Plan de Negocio para evaluar la viabilidad de implementar el primer CERT financiero para el sistema financiero peruano

Tesis presentada en satisfacción parcial de los requerimientos

para obtener el grado de Maestro en Marketing

por:

Quintana Tineo, Emisanti

Programa de la Maestría en Marketing

Lima, 03 de Abril del 2019

Esta tesis:

Plan de Negocio para evaluar la viabilidad de implementar el primer CERT financiero para el sistema financiero peruano.

Ha sido aprobada.

_____

José Luis Wakabayashi Muroya (Jurado)

_____

Estuardo Lu Chang-Say (Jurado)

_____

Cesar Neves Catter (Asesor)

Universidad ESAN

2019

Para todos aquellos que buscan que las cosas sucedan.

Para los que esuchan a su corazón y que no se rinden nunca ante la adversidad.

Para mi madre querida que me hizo el hombre que soy y que siempre me ha acompañado en los momentos más importantes de mi vida.

INDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

EMISANTI QUINTANA

Ejecutivo senior con más de 10 años de experiencia en la reestructuración y creación de productos de acuerdo con las necesidades de mercado. Orientado a la innovación, alto nivel de responsabilidad y compromiso. Ingeniero de Telecomunicaciones, MBA, Msc Marketing Science, con conocimientos en administración de negocios y aplicación de Design Thinking, Systematic Inventive Thinking.

EXPERIENCIA PROFESIONAL

ASOCIACIÓN DE BANCOS DEL PERÚ

Entidad gremial con más de 50 años, que agrupa a los bancos e instituciones financieras privadas del país. Promueve el fortalecimiento del sistema financiero, proporcionando a sus asociados servicios de información, tecnológicos, legales y seguridad electrónica. Cuentan con 130 trabajadores y US$12MM anuales de facturación.

Jefe de Innovación
Oct.2018 – A la fecha
Responsable de identificar oportunidades de eficiencia en la banca desarrollando y articulando proyectos y productos de innovación sobre un profundo conocimiento del negocio.

- Creación del producto FTR Cloud, logrando comercializarlo a 15 clientes en menos de un año y obteniendo ingresos de US$330K, lo que representa un cumplimiento del 25% de la cuota del año.
- Desarrollo de una solución para la recaudación de pagos en tiempo real, entre España y Perú para el cliente REPSOL, generando un ingreso de US$300K, por ventas del producto.

Jefe de Producto
May.2016 - Oct.2018
Responsable de analizar el mercado, sus necesidades y compararlas con el portafolio de ASBANC, con el fin de crear y mantener productos actualizados y atractivos para el cliente.

- Diseño e implementación del proyecto de Business Intelligence para el sistema financiero peruano que permite consolidar la información financiera bancaria a través de la gestión estratégica de la información, logrando un ingreso de US$200K al año en venta del proyecto.
- Creación y lanzamiento del producto Servefact, siendo la proyección estimada de ingresos de US$3MM, cumpliéndose en 7 meses US$420K de ingreso, logrando un cumplimiento de ventas del 14% de lo proyectado. DIcho servicio permite la transformación y validación de los comprobantes de pago electrónicos con SUNAT.
- Responsable de la creación y lanzamiento del producto CySecure, el cual permite proteger a las entidades financieras de los fraudes cibernéticos, siendo la proyección estimada de venta de US$7MM de dólares anuales, cumpliéndose en un año US$500K de ingreso correspondiente al 7% de lo proyectado.

- Resposable de la reformulación del servicio Analytical Fraud Services, el cual genera un ingreso de US$250K anuales, dicho servicio especializado en el análisis del comportamiento de las diversas modalidades de fraude.

Especialista de Tecnología de Información
Abr.2015 - May.2016
Apoyo en la definición a la gerencia general, en la evaluación e implementación de proyectos que se soporten en el uso de las tecnologías de información, participando en mesas interdisciplinarias para generar productos de interés común a la banca.

- Responsable de la certificación internacional SWIFT para el servicio de pagos, obteniendo una reducción de gastos operativos de 40% a través de un servicio de outsourcing con partners que permitan lograr dichas eficiencias.
- Lider del proyecto de la factura negociable, el mismo que logró modificar el DL 1178 permitiendoles a las pequeñas y medianas empresas utilizar una ICLV con el fin de poder hacer uno de de un fondo gubernamental por US$500K para su financiamiento.

Analista Senior de Tecnologia de Información
May.2010 - Abr.2015
Responsable de analizar la madurez y la efectividad de las tecnologías clave, la infraestructura, los sistemas y los procesos para garantizar que se implementen controles internos y abordar riesgos clave dentro de los activos críticos de la empresa.

- Migración de la plataforma ATM a MPLS de la infraestructura de la red de bancos (BANCARED) optimizandose los costos de operación en un 20% en el año 2013 versus el año 2012.
- Administración y soporte de la infraestructura de mensajería internacional SWIFT, logrando que la disponibilidad del servicio sea de 99.98%.
- Reduccion en 30% en costos de operación gracias a la migración del sistema de compensaciones de alto valor del BCRP incrementando la disponibilidad y seguridad del servicio.

FORMACION ACADEMICA
- ESAN, Maestría en Administracion de Empresas (MBA) 2013-2014
- Pontificia Universidad Católica, Ingenieria de Telecomunicaciones 1999-2007

OTROS ESTUDIOS
- UTEC, Certificación Internacional de Innovación Avanzada – SIT 2017-2018
- University of Virginia, Specialization in Design Thinking and Innovation 2017
- Peking University, Chinese Business and Economics Development 2014
- UPC, Diplomado en Business Intelligence 2011
- Laureate International University, Diplomado en Educacion Superior 2011-2012

DATOS DE INTERES
Manejo de MS Office, SPSS, Windows Server, Linux
Idiomas: Inglés (intermedio), Francés (básico)

RESUMEN EJECUTIVO

La adhesión del Perú al convenio de Budapest en febrero ultimo evidencia el compromiso del Poder Ejecutivo poder dar lucha a la ciberdelincuencia que permita lograr la seguridad digital de los ciudadanos y empresas del país, dentro de este último se encuentra la industria bancaria.

La seguridad digital es un tema muy preocupante que los bancos no pueden dejar de lado ya que un ciberataque puede amenazar su normal operación en los canales financieros tal como sucedió en el ultimo evento registrado el 18 de agosto del año pasado dañando su imagen corporativa y perdiendo de lado millones de dólares que no fueron intermediados ya sea por el pago de servicios y/o recaudación.

En ese sentido, la tesis identifica una clara oportunidad de negocio que permite hacer freno a todos estos problemas de ciberseguridad que viene afrontando el sector financiero, al crear una plataforma centralizada en ASBANC que permita atender en principio a los bancos con una participación de mercado menor al 18%, para ello se buscará un socio comercial de talla internacional que pueda ayudar a brindar todas las protecciones cibernéticas para que los problemas afrontados en los últimos tiempos puedan disminuir el riesgo actual donde el socio ofrezca la parte operativa de la plataforma y ASBANC ofrezca la parte comercial, dicha relación de negocios permitirá a los bancos no incurrir en costos de inversión inicial y solo tendrán un costo operativo mensual por la adquisición del servicio personalizado.

Se ha identificado que los decisores de compra dentro del mercado meta primario son los jefes y gerentes de seguridad electronica, los mismos que autorizan dentro de sus presupuestos anuales este tipo de gastos, para ello el influencer de lado de ASBANC que permita generar esa confianza en el proyecto recae en la figura del gerente de operaciones ya que mantiene un alto nivel de relacionamiento con las figuras claves dentro del negocio.

Si bien es cierto el problema que afronta la industria financiera es una clara oportunidad de negocio para ASBANC que permitirá generar los ingresos necesarios

para mejorar el ambiente de negocios de los asociados a través del rol de representación gremial que este ejerce, ante ello se sabe que la ciberseguridad es un problema muy grande en el mundo y los bancos peruanos no se encuentran preparados, es por ello que se plantea dentro del modelo de negocio asociarse con un socio estratégico de talla mundial para atender dichas necesidades, la propuesta de valor será ofrecer el servicio base MSS (Managed Security Services), el mismo que se encargará de detectar al interior de cada banco las vulnerabilidades y falencias de los sistemas e infraestructuras críticas, el potencial de mercado de ciberseguridad asciende a 5 millones de dólares anuales, de lo que se espera capturar 1.8 millones del mismo al tercer año, para ello se plantea una estrategia en el precio de introducción para su comercialización en $9,500 mensuales y luego se le ofrecería las soluciones de servicios avanzadas en $26,875 y la suite completa por $65,000 mensuales.

Después de haber realizado un sondeo del mercado a tráves de un focus group con los jefes y gerentes de seguridad del grupo de bancos objetivo, se determinó que todos tienen la necesidad latente de contar con una solución de ciberseguridad, es por ello que al presentar el concepto del servicio este fue aceptado unnimemente.

Este proyecto es marginal, por lo que se requiere una inversión inicial muy baja ya que utilizará la capacidad instalada existente, se espera que durante el primer año de operación del servicio obtener una ingreso por $230,000, el mismo que se incrementará durante los años siguientes que se proyectan, la evaluación económica arroja una VAN de $ 354,911 descontada a la tasa exigida por los accionistas del 22%.

