec, Fortinet, entre otros; el reto es contar con una solución que se adapte a las necesidades de la empresa y el costo de implementación; de acuerdo a la experiencia y servicios de seguridad prestados por la Empresa con los productos de seguridad de McAfee, se incluirá la solución McAfee Security Information and Event Management para recolectar y analizar los eventos generados en los clientes e identificar las posibles amenazas almacenadas en los diferentes logs.

▪ Plataforma de antivirus: El software de protección contra malware, virus y amenazas, que trabaja en la detección de programas maliciosos que pueden perjudicar los sistemas informáticos al momento de ser ejecutados y cumplen con el objetivo de alterar, perturbar o destruir el desempeño de los equipos que hacen parte de la plataforma tecnológica incluyendo estaciones de trabajo y servidores. Las plataformas de antivirus disponibles en el mercado están compuestas por un servidor (físico, en la nube) desde donde se administra el despliegue del producto a todos los equipos de la organización con las políticas que aplicarán a cada uno de ellos a nivel global y desde donde se pueden observar todos los eventos de amenazas y la acción tomada por el producto. Entre los fabricantes que

existen a nivel mundial se encuentran KASPERSKY, ESET, NORTON, AVAST, PANDA, AVG, BITDEFENDER, TRENDMICRO, SYMANTEC, SOPHOS, MCAFEE. PCM sólo comercializaba la solución del fabricante McAfee por estrategia corporativa, pero en el año 2017 se da la alianza con el fabricante Sophos, en vista del potencial del producto y su posicionamiento en el Cuadrante de GARTNER, que permite a las empresas tener una visión de la posición que ocupan los fabricantes y en qué punto del desarrollo se encuentran en visión de mercado y poder de implementación. De acuerdo con esto, la empresa, realiza la implementación y administración de plataformas de antivirus MCAFEE y SOPHOS, lo cual puede ampliarse de acuerdo a la infraestructura implementada en el cliente, una vez que sea implementado el SOC.

- Plataforma de firewall: Una de las soluciones de seguridad ampliamente utilizada en las empresas y que incluye funciones tales como protección al perímetro y bloqueo de tráfico no autorizado, filtrado de paquetes mediante una comparación de reglas que establecen cómo se maneja la comunicación, poseen licenciamiento antivirus adicional, anti spam y módulo de VPN para el establecimiento de conexiones remotas seguras. Los servicios prestados por la empresa en este aspecto están relacionados con el dimensionamiento, implementación y administración de firewall UTM basados en direcciones IP y puertos permitidos o denegados; firewall de nueva generación, capaces de detener los ataques mediante la inspección de tráfico avanzada, la detección y control de aplicaciones; de acuerdo a los requerimientos técnicos del cliente que en mayor parte se enfocan en la protección y análisis de tráfico no autorizado, así como el filtrado de contenido mediante perfiles de navegación establecidos y al presupuesto establecido. Los fabricantes con los que se tiene la experiencia descrita anteriormente son Firewall XG Sophos y FORCEPOINT. Existen otros fabricantes en el mercado que está bien situados en el top como CISCO, PALO ALTO, FORTINET, CHECK POINT, BARRACUDA, DELL SONICWALL entre otros.

- Plataforma de gestión de incidentes: La administración de los incidentes y el manejo eficiente de las solicitudes y requerimientos de servicio que se generan a través de los diferentes procesos y servicios prestados por la empresa, se llevan a cabo, mediante el registro y seguimiento de los casos solicitados para la atención por medio de la herramienta GLPI que permite a los clientes tener la asistencia permanente, especializada y mayores niveles de servicio y soporte para brindar satisfacción del cliente. El Software GLPI cumple

con los requerimientos de la Empresa para tener el control de los requerimientos solicitados y la atención oportuna como un valor de servicio prestado a los clientes.

- Consolas de administración de infraestructura: (Wintel, AIX, Linux, Switch). Todos los sistemas deben ser administrados mediante la consola de administración que permite interactuar mediante comandos o mediante una interfaz gráfica, cada uno de los fabricantes ofrece estas herramientas para que el administrador cuente con las herramientas necesarias de configuración y administración en los sistemas de red.

- Escáner de vulnerabilidades: Las herramientas de software para realizar el escaneo y detección de vulnerabilidades, constituyen a principal herramienta para el Ethical Hacking, quien con sus conocimientos y capacidades puede llevar a cabo un procedimiento de detección de vulnerabilidades de manera eficiente. La elección de la herramienta adecuada dependerá de las exigencias de la prueba de penetración que se debe realizar y del conocimiento y experticia del profesional que va a realizar el escaneo de vulnerabilidades. La amplia variedad de herramientas que existe, involucran algunas gratuitas con funciones limitadas y otras licenciadas. Entre las más utilizadas se encuentran Nessus, Nexpose, OpenVas, Retina, Microsoft Baseline Security Analyzer (MBSA), entre otras.