CAPÍTULO I. INTRODUCCION

1.1. Antecedentes

Las ciencias de la información avanzan a una velocidad impresionante, adecuándose a un nuevo consumidor que cada vez se transforma digitalmente, ya que la facilidad de uso de las aplicaciones móviles y negocios que brindan sus servicios a través de dichos medios hacen que sean también un punto de vulnerabilidad respecto a la información que se transa entre cliente y empresa, por eso se puede evidenciar que existe un nivel creciente de ataques cibernéticos y diferentes formas de poder ejecutarlos.

Por esta razón, una de las principales industrias, la industria financiera, pierde millones de dólares por año afectando su imagen corporativa, su reputación y también la estabilidad de su existencia, ya que necesitan estar al día con esta evolución que no tiene fin en términos de innovación, para poder superar las barreras informáticas que las grandes empresas de tecnología le agregan a su oferta de servicio. De acuerdo con ello, Simón Sinek (Sinek, 2018) expresa en su video "The Infinity Game (Sinek,2018)", una teoría basada en la diferencia de los "juegos infinitos" vs "juegos finitos", haciendo una analogía con la seguridad de la información, que expresada en términos coloquiales se podría decir que, un Ciberdelincuente cuenta con recursos ilimitados (el tiempo, una comunidad activa de hackers, entre otras herramientas), ya que juegan en un mundo donde no existen las reglas. Por lo tanto, una forma de poder hacer contraparte a esta situación es poder jugar con reglas similares, en un tablero de juego infinito, ya que actualmente las grandes corporaciones juegan con reglas conocidas y aceptadas por todos; sin embargo, estas reglas son limitadas en su campo de acción (juego finito), es entonces que se encuentra en un nuevo punto de la evolución humana donde el uso de la inteligencia artificial ayudará a los consumidores a poder adaptarse a nuevos entornos de manera efectiva, esto significará una evolución en los modelos de negocio ya existentes ya que muchas empresas visionando este nuevo camino han iniciado su proceso de transformación digital.

1.2. Objetivos

1.2.1. Objetivo general

Definir un plan de negocios para evaluar la viabilidad de implementar el primer CERT Financiero para el sistema financiero peruano.

1.2.2. Objetivos específicos

- Estimar el mercado potencial para el uso de una plataforma centralizada de Ciberseguridad.
- Crear un modelo de negocio que permita generar economías de escala.
- Determinar la rentabilidad de crear una plataforma centralizada de Ciberseguridad.

1.3. Justificación

En noviembre de 1988, un estudiante de la Universidad de Cornell lanzó en esta red un programa que se propagaba y se replicaba solo. Este programa, conocido con el nombre de "gusano de Internet", aprovechaba distintos fallos de seguridad del sistema Unix (el sistema operativo de la mayoría de los ordenadores conectados en la red). Con sólo el 3 o 4% de las máquinas contaminadas, la red estuvo totalmente indisponible durante varios días, hasta que se tomaron medidas cautelares (incluyendo la desconexión de numerosas máquinas de la red).

Para eliminar este "gusano de Internet", se creó un equipo de análisis ad hoc con expertos y se reconstituyó y analizó el código del virus, lo cual permitió, por una parte, identificar y corregir los fallos del sistema operativo, y, por otra parte, desarrollar y difundir mecanismos de erradicación.

Después de este incidente, el director de obras de Arpanet, la DARPA (Defense Advanced Research Projects Agency), decidió instalar una estructura permanente, el CERT Coordination Center (CERT/CC) parecido al equipo reunido para resolver el incidente.

Con el tiempo, los CERT ampliaron sus capacidades y pasaron de ser una fuerza de reacción a prestadores de servicios de seguridad completos que incluyen servicios preventivos como alertas, avisos de seguridad, formación y servicios de gestión de la

seguridad. Pronto el término “CERT” se consideró insuficiente, y a finales de los años noventa se acuñó el término “CSIRT”. En la actualidad, ambos términos (CERT y CSIRT) se usan como sinónimos (Ministerio de Comunicaciones, 2008).

1.4. Alcances y Limitaciones

1.4.1. Alcances

- **Alcance de recursos de investigación:**

De acuerdo con lo planteado por Arroyo (2012) en su propuesta de tesis, “[e]l estado de conocimientos sobre el tema de investigación mostrado a través de la revisión de la literatura existente, es amplio. Para lograr el objetivo de recolectar información exploratoria del negocio propuesto, el autor de esta tesis propone revisar” (Arroyo, 2012:4)

- Información encontrada en internet.
- Entrevistas en profundidad y/o focus group con el grupo objetivo.
- Entrevistarse con proveedores de soluciones tecnológicas.

- **Alcance de contenido:**

La tesis se enfoca en elaborar un plan de negocios para evaluar implementar una plataforma de Ciberseguridad para el sistema financiero peruano:

- Analizar la demanda de servicios de Ciberseguridad.
- Analizar la oferta de las empresas que brindan servicios de Ciberseguridad a nivel país.
- Determinar los factores internos y externos que afectan el normal desempeño de las operaciones financieras.
- Realizar un análisis estratégico para definir el crecimiento empresarial de dicha empresa para los próximos 10 años.

- El plan de negocios incluye las estrategias tácticas de marketing, operaciones, recursos humanos, y Financieros.
- Evaluar la viabilidad y rentabilidad del negocio.

1.4.2. Limitaciones

- **De información histórica:** existe poca información histórica a detalle en las bases consultadas respecto a los Ciberataques, ya que es un tema muy restringido.
- No se ha podido validar los leads ya que esta compuesto por opiniones de los seis bancos participantes.
- Confidencialidad de la información.

CAPÍTULO II. MARCO CONCEPTUAL

En el presente capítulo se tiene como principal objetivo brindar una visión integral del tema de Ciberseguridad, para ello se abordará desde su definición, evolución, las tipologías y cuales son las principales amenazas identificadas a nivel local e internacional.

2.1 Definición de Ciberseguridad

ISACA lo define como la protección de los sistemas conectados a Internet, incluyendo hardware, software y data contra los Ciberataques, donde la seguridad comprende la seguridad física y la Ciberseguridad ambos se complementan y son usados por las empresas para proteger los accesos no autorizados a los data center o sistemas computarizados, siempre bajo el triunvirato de la confidencialidad, integridad y la disponibilidad que profesa la seguridad informática.

En septiembre del 2018 La Asociación Española para el Fomento de la Seguridad de la Información en su VIII foro de Ciberseguridad (Thierry Karsenti, 2018) para el Cyber Security Center presentó una línea de evolución en los ataques a la Ciberseguridad a lo largo de la historia presentado por la empresa Checkpoint, en dicha evolución se mostraron como es que las modalidades han ido haciéndose cada vez más complejas debido a que han sido perfeccionadas entre una generación y otra, a continuación se muestra en la tabla 2.1 las cinco generaciones con la cual se les clasifico:

Tabla 2.1: Evolución de las ciberamenazas

I Generación	Los ataques de virus en ordenadores independientes comenzaron sobre todo como bromas o con afán destructivo. Para detener estas molestias, se desarrollaron productos antivirus.
II Generación	Los hackers ya no necesitan ir de PC en PC para infectar, puesto que pueden conectarse desde internet. Nace la industria de la seguridad en red y se lanza el primer firewall.
III Generación	Los atacantes empezaron a analizar redes y software para encontrar y explotar vulnerabilidades en toda la infraestructura de TI. Los firewalls y antivirus resultaron ser insuficientes frente a exploit. Thierry Karsenti explica que su

	compañía comenzó a centrarse en la prevención y lanzó sistemas de prevención de intrusos (IPS).
IV Generación	Los ciberataques alcanzaron un nuevo nivel de sofisticación, que abarcaban desde el espionaje internacional hasta las brechas masivas de información personal y la interrupción de Internet a gran escala. Los ataques se ocultaban de mil maneras, desde currículums hasta archivos de imágenes, evasivos y polimórficos. La seguridad de internet de segunda y tercera generación proporcionaba control de acceso e inspeccionaba todo el tráfico. Sin embargo, no era capaz de enfrentarse a los nuevos ataques polimórficos. En respuesta a esto, se introdujo el 'sandboxing', para analizar de forma dinámica el contenido que llega desde el exterior y para afrontar los ataques de día cero.
V Generación	Las herramientas de hacking avanzadas 'de grado militar' se filtran, permitiendo a los atacantes moverse rápido e infectar un gran número de empresas y entidades cubriendo enormes áreas geográficas. Los ataques a gran escala y multivectoriales generan la necesidad de contar con estructuras de seguridad integradas y unificadas. Las generaciones anteriores de patching y las tecnologías líderes de detección de primera generación no son capaces de lidiar con los ataques rápidos y sigilosos de quinta generación. En este contexto, se desarrolla una arquitectura unificada con soluciones avanzadas de prevención de amenazas que comparten la inteligencia de amenazas en tiempo real, evitando ataques en diferentes escenarios como instancias virtuales, despliegues en la nube, EndPoint, oficinas remotas y dispositivos móviles.

Fuente: CheckPoint (2018)

2.2 Tipologías de Ciberseguridad

Existen diferentes formas de poder definir este punto, por ello la seguridad que se aplique debe ser proporcionada y compensada de acuerdo con el valor y grado de confianza en el sistema informático que soporta la operación del negocio, la severidad, la probabilidad y el grado potencial del daño, por ello se muestran las principales tipologías en la tabla 2.2, mayor alcance en la información se podrá encontrar en el Anexo VIII.

Tabla 2.2: Principales tipos de ciberseguridad

a. Las prácticas de gestión de seguridad b. Sistemas de control de acceso y la metodología c. Telecomunicaciones y seguridad de redes d. Criptografía e. Operaciones de Seguridad f. Aplicación y sistemas de seguridad de desarrollo g. Seguridad física h. La continuidad del negocio y la planificación de recuperación de desastres i. Leyes, investigación y ética

Fuente: First.org
Elaboración: Autor de la tesis

a. Las prácticas de gestión de seguridad:

Se le definen para la clasificación de la información y de activos, el proceso de clasificación o categorización de información y activos proporciona una base para la definición de los controles y ayuda a diferenciar los tipos de medidas de seguridad.

b. Sistemas de control de acceso y la metodología:

Con el objetivo de mantener la confidencialidad, integridad y disponibilidad de la información es importante que se defina una correcta estrategia de acceso a la información que permita realizar una clasificación en cuatro aspectos: prevención, detección, correctivo, de compensación.

c. Telecomunicaciones y seguridad de redes:

Métodos de comunicación, formatos para el transporte de datos, y las medidas adoptadas para asegurar la red y la transmisión

d. Criptografía:

Se ocupa de las medidas de seguridad que se utilizan para garantizar que la información transmitida es legible sólo por los usuarios apropiados.

e. Operaciones de Seguridad

Aplicación de controles y protecciones correctas en el hardware, software y otros recursos del sistema, al mantenimiento de una auditoría y seguimiento adecuados; y la evaluación de las amenazas y las vulnerabilidades del sistema.

f. Aplicación y sistemas de seguridad de desarrollo:

Adoptar buenas prácticas en el desarrollo donde el código de software deberá ser escrito siguiendo una pauta de codificación segura

g. Seguridad física

Aborda el entorno que rodea al sistema de información y medidas de prevención adecuadas para proteger físicamente el sistema.

h. La continuidad del negocio y la planificación de recuperación de desastres:

La planificación de la continuidad del negocio es el proceso de elaboración de los planes que garanticen que las funciones críticas del negocio tengan la capacidad de soportar una diversidad de situaciones de emergencia. En cambio, la planificación de recuperación de desastres consiste en desarrollar los preparativos para solventar un potencial desastre, y también se ocupa de los procedimientos que deberán seguir los recursos durante y después de una pérdida.

i. Leyes, investigación y ética:

Establece las expectativas que los profesionales de seguridad deben entender, así como leyes internacionales sobre la seguridad de la información, tipologías de ciberdelitos que se pueden cometer y las complicaciones específicas que la investigación de un ciberdelito representa para el equipo de analistas de una organización

2.3 Las amenazas cibernéticas

A medida que se desarrollan los cambios tecnológicos existen diferentes formas de ataque por parte de los denominados terroristas de la información o también denominados Hackers lo que obliga a las organizaciones a invertir en soluciones que les permita robustecer los pilares básicos de la seguridad de información que son confidencialidad, integridad y disponibilidad, a continuación, se listará las principales amenazas cibernéticas expuestas (Laudon, 2013)

Tabla 2.3: Principales Amenazas Cibernéticas

Codigo Malicioso o Malware: Virus, Gusanos, Caballos de troya,Backdoors y Bots
Programas Potencialmente Ideseables (PUPS): Adware, parasito de navegador y spyware
Phishing y Robo de Identidad
Sitios web de falsificacion (Pharming)
SPAM(Basura)
Ataques de denegación de servicio (DOS)
Ataques distribuidos de Denegación de Servicios (DDOS)
Husmeo o SNIFFING
Ataques Internos
Software de Servidor y Cliente mal diseñado

Fuente: Laudon (2013)
Elaboración: Autor de la tesis

a. Código Malicioso o Malware:

Virus: Programa informático que tiene la capacidad de duplicarse o hacer copias de si mismo y extenderse a otros archivos.

Gusano: Malware diseñado para extenderse de una computadora a otra.

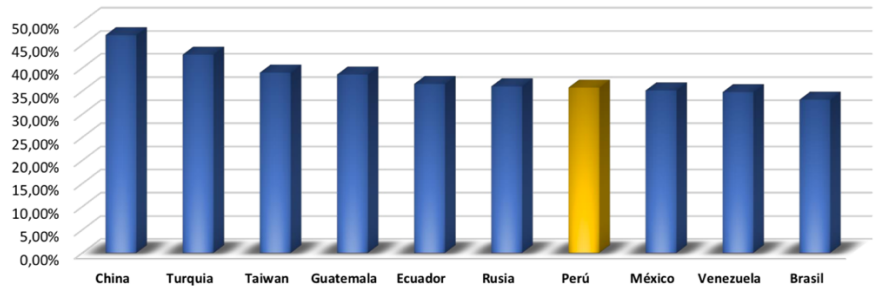
Caballo de Troya: Programa que parece ser benigno, pero luego hace algo inesperado. A menudo es una vía para que los virus y otro tipo de código malicioso se introduzcan en un sistema de computo.

Puerta Trasera: Característica de los virus, gusanos y troyanos que permite que un atacante acceda de forma remota a una computadora comprometida.

Bot: Tipo de código malicioso que se puede instalar de manera encubierta en una computadora cuando esta se conecta a internet. Una vez instalado el bot responde a los comandos externos enviados por el atacante.

En la Figura 2.1 se puede observar la estadística en la cual China ocupa el primer lugar con una tasa de infección del 46%, en segundo lugar, Turquía con una tasa de infección del 41% y en séptimo lugar Perú con una tasa de infección del 35.75% en lo que corresponde a Malware Financiero sobre una base obtenida de 288, 783, 981 puestos de trabajo y servidores comprometidos en 190 países de todo el mundo.

Figura 2.1: Malware Financiero



Fuente: AIUKEN Cybersecurity (2018)

a. Programas Potencialmente Indeseables (PUPS):

Adware: Programa potencialmente indeseable que hace aparecer publicidad emergente en una computadora.

Parásito de navegador: Programa que puede monitorear y modificar la configuración del navegador de un usuario.

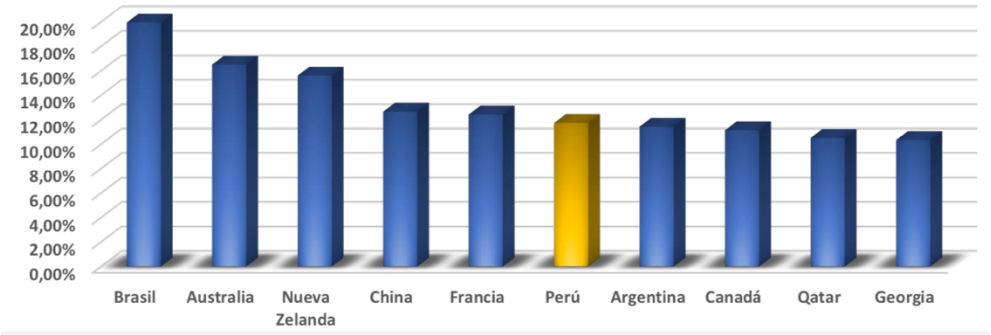
Spyware: Software que se utiliza para obtener información tal como las pulsaciones de teclas de un usuario, correo electrónico, mensajes instantáneos, etc.

Ingeniera Social: Explotación de la falibilidad e ingenuidad humana para distribuir el malware.

b. Phishing: Cualquier intento engañoso habilitado en línea por parte de alguien que quiere obtener información confidencial a cambio de un beneficio económico.

En la Figura 2.2 se puede observar la estadística en la cual Brasil ocupa el primer lugar con una tasa de infección del 19,95%, en séptimo lugar Perú con una tasa de infección del 11,73% en lo que corresponde a Phishing Financiero sobre una base obtenida de 479, 528, 279 ataques de Phishing detectados contra recursos online situados en 190 países de todo el mundo.

Figura 2.2: Phishing Financiero



Fuente: AIUKEN Cybersecurity (2018)

c. Pharming: Falsificación de un sitio web, consiste en redirigir un vinculo a un sitio web que no es el deseado, pero se enmascara como si lo fuera.

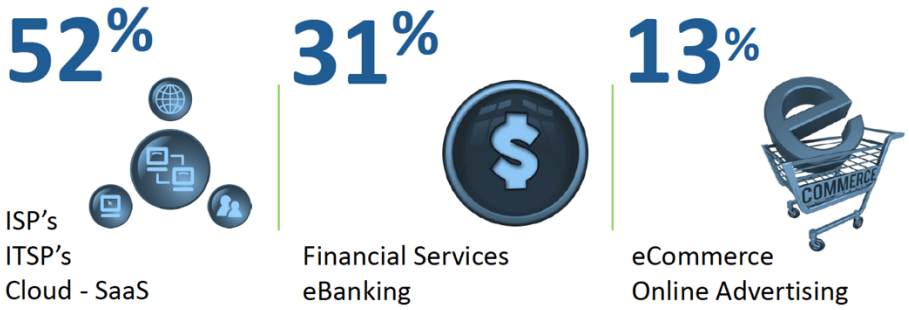
d. Spam: Sitios Web que prometen algún producto o servicio, pero en realidad son una serie de anuncios que te llevan hacia sitios con código malicioso.

e. Ataque de denegación de servicio (DOS): Inundación de un sitio web con trafico inútil para desbordar y saturar la red

f. Ataque distribuido de denegación de servicio (DDoS): Uso de varias computadoras para atacar la red objetivo desde varios puntos de lanzamiento.