- Plataforma de NGIPS: Es un sistema de prevención de intrusiones de próxima generación que descubre y bloquea amenazas sofisticadas de red, empleando técnicas avanzadas de detección y emulación para ofrecer protección contra ataques que tengan alto grado de precisión. El NGIPS de McAfee está calificado en el cuadrante de Gartner como líder para sistemas de detección y prevención de intrusiones, la solución integrada de McAfee simplifica las operaciones de seguridad mediante la combinación con McAfee Global Threat Intelligence para responder de manera rápida y precisa a los ataques que se propagan en la red. Existen otros fabricantes como Cisco pero todo depende de los requerimientos técnicos. (McAfee, 2018)

6.3.3 Asociaciones clave: A nivel de asociaciones clave se debe tener una estrecha relación con los fabricantes líderes en seguridad TI. PCM actualmente tiene relación con los siguientes fabricantes de seguridad: MCAFEE, SOPHOS, FORCEPOINT, KOD LATAM SECURITY. Todos los fabricantes nunca llegan de manera directa a los clientes exceptuando algunos proyectos de grandes dimensiones con cuentas estratégicas. Todos los fabricantes para llegar al mercado manejan un esquema de canales o Partners los cuales se categorizan en varias categorías definidas por volúmenes de ventas y personal

certificado en las diferentes soluciones. A continuación, se nombrará la categoría de Partner en la que se encuentra la empresa y la relación que se ha tenido con cada uno:

- MCAFEE: Con este fabricante la empresa inició la venta de soluciones de seguridad en el año 2002 específicamente con soluciones de antivirus para las estaciones de trabajo de sus clientes. Posteriormente incursiona con la venta y comercialización de soluciones más avanzadas como lo son Firewall, IPS (*Intrusion prevention System*), Web Gateway, Email Gateway, ATD (*Advanced Threat Defense*), SIEM (*Security Information and Event Management*), TIE (*Threat Inteligence Exchange*) y DLP (*Data Loss Prevention*). Este fabricante cuenta con las siguientes categorías de Partner empezando desde la más alta que es PLATINUM, GOLD, SILVER y RGISTER. Actualmente PCM se encuentra en la categoría de Partner Gold, aunque años atrás se encontraba en la categoría PLATINUM (Categoría más alta de Partner) por registrar excelentes números en ventas. Para estar en esta categoría de Partner se debe cumplir con una cuota de ventas por un millón de dólares establecida por esta fabricante para todos sus canales y que se debe cumplir año a año para mantener la categoría.

- SOPHOS: La relación con este fabricante inició en el año 2017 a la entrada de este en el mercado latinoamericano. Este fabricante nombra a 4 canales Platinum, dentro de los cuales nombraron a PCM viendo el potencial en el sector gubernamental. Esto le permite a la compañía contar con excelentes descuentos y precios bastante competitivos frente a otras marcas ya que es objetivo de la marca entrar rápidamente al mercado. Las soluciones que se comercializan de este fabricante son las de antivirus y firewall las cuales están posicionadas en el cuadrante mágico de Gartner.

- FORCEPOINT: Esta relación se generó básicamente porque el fabricante McAfee con el que PCM lleva una relación de varios años, vendió su solución de Firewall a otro fabricante llamado WEBSENSE que posteriormente es adquirida por FORCEPOINT. La alianza está enfocada a realizar las renovaciones de los Firewall MCAFEE con la que cuentan varios clientes. La categoría de Partner actual es la de silver Partner.

- KOD LATAM SECURITY: Este es un fabricante uruguayo de seguridad con el cual se inició relaciones en 2016 gracias a la cámara de comercio de Bogotá, referencio a PCM como un posible aliado en Colombia ya que ellos se encontraban buscando aliados en

Latinoamérica, siendo PCM el Partner exclusivo para Colombia. Este es un aliado importante para la compañía ya que ofrece un amplio y extenso portafolio de servicios y consultoría en ciberseguridad y además cuentan con una solución única de protección y seguridad en ambientes virtuales que ningún otro fabricante maneja.

Adicional a estos fabricantes con los que tiene relación la empresa existen un gran número de fabricantes de soluciones de seguridad y que son competencia directa en algunos productos de los fabricantes con los que tiene relación PCM. Algunos de estos son FORTINET, CHECKPOINT, PALO ALTO, HP, CISCO, KASPERSKY, SYMANTEC, TRENDMICRO, entre otros.

Estas asociaciones son clave ya que trabajar de la mano con los fabricantes permite mantener una actualización constante de las tecnologías con las que cuentan los clientes hoy en día. Adicional a esto se permite trabajar con el personal de TI el plan de formación y certificación requerido para la prestación de los servicios de un SOC.

6.4 VIABILIDAD ECONÓMICA

En el componente de viabilidad económica del Business Model Canvas (estructura de costos y estructura de ingresos) de acuerdo a lo propuesto en los diferentes módulos del Business Model Canvas se desagregaron tanto la estructura de costos como la estructura de ingresos para posteriormente proponer una viabilidad económica del modelo:

6.4.1 Estructura de Costos: Para la estructura de costos de la UES se analizaron las dos primeras fases dado que para la implementación del SOC que es la tercera fase la empresa aún se encuentra en proceso de dimensionamiento y no se tienen muy claros a nivel de costos de implementación.

Para la primera Fase I de la UES el grueso de la Inversión está concentrado en el salario y prestaciones sociales del ingeniero especialista que actualmente está $ 5.500.000 pesos más sus prestaciones de ley. Aunque este costo no va al 100% a la UES, ya que el actualmente el 50% está atado a un proyecto de otra línea de negocio que es la administración de soluciones Microsoft. Los demás costos van a atados a costos de ventas que también son compartidos con las demás líneas de negocio. Entre estos se destacan la fuerza de ventas, la empresa de tele mercadeo, el analista de marketing, la inversión en

página web y publicidad online. A continuación, se presentan los diferentes costos contemplados para esta primera fase en la siguiente taba (ver tabla 7)

TABLA 7.
Costos Fase I – UES (Mes uno)

Valor	PERIODICIDAD	ITEM
$ 3.987.500	Mensual	Salario Ing. CEH
$ 3.100.000	Mensual	Empresa Telemecadeo
$ 2.610.000	Mensual	Salarios y prestaciones Fuerza de Ventas
8%	Variable	Comisiones por Ventas (Facturación)
$ 600.000	Mensual	Google Adwords
$ 2.500.000	Único	Diseño y optimización SEO Sitio Web
15%	Variable	Costos operativos (Ventas)
$ 12.797.500		**Total**

Para la segunda fase que es la implementación de un servicio de monitoreo se requiere hacer la inversión de 2 televisores, 2 equipos portátil, licencia de acceso remoto y la promoción y/o contratación de un especialista adicional para apoyar los servicios de ethical hacking y para los servicios monitoreo.

TABLA 8.
Costos Fase II – UES (Mes siete)

Valor	CANTIDAD	ITEM
$ 1.10000	2	Televisor 40”
$ 450.000	2	Monitor 24”
$ 2.500.000	2	Portátil
$ 1.200.000	1	Software de Acceso remoto
$ 3.987.500	1	Salario Ingeniero CEH (50%)
$ 4.350.000	1	Salario Ingeniero II

$ 12.597.000	**Total**

Cabe resaltar que para la implementación del modelo de servicio de monitoreo y administración se arrancara con personal que ya se encuentra en la compañía, los cuales están costeados con los otros proyectos de la compañía. A pesar de que esta fase se va a implementar en el mes de julio de 2019, desde la fase I se empezará con la promoción de este servicio con el fin de ir generando demanda para estos servicios.

6.4.2 Estructura de Ingresos: Para la fase que son los servicios de consultoría se tienen definidos las siguientes tarifas base (ver Tablas 9,10,11,12 y 13):

TABLA 9.
Lista de Precios Análisis de Vulnerabilidades Servicios UES

Tipo de Activo	Cantidad	Valor C/U	Max. Valor
IP	1 – 4	$ 600.000	$ 2.400.000
	5 – 9	$ 550.000	$ 4.950.000
	10 – 14	$ 500.000	$ 7.000.000
	15 – 19	$ 450.000	$ 8.550.000
WEB	1 – 4	$ 700.000	$ 2.800.000
	5 – 9	$ 650.000	$ 5.850.000
	10 – 14	$ 550.000	$ 7.700.000
	15 – 19	$ 500.000	$ 9.500.000
WEB APP	1	$ 1.300.000	$ 1.300.000
	2	$ 1.200.000	$ 2.400.000
	3	$ 1.100.000	$ 3.300.000
	4	$ 1.000.000	$ 4.000.000