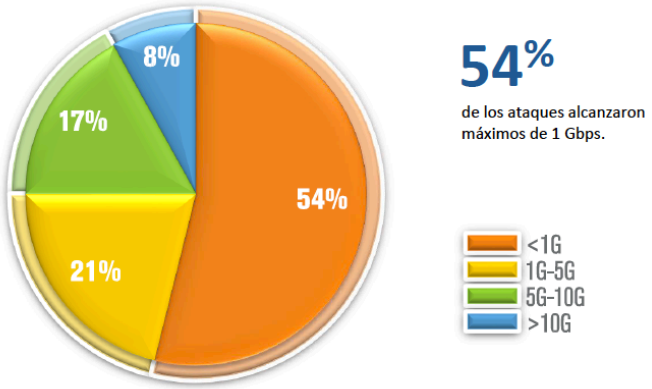
En la Figura 2.3 se puede observar los principales objetivos de la DDoS por tipo de industria, donde la industria financiera ocupa el segundo lugar dentro del segmento objetivo, asimismo se puede observar en la figura 2.4 que el 54% de los ataques alcanzaron máximos de 1 Gbps.

Figura 2.3: DDoS objetivos por Industria



Fuente: AIUKEN Cybersecurity (2018)

Figura 2.4: Volumetría de los Ataques DDoS



Fuente: AIUKEN Cybersecurity (2018)

g. Husmeador (Sniffer): Tipo de programa para escuchar clandestinamente que monitorea la información que viaja a través de la red

h. Ataques Internos: Los empleados tienen acceso a información privilegiada y, ante procedimientos de seguridad interna defectuosos, pueden entrar libremente a los sistemas de una organización sin dejar rastro.

2.4 Relación entre las amenazas cibernéticas y las tipologías de Ciberseguridad:

De acuerdo con los puntos 2.2 y 2.3 vistos en los acápites anteriores, se puede observar en la tabla 4.4 la relación existente entre las principales amenazas cibernéticas y sus tipologías.

Tabla 2.4: Relación entre amenazas y tipologías Ciberseguridad

Amenazas	**Tipologías**
Código Malicioso y Malware	Aplicación y sistemas de seguridad de desarrollo
Programas Potencialmente Indeseables	Operaciones de Seguridad
Phishing y Robo de Identidad	Telecomunicaciones y seguridad de redes
Sitios web de falsificación (Pharming)	Telecomunicaciones y seguridad de redes
SPAM(Basura)	Operaciones de Seguridad
Ataques de denegación de servicio (DOS)	La continuidad del negocio y la planificación de recuperación de desastres.
Husmeo o SNIFFING	
Ataques Internos	Leyes, investigación y ética.

Fuente: Autor de la tesis

CAPÍTULO III. LA ASOCIACION DE BANCOS

En este capítulo se aborda, los roles que desempeña ASBANC, el plan estratégico planteado hacia el 2021 y describir cuáles son las líneas de servicios que viene brindando, así como también un análisis de su situación financiera.

3.1 Reseña Histórica

El 26 de enero de 1967, un grupo de representantes de 15 bancos comerciales suscribieron la minuta de constitución de la Asociación de Bancos del Perú - ASBANC - y el 22 de junio del mismo año el acta de instalación, siendo su principal objetivo representar a los bancos afiliados y ejercer su presencia en las decisiones que afecten al sector.

3.2 Rol de ASBANC

Los Estatutos de ASBANC en su artículo 2 señalan que el rol de ASBANC con sus asociados es el siguiente:

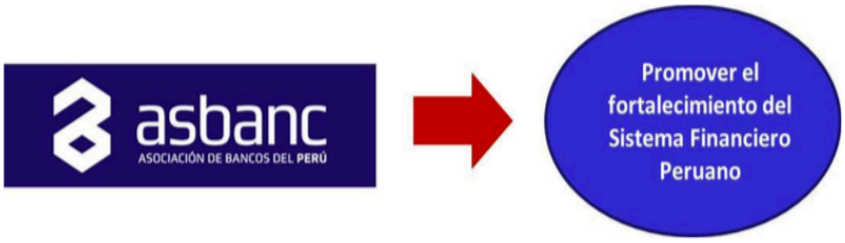
1. Ejercer con las facultades necesarias y suficientes la representación de sus asociados en los asuntos que, por su naturaleza, tengan carácter de comunes, promoviendo y defendiendo sus legítimos intereses;
2. Promover el fortalecimiento del Sistema Financiero Peruano.
3. Colaborar con los Poderes Públicos para el estudio y la expedición de normas que tiendan al mejoramiento de la legislación bancaria, financiera y comercial del país;
4. Promover y realizar estudios y publicaciones en los campos bancario, financiero y tributario.
5. Proporcionar a sus asociados servicios de información, asesoría y consulta en asuntos de interés general, para lo cual, sin menoscabo de la necesaria reserva bancaria, les solicitará las informaciones que juzgue necesarias;
6. Fomentar el desarrollo de relaciones cordiales entre sus asociados.
7. Llevar a cabo en la medida más amplia posible una divulgación de los servicios y de los problemas de sus asociados y una labor de relaciones públicas; incluyendo el mantenimiento de relaciones amistosas y de colaboración con Asociaciones

representativas de los diferentes sectores de la actividad nacional y asociaciones similares en el extranjero.

8. Estimular la formación y especialización bancaria y financiera de los recursos humanos a través del Centro de Estudios Financieros – CEFI de la Asociación de Bancos del Perú y fomentar el desarrollo de instituciones docentes con programas afines a la actividad bancaria y financiera.
9. Promover el establecimiento y ejecución de políticas generales de seguridad a través de su Programa Integral de Seguridad Bancaria, con miras a lograr un entorno confiable para el desarrollo de la actividad financiera.
10. Establecer, operar y mantener los servicios de interés común que requieren sus asociados.

Al analizar lo señalado, se observa que todos los puntos del artículo 2 se pueden resumir en "Promover el fortalecimiento del Sistema Financiero" según se esquematiza en la figura 3.1

Figura 3.1: Rol de ASBANC



Fuente: Autor de la tesis

3.3 Descripción de la estrategia de ASBANC

3.3.1 Visión:

Representar a las instituciones privadas del sector financiero, velando por el desarrollo sostenible del sistema financiero y del país.

3.5.1 Misión:

Ejercer de articulador entre las instituciones financieras del país, identificando, desarrollando y administrando aspectos de interés común a las mismas, para su promoción y desarrollo.

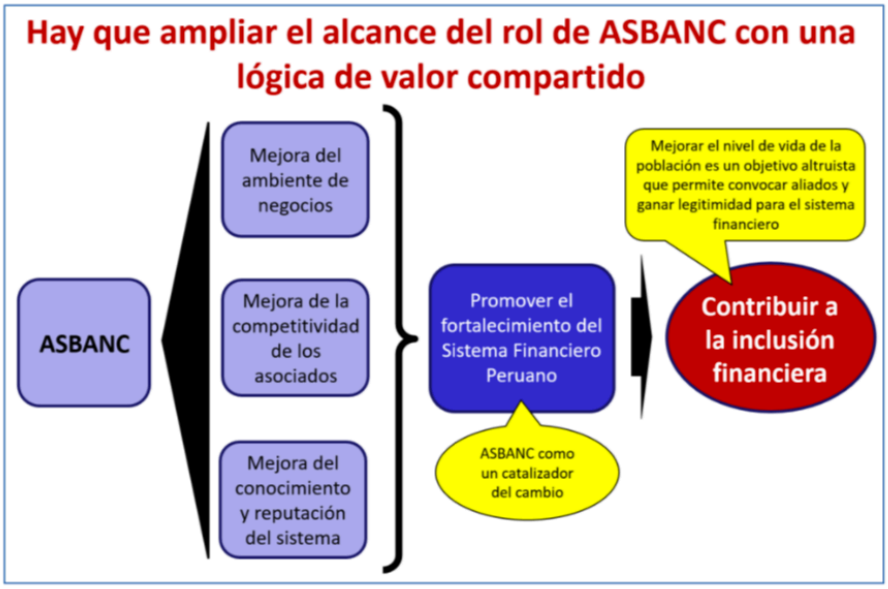
3.5.1 Lógica del Plan Estratégico:

La Asociación de Bancos elaboró en el 2018 un plan estratégico para el periodo 2019-2021 donde se plantea que el objetivo sea “Contribuir a la inclusión financiera”, siendo este un objetivo que va más allá de favorecer al sistema bancario y apunta a causar un impacto favorable en el nivel de vida de la población peruana.

Plantearse un objetivo altruista permite convocar como aliados a otras organizaciones del Estado y empresas privadas y así ganar legitimidad para el sistema financiero, dicha lógica cae dentro de lo que el gurú de la estrategia Michael Porter llamo como valor compartido (Porter & Kramer, 2011), en donde ASBANC asume la función de catalizar el cambio en el sistema financiero, como se muestra en la figura 3.2, en ese sentido para lograr dicha legitimidad se plantea una serie de perspectivas que permitirán apoyar tal objetivo.