TABLA 10.
Lista de Precios Pentesting Servicios UES

Tipo	Cantidad	Valor C/U	Max. Valor
CAJA BLANCA	1 – 4	$ 900.000	$ 3.600.000
	5 – 9	$ 800.000	$ 7.200.000
	10 – 14	$ 750.000	$ 10.500.000
	15 – 19	$ 700.000	$ 13.300.000
CAJA GRIS	1 – 4	$ 1.100.000	$ 4.400.000
	5 – 9	$ 1.000.000	$ 9.000.000
	10 – 14	$ 900.000	$ 12.600.000
	15 – 19	$ 850.000	$16.150.000

NEGRA	NA	$ 9.000.000	NA

TABLA 11.
Lista de Precios Análisis de Vulnerabilidades WIFI Servicios UES

Tipo de Activo	Cantidad	Valor C/U	Max. Valor
SSID	1 - 4	$ 500.000	$ 2.000.000
	5 - 9	$ 450.000	$ 4.050.000
	10 - 14	$ 400.000	$ 5.600.000
	15 - 19	$ 350.000	$ 6.650.000

TABLA 12.
Lista de Precios Hardening de Arquitectura Servicios UES

Tipo de Activo	Cantidad	Valor C/U	Max. Valor
Segmento de Red	1 - 4	$ 500.000	$ 2.000.000
	5 - 9	$ 450.000	$ 4.050.000
	10 - 14	$ 400.000	$ 5.600.000
	15 - 19	$ 350.000	$ 6.650.000

TABLA 13.
Lista de Precios Servicio de Administración y Monitoreo de Incidentes de Seguridad UES

Tipo de Activo	Cantidad de nodos	Valor Mensual
Solución Endpoint	1 – 500	$ 500.000
	501 – 1000	$ 750.000
	1001 – 1500	$ 1.000.000
	1501 – 2000	$ 1.200.000
	2001 - 5000	$ 1.600.000
	5001 – 10000	$ 1.900.000
	+10.001	$ 2.500.000

Estas diferentes tablas de precios se elaboraron con base en la cantidad de horas que le demandan al especialista realizar la labor y se calculó un estimado de costo hora ingeniero, en base su salario y el salario ofertado por el mercado teniendo en cuenta todas las prestaciones de ley.

Para la tabla 13 que es para los servicios de la Fase II de Monitoreo y administración de las soluciones se proyectó que un especialista puede atender alrededor de 20.000 nodos distribuidos en aproximadamente 5 clientes.

El esquema de venta para esta segunda fase, consistirá en el cobro de un valor mensual que se calculará en base a la cantidad de nodos o estaciones de trabajo de los

clientes. Este esquema beneficiará mucho a los clientes ya que le quitará labores de administración de las soluciones y se pueden concentrar en actividades más estratégicas para la operación del negocio. Adicional a esto reduce la contratación de un perfil de alto nivel que requiere constante capacitación y genera un alto costo para la compañía que en el momento en que ese recurso decida irse de la compañía se entraría en un desgaste de tiempo en la consecución que igual requerirá una curva de aprendizaje de largo aliento.

6.4.3 Viabilidad del modelo:

Antes de presentar los datos hay que recalcar que muchos de los costos de las actividades clave se comparten con las demás líneas de negocio de la compañía y que no se deben tomar en un 100% para la UES. Adicionalmente se puede observar que en principio los márgenes de rentabilidad no son representativos, las consolidaciones de los servicios prestados por la UES apalancaran más oportunidades de negocio en las demás líneas de negocio de la compañía

A continuación, se presenta el modelo económico para la Fase I: (Ver Tabla 14)

Tabla 14

Modelo de viabilidad economica Fase I

FLUJO DE CAJA PROYECTADO								
EMPRESA			UES - PCM FASE I					
Período:			AÑO 2019					
			1	2	3	4	5	6
1.	Saldo Inicial de Caja			-9.535.000	$ (7.318.250,00)	$ (3.713.575,00)	$ 280.551,25	$ 6.379.721,44
2,0	INGRESOS DE EFECTIVO							
2,1		Analisis de Vulnerabilidades	$ 4.500.000,00	$ 5.175.000,00	$ 5.692.500,00	$ 6.546.375,00	$ 7.528.331,25	$ 8.657.580,94
2,2		Pentesting		$ 7.000.000,00	$ 7.700.000,00	$ 9.240.000,00	$ 10.164.000,00	$ 11.180.400,00
2,3		Hardening		$ 3.000.000,00	$ 3.450.000,00	$ 3.967.500,00	$ 4.562.625,00	$ 5.247.018,75
3,4		Otros ingresos		$ -	$ -	$ -	$ -	$ -
	Total ingresos		4.500.000	15.175.000	$ 16.842.500,00	$ 19.753.875,00	$ 22.254.956,25	$ 25.084.999,69
3,0	EGRESOS OPERATIVOS							
3,1		Herramienta de Monitoreo	$ -	$ -	$ -	$ -	$ -	$ -
3,2		Salario Ingeniero CEH	$ 3.987.500,00	$ 3.987.500,00	$ 3.987.500,00	$ 3.987.500,00	$ 3.987.500,00	$ 3.987.500,00
3,2		Salario Ingeniero 2				$ 5.075.000,00	$ 5.075.000,00	$ 5.075.000,00
3,3		Empresa de Telemercadeo	$ 3.100.000,00	$ 3.100.000,00	$ 3.100.000,00			
3,4		Google Adwords	$ 600.000,00	$ 600.000,00	$ 600.000,00	$ 600.000,00	$ 600.000,00	$ 600.000,00
3,5		Diseño y optimizacion SEO Sitio Web	$ 2.500.000,00	$ -	$ -	$ -	$ -	$ -
		Salarios y prestaciones Fuerza de Ventas	$ 2.610.000,00	$ 2.610.000,00	$ 2.610.000,00	$ 2.610.000,00	$ 2.610.000,00	$ 2.610.000,00
3,6		Comisiones x vtas	$ 360.000,00	$ 1.214.000,00	$ 1.347.400,00	$ 1.580.310,00	$ 1.780.396,50	$ 2.006.799,98
3,7		RETEFUENTES	$ 157.500,00	$ 245.000,00	$ 269.500,00	$ 323.400,00	$ 355.740,00	$ 391.314,00
3,8		COSTOS OPERATIVOS (15%)	$ 675.000,00	$ 1.050.000,00	$ 1.155.000,00	$ 1.386.000,00	$ 1.524.600,00	$ 1.677.060,00
3,9		Pago de Impuestos ICA	$ 45.000,00	$ 151.750,00	$ 168.425,00	$ 197.538,75	$ 222.549,56	$ 250.850,00
3,10			$ -	$ -	$ -	$ -	$ -	$ -
	Total Egresos		14.035.000	12.958.250	$ 13.237.825,00	$ 15.759.748,75	$ 16.155.786,06	$ 16.598.523,97
4.	FLUJO NETO OPERATIVO (2-3)		-9.535.000	2.216.750	$ 3.604.675,00	$ 3.994.126,25	$ 6.099.170,19	$ 8.486.475,72

Para la fase II ya contando con unas ventas consolidadas en los servicios de Ethical Hacking se propone una proyección de ventas para los servicios de monitoreo y administración de soluciones para incidentes de seguridad. Este modelo es bastante interesante ya que a medida que se va creciendo en clientes los márgenes de rentabilidad son mayores ya que con la misma infraestructura que se cuenta se pueden atender un número mayor de clientes aumentando notablemente la facturación.

El punto de equilibrio se daría también a partir del 4 mes ya que en la fase II se incluyen tanto los costos de esta fase como de la fase I.

A continuación, se presenta el modelo económico para la Fase II: (Ver Tabla 15)