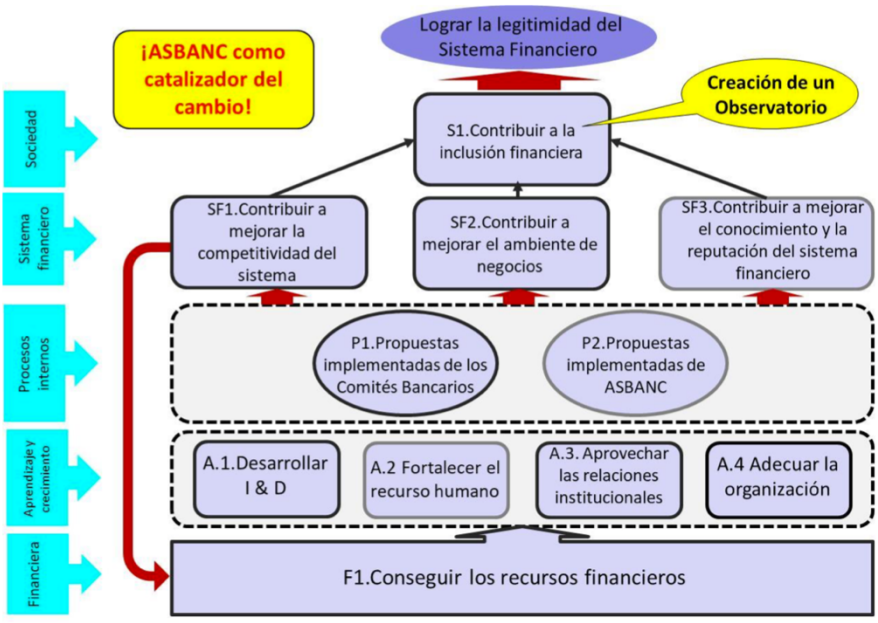
Dentro de esta nueva lógica que propone el plan estratégico, se encuentra la generación de ingresos brindando servicios útiles para financiar la representación gremial, por ello se busca el desarrollo de nuevos servicios como el que esta planteando este trabajo de tesis a partir del fortalecimiento de la perspectiva de aprendizaje y desarrollo, que se puede ver en la figura 3.3.

Figura 3.2: Lógica del Plan Estratégico 2019 – 2021



Fuente: ASBANC

Figura 3.3: Plan Estratégico 2019 – 2021

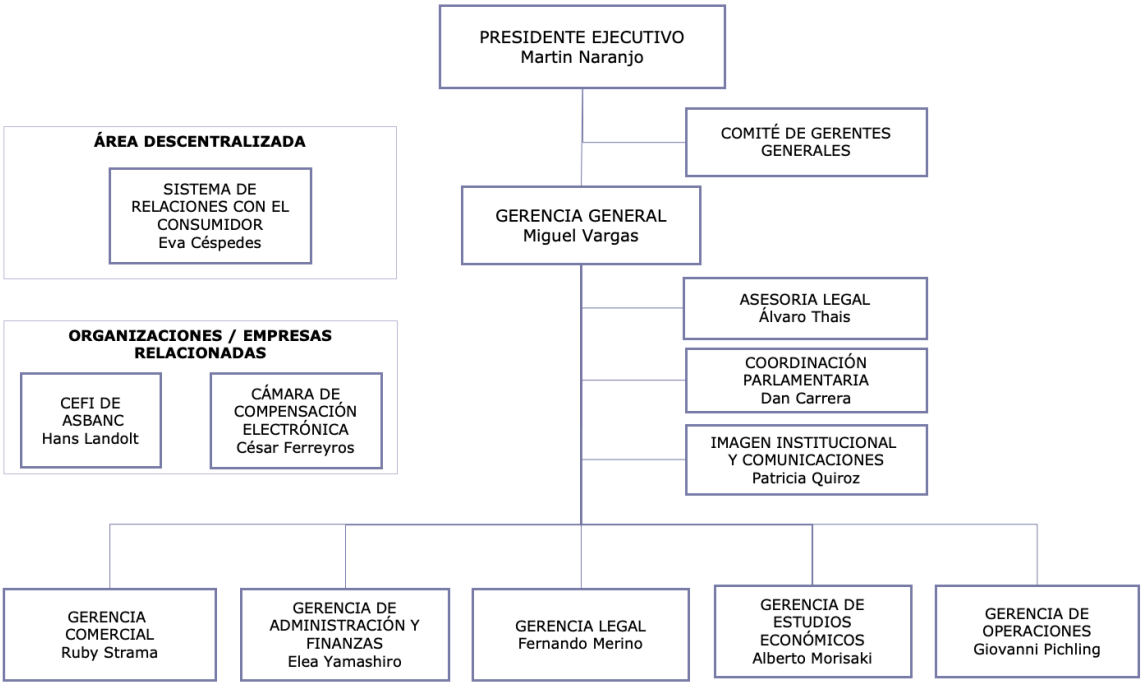


Fuente: ASBANC

3.4 Estructura Organizacional:

Al mes de mayo del 2018, ASBANC, CCE y CEFI cuenta con un total de 154 ejecutivos y empleados, los cuales 136 corresponden a ASBANC, 10 al CEFI y 8 al CCE, si se subdivide en el tipo de rol que asume cada gerencia, se tiene que son 76 profesionales que se encuentran en servicios, 48 en funciones gremiales y 24 en funciones administrativas, según se observa en la figura 3.4, siendo los profesionales de servicios que se encargan de atender y dar soporte a los bancos y empresas asociadas.

Figura 3.4: Organigrama

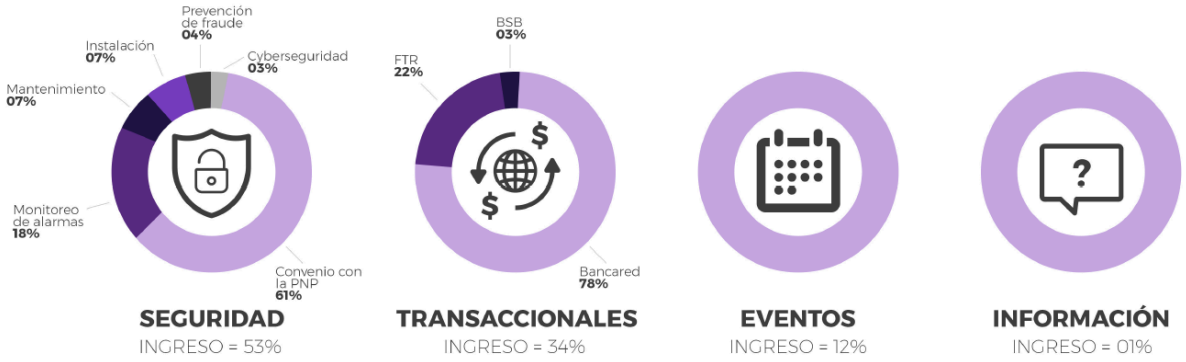


Fuente: ASBANC
Elaboración Propia

3.5 Líneas de Negocio

Dentro del portafolio de servicios se puede encontrar las siguientes cuatro categorías de servicios, siendo el ingreso anual de ASBANC alrededor de los 29 millones de soles en el 2017, en la figura 3.5 se observa la composición porcentual del portafolio correspondiente a los servicios de seguridad que representa 53%, los servicios transaccionales el 34%, los eventos el 12% y los servicios de información apenas el 01%.

Figura 3.5: Portafolio de Servicios ASBANC



Fuente: ASBANC
Elaboración Propia

3.5.1 Servicios de Información:

Relacionados a los informes estadísticos que se ofrecen a los asociados y/o empresas financieras sobre las tendencias del sector, los productos y servicios ofertados.

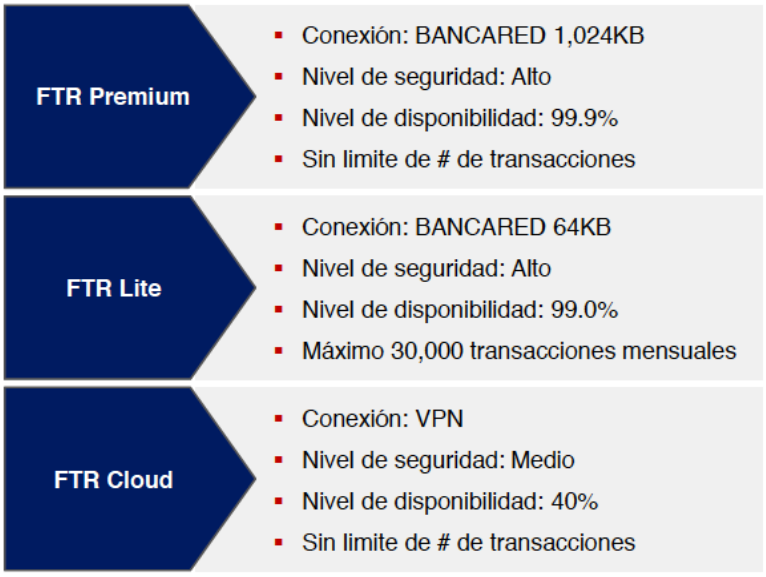
3.5.2 Servicios Transaccionales:

Relacionados a los servicios que permiten tener información en línea entre el banco y las empresas asociadas para la recaudación, entre los servicios se encuentra al FTR que es el Facilitador Transaccional de Recaudaciones, y BANCARED que es la red privada de bancos.

3.5.2.1 FTR

El servicio FTR es una solución tecnológica que permite el intercambio de información de recaudación entre el cliente y los bancos afiliados en tiempo real, contando con tres variantes de producto: Premium, Lite y Cloud.