Tabla 15

Modelo de viabilidad economica Fase II

FLUJO DE CAJA PROYECTADO												
EMPRESA			UES - PCM FASE II									
		Período:	2019									
			7		8		9		10		11	12
1.	Saldo Inicial de Caja		$ -	$	(5.036.067)	$	2.354.453	$	12.594.333	$	26.127.841	$ 43.477.807
2,1		Servicio de Monitoreo	$ 2.500.000	$	3.500.000	$	4.375.000	$	5.468.750	$	6.835.938	$ 8.544.922
2,2		Analisis de Vulnerabilidades	$ 9.826.660	$	11.300.659	$	12.995.758	$	14.945.122	$	17.186.890	$ 19.764.924
2,3		Pentesting	$ 11.180.400	$	12.298.440	$	13.528.284	$	14.881.112	$	16.369.224	$ 18.006.146
3,4		Hardening	$ 2.700.922	$	2.727.931	$	2.755.210	$	2.782.763	$	2.810.590	$ 2.838.696
	Total ingresos		$ 23.507.060	$	29.827.030	$	33.654.252	$	38.077.747	$	43.202.641	$ 49.154.687
3,0	EGRESOS OPERATIVOS											
3,1		Equipos portatil	$ 5.000.000	$	-	$	-	$	-	$	-	$ -
3,2		Especialista de Seguridad I	$ 3.987.500	$	3.987.500	$	3.987.500	$	3.987.500	$	3.987.500	$ 3.987.500
3,2		Especialista de Seguridad II	$ 4.350.000	$	5.075.000	$	5.075.000	$	5.075.000	$	5.075.000	$ 5.075.000
3,3		Televisores	$ 2.200.000	$	-	$	-	$	-	$	-	$ -
3,4		Google Adwords	$ 600.000	$	600.000	$	600.000	$	600.000	$	600.000	$ 600.000
3,5		Licencia Acceso remoto	$ 1.200.000									
3,6		Salarios y prestaciones Fuerza de Ventas Comercial N°1	$ 2.610.000	$	2.610.000	$	2.610.000	$	2.610.000	$	2.610.000	$ 2.610.000
3,7		Salarios y prestaciones Fuerza de Ventas Comercial N°2	$ 2.610.000	$	2.610.000	$	2.610.000	$	2.610.000	$	2.610.000	$ 2.610.000
3,8		Comisiones x vtas	$ 1.880.565	$	2.386.162	$	2.692.340	$	3.046.220	$	3.456.211	$ 3.932.375
3,9		RETEFUENTES	$ 343.933	$	395.523	$	454.852	$	523.079	$	601.541	$ 691.772
3,10		COSTOS OPERATIVOS (15%)	$ 3.526.059	$	4.474.055	$	5.048.138	$	5.711.662	$	6.480.396	$ 7.373.203
3,11		Pago de Impuestos ICA	$ 235.071	$	298.270	$	336.543	$	380.777	$	432.026	$ 491.547
	Total Egresos		$ 28.543.128	$	22.436.510	$	23.414.372	$	24.544.238	$	25.852.675	$ 27.371.397
4.	FLUJO NETO OPERATIVO (2-3)		$ (5.036.067)	$	7.390.520	$	10.239.880	$	13.533.508	$	17.349.966	$ 21.783.290

Inicialmente en este modelo no se tiene contemplado la contratación de un especialista para atender el modelo, se trabajará con los recursos actuales de la compañía de los proyectos en que se tiene un esquema de visita mensual. Esto mientras se va madurando el modelo de servicios que ya con una base mínima de clientes se pueda contratar el recurso para dicha labor especifica.

Este modelo tiene un beneficio de ahorro en costos de desplazamiento del ingeniero y de tiempos de respuesta mucho más rápidos generando un valor agregado tanto para la empresa como para los clientes.

7. Conclusiones

El desarrollo de la Unidad Estratégica de Seguridad - UES representa para PCM una gran oportunidad de crecimiento y consolidación en el mercado de soluciones de TI y Ciberseguridad. De acuerdo a lo presentado en los resultados se presentan las siguientes conclusiones con base en las 4 áreas principales de un negocio y como se presentó en el presente diseño del Business Model Canvas para la UES.

Desde el componente de clientes recalcamos sobre el gran potencial del mercado ya que hoy en día el aseguramiento de la información es un elemento que impacta a todas las organizaciones sin importar su tamaño. Es imprescindible para la UES desarrollar y mantener cada uno de los canales de comunicación propuestos para gestionar y mantener las relaciones con los clientes. En dichas relaciones se deben generar los procesos de comunicación entre las diferentes áreas, especialmente entre las de comercial e ingeniería que son las que más interactúan con los clientes y que deben garantizar altos niveles de satisfacción en los clientes.

La propuesta de valor sin duda es el componente primordial para el éxito de la UES. Su éxito dependerá en la gestión adecuada de cada una de las etapas de relación con los clientes que van desde la detección y entendimiento de las necesidades hasta la prestación, entrega y cierre de los proyectos de la UES. En todo momento el cliente debe percibir la experiencia, el servicio y el acompañamiento de una organización comprometida con sus necesidades. A nivel de seguridad informática son pocas las empresas que implementan estos servicios de manera preventiva, generalmente demandan estos servicios de manera reactiva cuando ya han tenido algún incidente o falla de seguridad. Por esta razón

la organización debe estar preparada para responder de manera rápida y ágil a las necesidades demandadas por los clientes.

Para el cumplimiento de dicha propuesta de valor es necesario para la UES contar con una infraestructura óptima que apoye y apalanque su cumplimiento. Desde el componente de infraestructura se hace énfasis en los recursos humanos y tecnológicos. El personal designado para la UES deberá estar constante aprendizaje ya que día a día se generan miles de amenazas desconocidas y se deberá trabajar de manera de manera conjunta con los diferentes fabricantes que son los socios clave y que tienen mayor visibilidad de las diferentes amenazas a nivel mundial.