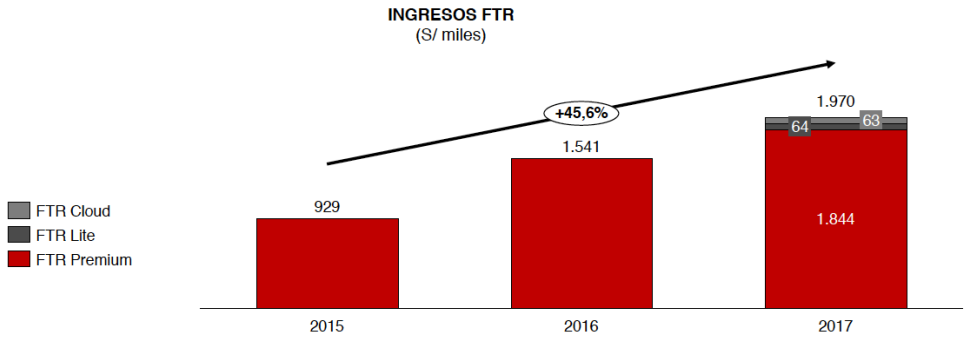
Figura 3.6: Tipologías del servicio FTR



Fuente: Autor de la tesis

Este servicio ha venido creciendo a un ritmo de 45.6% promedio anual durante los últimos tres años como se puede visualizar en la figura 3.5, este crecimiento ha permitido que a la fecha se cuente ya con 50 clientes en total.

Figura 3.7: Ingresos del FTR



Fuente: ASBANC

Clientes Target:

Empresas con alto volumen de transacción por recaudación (empresas proveedoras de financiamiento y prestadora de servicios masivos principalmente).

Entidades Financieras Afiliadas:

Se encuentra a las más representativas del sector financiero, las mismas que figuran en la figura 3.8

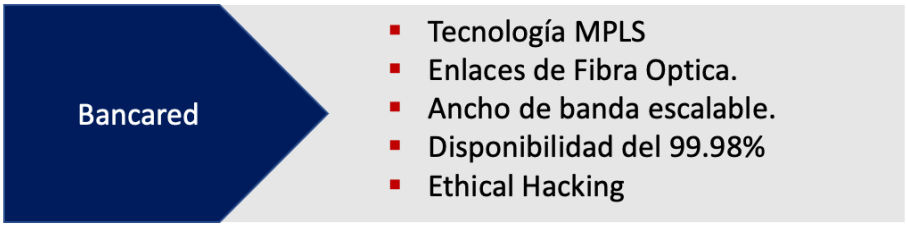
Figura 3.8: Entidades Afiliadas

Fuente: Autor de la tesis

3.5.2.2 Bancared

El servicio Bancared es una red que sirve como único medio de conexión con las entidades financieras del país, esta conexión es una red privada de comunicaciones segura, flexible, veloz y con una alta disponibilidad, sus características técnicas se pueden visualizar en la figura 3.9.

Figura 3.9: Características del servicio Bancared



Fuente: Autor de la tesis

Clientes Target:

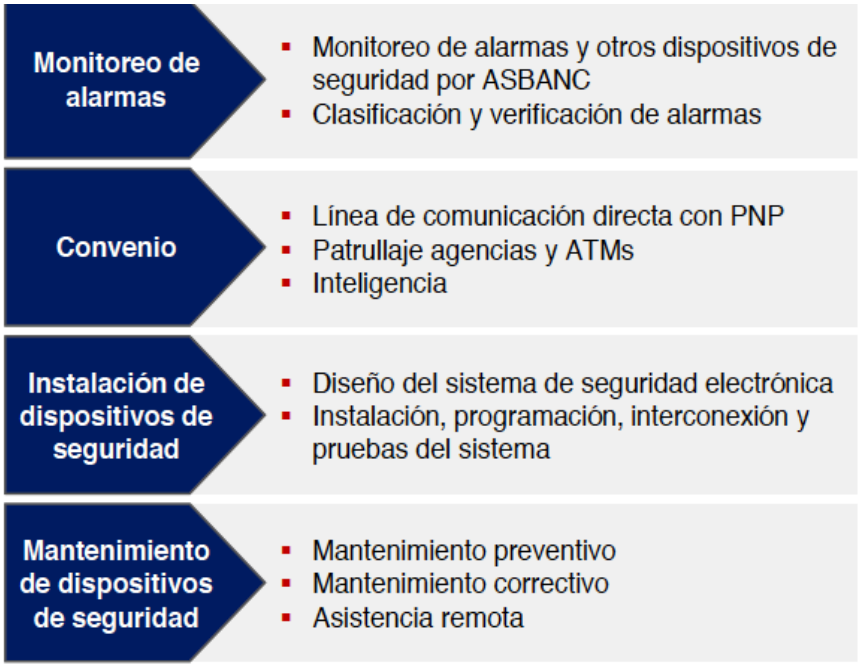
Bancos, financieras, microfinancieras, cajas, empresas aseguradoras, AFP y empresas del sector bursátil.

3.5.3 Servicios de Seguridad:

Existen dos subcategorías la física, dentro de la seguridad física se encuentra los servicios de Monitoreo, Convenio, Instalación y Mantenimiento, el detalle de los mismos se puede visualizar en la figura 3.10, dentro de los servicios de seguridad electrónica se tiene los servicios de AFS y Ciberseguridad, la explicación a ambos se puede observar en la figura 3.11, donde el servicio de Ciberseguridad actual es el que se quiere repotenciar para ofrecer a los asociados como una nueva línea, ya que el servicio actual sólo se encarga de brindar un informe sobre las vulnerabilidades encontradas en la Deep Web.

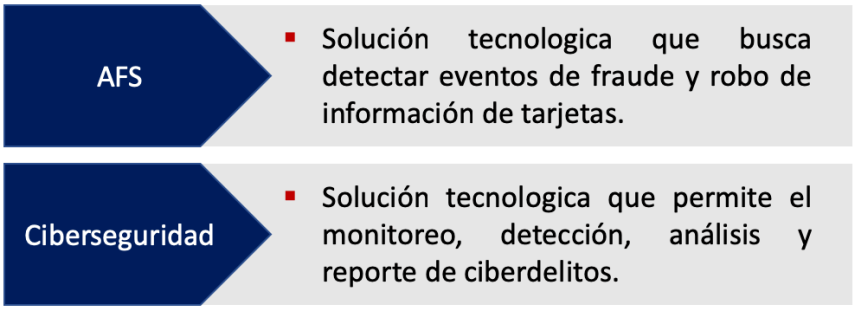
Asimismo, si se realiza un análisis sobre el ingreso total de los servicios de seguridad física, el mismo que puede visualizarse en la figura 3.12 y adicionalmente se observa que los servicios de AFS y Ciberseguridad han ido decreciendo su ingreso de manera considerable, es por ello por lo que el presente plan de tesis tiene como objetivo repotenciarlo y volverlo en una de las líneas principales de servicio de la asociación.

Figura 3.10: Servicios de seguridad física



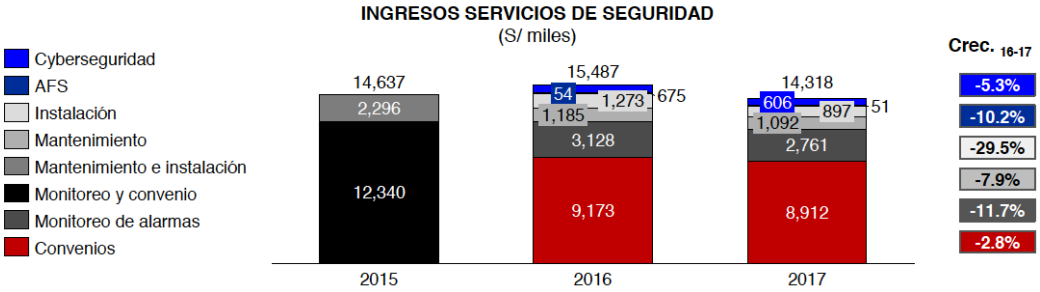
Fuente: Autor de la tesis

Figura 3.11: Servicios de seguridad electrónica



Fuente: Autor de la tesis

Figura 3.12: Ingresos Servicios de Seguridad



Fuente: ASBANC

3.5.4 Eventos:

Este servicio se realiza de manera eventual y se centra en la realización de cuatro eventos al año, entre ellos se encuentran el de Riesgo Operacional, Business Innovation Summit, Seminario de prevención de Fraudes y el de Prevención de Lavado de Activos, la publicidad relacionada a ellos se puede visualizar en la figura 3.13.

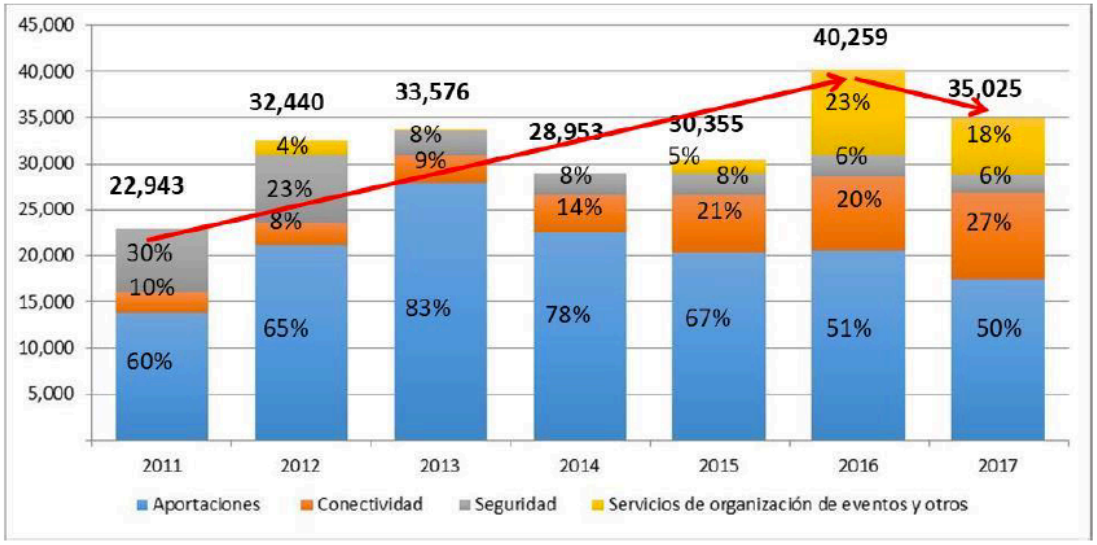
Figura 3.13: Publicidad de eventos

Fuente: ASBANC

3.6 Evolución de los ingresos

Los ingresos de ASBANC crecieron 52.7% en el periodo 2011- 2017 sin embargo, en el último periodo 2016 – 2017 decrecieron un 13% los ingresos por aportaciones que han ido disminuyendo a partir del año 2013 progresivamente, pasando de 83% a 50% en el año 2017 muy por el contrario ocurre con los servicios de conectividad, eventos y seguridad que han incrementado su ingreso como se puede observar en la figura 3.14.