Tal como se planteó en la propuesta de valor, es necesario definir la tecnología requerida para la implementación del SOC que estará determinada por la implementación de las fases I y II e igualmente por las necesidades de los clientes que requerirán la administración y el monitoreo de sus soluciones propias o de soluciones que incluyen hardware & software como servicio. Adicional a esto la implementación del SOC requerirá la definición del esquema de servicio que puede ser 5x8 o 7x24 lo cual impactará considerablemente en los costos y en el mismo modelo de servicio.

Desde el punto de vista metodológico cabe resaltar la técnica de las 6 propuestas por los autores para el diseño del Business Model Canvas. Con la técnica de Ideación, lo que más resalta fue la participación de un grupo interdisciplinario lo cual fue clave para la discusión y el desarrollo del brainstorming de cada uno de los módulos. Cada uno desde su experiencia y conocimiento aportaron tanto en nuevas ideas como en complementar las ideas de los demás integrantes. También se resalta que con esta técnica se pudieron desarrollar las 3 de las 5 fases del proceso de diseño del Business Model Canvas ya que las fases de aplicación y gestión dependerán de la organización si desea aplicar el diseño propuesto.

8. Recomendaciones para la organización

En primera instancia cabe resaltar la gran oportunidad de crecimiento de la UES en la prestación de servicios de ciberseguridad, teniendo presente el alto riesgo al que se encuentran expuestas las organizaciones por la perdida y/o robo de información y adicionalmente por el bajo conocimiento y experiencia de las empresas en las áreas de

seguridad informática, al requerir implementar procesos y controles más estrictos que requieren un proceso de maduración de largo aliento que sin la ayuda de un tercero con experiencia lograrían llevar a cabo.

Igualmente, las organizaciones se están viendo obligadas a cumplir con diferentes normativas que garanticen la seguridad de los datos de sus clientes, lo que permite a empresas de ciberseguridad como PCM ofrecer un portafolio amplio de servicios en ciberseguridad. Por esta razón PCM debe generar constantes comunicaciones con sus clientes recalcando la importancia de asegurar la información y contar con respaldos de esa información en caso de algún ataque o incidente de seguridad.

Con la implementación adecuada de la UES la empresa podrá llegar a posicionarse como un socio estratégico de las empresas para el manejo de la ciberseguridad siendo este un pilar fundamental en el desarrollo de los negocios y adicionalmente contribuirá y potencializará la generación de más proyectos de TI en las demás líneas de negocio que hoy en día PCM sigue comercializando.

Se propone la organización definir la viabilidad económica del modelo en la fase III en el mes 4 de la fase II con el fin de determinar ya puntualmente los recursos necesarios para la implementación y montaje del SOC.

9. Referencias

ARANDA-SOFTWARE. (s.f.). *Aranda Software*. Obtenido de www.arandasoft.com

CONSEJO DE ESTADOS DE EUROPA. (23 de 11 de 2001). *ORGANIZACION DE ESTADOS AMERICANOS.* Obtenido de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

EAE BUSINESS SCHOOL. (2015). Obtenido de https://retos-directivos.eae.es/quien-es-alexander-osterwalder/

MAILCHIMP. (s.f.). *MAILCHIMP*. Obtenido de www.mailchimp.com

McAfee. (5 de 11 de 2018). *McAfee*. Obtenido de https://www.mcafee.com/enterprise/es-es/products/network-security-platform.html

Mintic. (2017). *Ministerio de las telecomunicaciones*. Obtenido de www.mintic.gov.co

Mintzberg. (1978) *Patterns in strategy formulation*. Management science. California. Informs.

Pigneur, Osterwalder. (2010). *Generacion de modelos de Negocio.* Deusto, Grupo Planeta.

Policial, C. C. (2016 – 2017). *Amenazas del Cibercrimen en Colombia.* Bogotá.

SOCCOLOMBIA. (s.f.). Obtenido de www.soccolombia.com/documentos/documento1.pdf

SYMANTEC. (2017). *ISTR internet security threat report.*

Vicedo, B. O. (2015). *10 PASOS PARA DESARROLLAR UN PLAN ESTRATÉGICO Y UN BUSINESS MODEL CANVAS.* Obtenido de 3C empresa: https://doi.org/10.17993/3cemp.2015.040424.231-247