Figura 3.14: Evolución de los ingresos



Fuente: ASBANC
Elaboración: Propia

3.7 Estados financieros

En la tabla 3.1 se puede visualizar un análisis vertical y horizontal de los estados financieros desde el año 2011 hasta el 2017, en el se puede observar que las aportaciones han ido disminuyendo considerablemente, estos aportes corresponden a la cuota gremial, sin embargo los ingresos correspondientes a los servicios de tecnología han ido aumentando, asimismo dentro de los servicios de seguridad registrado como PISB estos han ido disminuyendo su ingreso, así como también los servicios registrados contablemente como ingeniería y mantenimiento, mientras que los eventos ofrecidos por ASBANC son eventuales y depende de la demanda de los asociados.

Tabla 3.1: Análisis vertical y horizontal de los estados financieros

	2011	2012	2013	2014	2015	2016	2017	% de variación 2012 - 2011	2013 - 2012	2014 - 2013	2015 - 2014	2016 -2015	2017 - 2016
Ingresos de Actividades Ordinarias	**22,943**	**32,440**	**33,576**	**28,953**	**30,355**	**40,259**	**35,025**	**41%**	**4%**	**-14%**	**5%**	**33%**	**-13%**
Aportaciones	6,701	13,708	14,981	9,615	8,453	11,364	8,587	105%	9%	-36%	-12%	34%	-24%
Servicios de tecnologia	2,249	2,482	3,050	4,036	6,334	7,956	9,321	10%	23%	32%	57%	26%	17%
Servicios de la unidad de ingenieria y mantenimiento	6,953	7,353	2,564	2,410	2,296	2,308	2,003	6%	-65%	-6%	-5%	0%	-13%
Servicio PISB	7,040	7,443	12,954	12,893	11,832	9,232	8,899	6%	74%	0%	-8%	-22%	-4%
Servicios de organización de eventos y otros		1,454	27		1,439	9,399	6,214		-98%	-100%		553%	-34%
Gastos Operativos	**-20,114**	**-26,993**	**-31,836**	**-30,070**	**-30,684**	**-36,211**	**-33,145**	**34%**	**18%**	**-6%**	**2%**	**18%**	**-8%**
Gastos de administración y de ventas	-20,322	-27,123	-31,823	-29,947	-30,175	-35,638	-32,701	33%	17%	-6%	1%	18%	-8%
Depreciación y amortización	-323	-358	-484	-546	-600	-577	-472	11%	35%	13%	10%	-4%	-18%
Otros ingresos, neto	531	488	472	424	92	5	28	-8%	-3%	-10%	-78%	-95%	513%
Ganancia (Pérdida) Operativa	**2,829**	**5,447**	**1,740**	**-1,117**	**-330**	**4,048**	**1,880**	**93%**	**-68%**	**-164%**	**-70%**	**-1328%**	**-54%**
Ingresos financieros	112	229	127	84	5	5	11	105%	-45%	-33%	-94%	-10%	129%
Gastos financieros			-3		-28	-47	-35			-100%		71%	-26%
Diferencia de cambio, neta	290	262	-344	-46	13	-39	-77	-10%	-231%	-87%	-128%	-406%	100%
Ganancia (Pérdida) Neta	**3,231**	**5,938**	**1,520**	**-1,078**	**-339**	**3,967**	**1,779**	**84%**	**-74%**	**-171%**	**-69%**	**-1270%**	**-55%**

	2011	2012	2013	2014	2015	2016	2017
Ingresos de actividades ordinarias	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**
Aportaciones	29%	42%	45%	33%	28%	28%	25%
Servicios de tecnologia	10%	8%	9%	14%	21%	20%	27%
Servicios de la unidad de ingenieria y mantenimiento	30%	23%	8%	8%	8%	6%	6%
Servicio PISB	31%	23%	39%	45%	39%	23%	25%
Servicios de organización de eventos y otros	0%	4%	0%	0%	5%	23%	18%
Gastos operativos	**-88%**	**-83%**	**-95%**	**-104%**	**-101%**	**-90%**	**-95%**
Gastos de administración y de ventas	-89%	-84%	-95%	-103%	-99%	-89%	-93%
Depreciación y amortización	-1%	-1%	-1%	-2%	-2%	-1%	-1%
Otros ingresos, neto	2%	2%	1%	1%	0%	0%	0%
Ganancia (pérdida) operativa	**12%**	**17%**	**5%**	**-4%**	**-1%**	**10%**	**5%**
Ingresos financieros	0%	1%	0%	0%	0%	0%	0%
Gastos financieros	0%	0%	0%	0%	0%	0%	0%
Diferencia de cambio, neta	1%	1%	-1%	0%	0%	0%	0%
Ganancia (pérdida) neta	**14%**	**18%**	**5%**	**-4%**	**-1%**	**10%**	**5%**

Fuente: ASBANC

3.8 Conclusiones

ASBANC al contar con un nuevo plan estratégico que demanda la generación de una mayor inclusión financiera y que permita el incremento de la legitimidad del sector requiere de un financiamiento que se logrará en mayor parte a través de la generación de nuevos servicios, por eso dentro de los servicios de seguridad electrónica se tiene una clara oportunidad para el desarrollo de un CSIRT financiero que permita mejorar la competitividad del sistema financiero y mejorar el ambiente de negocios.

CAPÍTULO IV. DESAFIOS DEL SECTOR

En este capítulo se brindará una perspectiva holística de la industria bancaria, pasando por un análisis de perspectivas a nivel mundial, análisis de rentabilidades, el tema reputacional y finalmente abordar las tendencias bancarias.

4.1 Perspectivas económicas a nivel mundial

De acuerdo con las cifras del Fondo Monetario Internacional, a abril de 2018, se prevé que el PBI a nivel mundial es de 3.9% para los años 2018 y 2019. A julio de 2018, las proyecciones no han cambiado.

Este crecimiento tendrá dos velocidades, las de las economías avanzadas, a un menor ritmo impulsadas por EE. UU. y un menor ritmo en la zona euro, liderada por Alemania. El empuje de la economía mundial se espera que provenga, según el FMI, de las economías emergentes en general y del Asia en desarrollo, en particular. A nivel de países, China seguirá liderando el crecimiento de los países en desarrollo y emergentes, pero una menor tasa que años pasados. En el 2017 el PBI fue de 6.9%, en 2018 se estima que será 6.6%. En el 2019 se espera sea 6.4%.

El crecimiento en un punto porcentual en Sudamérica, según el FMI, el alza de precios de las materias primas, que continúa brindando respaldo a los exportadores de la región, la baja en las perspectivas respecto de la edición de abril, refleja la complicación del panorama para las grandes economías, debido a la constricción de las condiciones financieras y el ajuste necesario de las políticas (Argentina); los persistentes efectos de las huelgas y la incertidumbre política (Brasil); y las tensiones comerciales y la prolongada incertidumbre que rodea la renegociación del TLCAN y el programa de políticas del nuevo gobierno (México). Las perspectivas de Venezuela, que está sufriendo un colapso drástico en la actividad y una crisis humanitaria (ver Tabla 3.1).

El FMI señala, que, si bien el pronóstico de base del crecimiento mundial se mantiene más o menos invariable, los riesgos ahora se inclinan a la baja a corto plazo y, tal como se pronosticó en abril de 2018, continúan sesgados a la baja a mediano plazo. Los riesgos a la baja son ahora más pronunciados, especialmente en torno a las posibilidades de medidas sostenidas y crecientes en el terreno del comercio exterior y de constricción de las condiciones financieras internacionales.