FICHA BIBLIOGRÁFICA DE DOCUMENTO DE OPCIÓN DE GRADO

TITULO COMPLETO			
DISEÑO DEL BUSINESS MODEL CANVAS PARA LA NUEVA LINEA DE NEGOCIO "UES -UNIDAD ESTRATEGICA DE SEGURIDAD" DE PCM S.A.S			
AUTORES			
Apellidos completos		**Nombres completos**	
SANTAMARIA MARTINEZ		**CAMILO**	
TUTOR DE TRABAJO DE GRADO			
Apellidos completos		**Nombres completos**	
OCHOA URREGO		**RAFAEL LEONARDO**	
PROGRAMA ACADÉMICO			
Nombre del programa		**Tipo de programa (marque con una x)**	
ALTA GERENCIA		**Pregrado**	
		Especialización	**X**
		Maestría	
CIUDAD	**AÑO DE PRESENTACIÓN DEL TRABAJO DE GRADO**	**NÚMERO DE PÁGINAS**	
BOGOTA	**2019**	**54**	
PALABRAS CLAVES			
Español		**Inglés**	

RESUMEN
(Máximo 250 palabras)

El panorama de un crecimiento exponencial de amenazas informáticas representa una oportunidad única de prestar servicios en Ciberseguridad, representado en un gran potencial del mercado. Por esta razón PCM tiene como objetivo desarrollar una nueva línea de negocio denominada "UES – Unidad Estratégica de seguridad". Para la implementación de esta nueva línea se propone el diseño a través del Businness Medel Canvas que es una herramienta que permite desarrollar un modelo de negocio. Este Business Model Canvas comprende la estructuración de 9 Módulos distribuidos en las 4 áreas principelas de un negocio que son: Clientes. Propuesta de valor, Infraestructura y viabilidad económica. Para cada uno de los 9 módulos se propondrán los elementos mas relevantes para la implementación de la nueva línea de negocio los cuales permitirán a la organización ver de manera fácil y practica como desarrollar el modelo para la nueva línea de negocio,

LICENCIA DE USO A FAVOR DE LA FUNDACIÓN UNIVERSITARIA EMPRESARIAL DE LA CÁMARA DE COMERCIO DE BOGOTÁ – UNIEMPRESARIAL, POR PARTE DE ESTUDIANTES.

El suscrito

Camilo Santamaria Martinez con C.C. N° 1.020.721.501, actuando en calidad de autor de el trabajo de grado) que lleva por título _DISEÑO DEL BUSINESS MODEL CANVAS PARA LA NUEVA LINEA DE NEGOCIO "UES -UNIDAD ESTRATEGICA DE SEGURIDAD" DE PCM S.A.S elaborada para efectos de optar por el título, de ESPECIALISTA EN ALTA GERENCIA.

Hago entrega a UNIEMPRESARIAL de una copia de dicho trabajo académico en formato digital o electrónico (CD-ROM, etc.) otorgando licencia o autorización de uso sobre la misma, para que en los términos de la Decisión Andina 351, la Ley 23 de 1982 y demás normas aplicables, realice los actos de explotación de los derechos patrimoniales y de manera especial, para que la divulgue, reproduzca, comunique al público y la ofrezca en préstamo al público. La presente licencia o autorización se extiende no solo a la fijación en medio o formato físico, analógico o material, sino también al medio virtual, electrónico, óptico, usos de red, Internet, extranet, intranet, repositorio institucional y demás formatos conocidos o por conocer.

El autor de la obra, manifiesta de igual manera que la obra objeto de esta licencia o autorización de uso es creación original y que se realizó sin infringir los derechos de autor que le correspondan a terceros.

PARÁGRAFO: Si llegase a presentarse cualquier tipo de reclamación o acción por parte de un tercero en cuanto a los derechos de autor sobre la obra en mención, asumiré la responsabilidad, dejando indemne a UNIEMPRESARIAL y saliendo en defensa de los derechos aquí autorizados.

Para constancia se firma el presente documento en Bogotá, el año 2019 del mes marzo a los 21días.

FIRMA

Firma  **C.C. 1.020.721.501**

CON SEGURIDAD SU MEJOR SERVICIO DE TI
PCM S.A.S

Calle 41 N° 26B – 26
PBX 3690480
NIT 860.403.052-3
Bogotá D.C. Colombia

Bogotá marzo 21 de 2018

Señores
UNIEMPRESARIAL
Ciudad.

Referencia: Conocimiento de consultoría y uso de marca con fines académicos

Cordial saludo,

Con la presente manifestamos tener conocimiento sobre la consultoría empresarial realizada en nuestra organización por CAMILO SANTAMARIA con CC. 1.020.721.501 y cuyos resultados serán de gran aporte para nuestra empresa. Por lo anterior autorizamos el uso de nombre de nuestra compañía para ser usado con fines académicos.

Cordialmente,

JAIME ALBERTO SANTAMARIA
CC: 80.092.963
CARGO: REPRESENTANTE LEGAL SUPLENTE
PCM SAS