Las proyecciones que realiza el FMI para el Perú a mayo de 2018, fue de 3.7% y 4% para el 2019. Estas proyecciones difieren respecto al BCR, quien estimo a junio del 2018 que el PBI para los años 2018 y 2019 sería de 4.2%. A setiembre del presente año, ha existido una rectificación del estimado, para el 2018, se ha estimado que baje a 4%. "...[L}a composición del crecimiento ha cambiado respecto a las cifras presentadas en junio. Ahora el BCR ve menos impulso a la actividad por el lado fiscal, mientras el sector privado continúa dando señales de ser el principal motor de la recuperación." (Diario El Comercio, 2018)

Tabla 4.1: Proyección del producto mundial

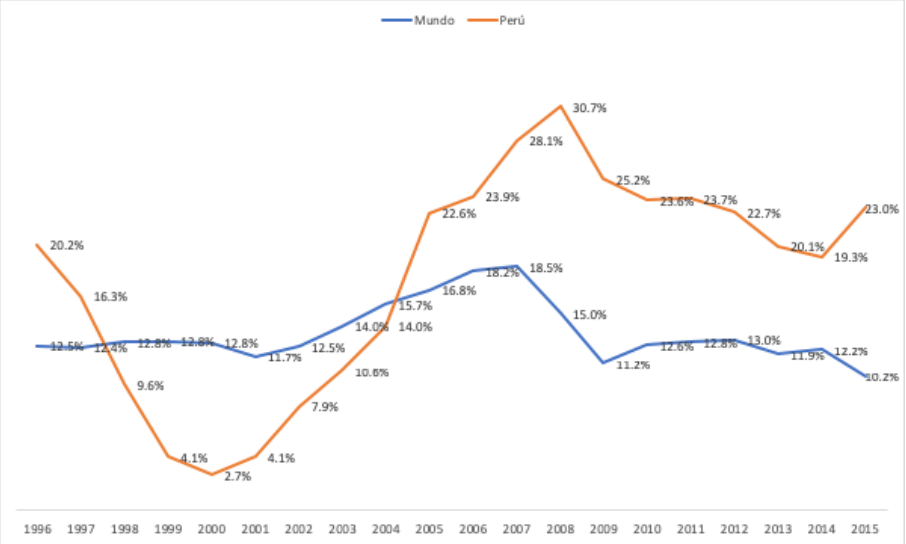
		Projections	
	2017	2018	2019
World Output	**3.8**	**3.9**	**3.9**
Europe	**3.0**	**2.7**	**2.3**
Advanced Europe	**2.4**	**2.3**	**2.0**
Euro Area[4,5]	2.3	2.4	2.0
Germany	2.5	2.5	2.0
France	1.8	2.1	2.0
Italy	1.5	1.5	1.1
Spain	3.1	2.8	2.2
Emerging and Developing Europe[6]	**5.8**	**4.3**	**3.7**
Asia	**5.7**	**5.6**	**5.6**
Advanced Asia	**2.4**	**2.1**	**1.9**
Japan	1.7	1.2	0.9
Korea	3.1	3.0	2.9
Australia	2.3	3.0	3.1
Emerging and Developing Asia	**6.5**	**6.5**	**6.6**
China	6.9	6.6	6.4
India[4]	6.7	7.4	7.8
North America	**2.3**	**2.8**	**2.6**
United States	2.3	2.9	2.7
Canada	3.0	2.1	2.0
Mexico	2.0	2.3	3.0
Puerto Rico[4]	–7.7	–3.6	–1.2
South America[5]	**0.7**	**1.7**	**2.5**
Brazil	1.0	2.3	2.5
Argentina	2.9	2.0	3.2
Colombia	1.8	2.7	3.3
Venezuela	–14.0	–15.0	–6.0
Chile	1.5	3.4	3.3
Peru	2.5	3.7	4.0
Ecuador	2.7	2.5	2.2
Bolivia	4.2	4.0	3.8
Uruguay	3.1	3.4	3.1
Paraguay	4.3	4.5	4.1

Fuente: FMI (2019)

4.2 El ROE bancario de los principales países americanos y europeos

El Return on Equity (ROE), es un indicador financiero que determina la rentabilidad del capital, mide el rendimiento que obtienen los accionistas de los fondos invertidos. A lo largo de los años el ROE del sistema bancario en el Perú ha estado por encima del ROE a nivel mundial. En el 2015 el ROE de los Bancos peruanos fue de 20.20%, siendo el promedio en el mundo de 10.23%. En la figura 4.1 se puede observar lo mencionado.

Figura 4.1: ROE de los Bancos a nivel mundial y Perú



Fuente: Stlouisfed.org (2019)

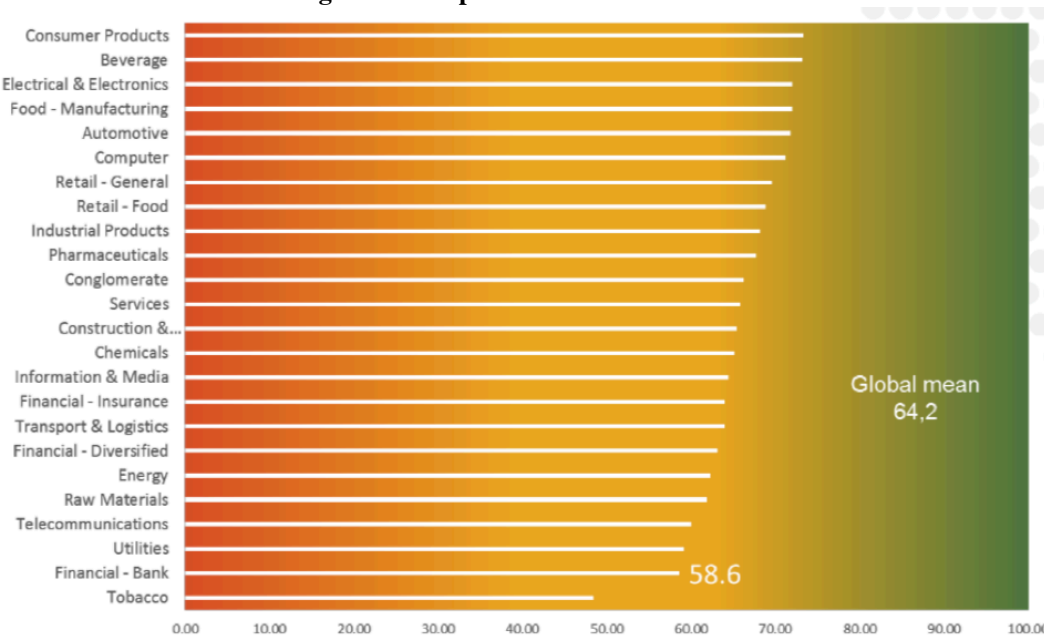
4.3 La reputación de la banca

La reputación corporativa se puede definir como una "representación colectiva de las acciones y resultados pasados de una empresa, que describen la capacidad de la empresa para entregar resultados valiosos a múltiples grupos relevantes (Reputation Institute, 2015), la reputación mejora la lealtad y la recomendación del cliente, puede también tener un impacto en la adquisición de nuevos clientes.

En un estudio realizada por RepTrak para evaluar la reputación de 25 industrias, se observa que el sector Financiero – Banca se encuentra en el penúltimo lugar de las

industrias analizadas, con un nivel de reputación de 58.6%, por debajo del promedio que es 64.2%, según se puede observar en la figura 4.2

Figura 4.2: Reputación de la Industria



Fuente: Reputation Institute (marzo 2015)

Según RepTrak, la reputación de la industria bancaria varía mucho. Países donde los bancos han recibido los puntajes más bajos de RepTrak® son España, Irlanda y Portugal, mientras que en Australia la reputación de la industria bancaria es la más alta, ver en la tabla 4.2

De acuerdo con esta fuente[1], al comparar los puntajes de la industria bancaria en 15 países, se observa que los países que tienen una reputación más baja son Portugal, Irlanda y España, países europeos que todavía están luchando para que la gente vuelva a trabajar después de que sufrieran la recesión. La tasa de desempleo aún persiste por encima del 10% en Irlanda, aproximadamente 14% en Portugal y 24% en España.

En el Perú la reputación de los bancos también se encuentra en penúltima posición respecto a las industrias analizadas y por debajo del promedio 61.2 puntos sobre 64.2

[1] Son siete las dimensiones analizadas por RepTrak: Productos y servicios, Innovación, Lugar de trabajo, Gobernanza, Ciudadanía, Liderazgo y Actuación. Las dimensiones RepTrak son la explicación racional de las conexiones emocionales. La gobernanza y los Productos /Servicios son los dos principales impulsores de la reputación en la industria bancaria mundial, seguidos por la Ciudadanía como el tercer conductor. La industria bancaria mundial tiene puntuaciones de reputación débiles en seis de las siete dimensiones analizadas.

que corresponde al promedio.

Tabla 4.2: RepTrak® promedio de la industria bancaria por país

Country	Industry Ranking Within Country	2014 RepTrak® Pulse
Australia	7 of 12	65.9
New Zealand	2 of 5	64.9
Canada	16 of 19	63.9
Brazil	12 of 18	63.8
South Africa	2 of 5	63.6
UK	20 of 21	63.3
USA	21 of 22	62.6
Peru	9 of 10	61.2
Sweden	3 of 4	61.1
Italy	14 of 15	60.2
Mexico	11 of 14	58.6
Denmark	11 of 12	55.2
Portugal	16 of 16	51.6
Ireland	17 of 17	47.6
Spain	20 of 20	45.7

Fuente: RepTrak (2018)

4.4 Tendencias de la banca

Según Deloitte (Deloitte, 2018), el presente año 2018 podría ser clave para acelerar la transformación de los bancos hacia instituciones tecnológicamente modernas y operativamente ágiles, para que puedan seguir siendo dominantes en un sistema en rápida evolución. Este cambio no es fácil ya que la mayoría de los bancos lidian con múltiples desafíos: Regulaciones complejas y divergentes, sistemas heredados, modelos y tecnologías disruptivas, nuevos competidores y, por último, pero no menos importante, una base de clientes con expectativas cada vez mayores. Deloitte identifica seis temas macro que deberían ser críticos para el crecimiento a largo plazo y cinco líneas de negocios para la banca, ambos frentes pueden ser observados en la figura 4.3.

Figura 4.3: Crecimiento a largo plazo y líneas de negocio

Fuente: Deloitte (2018)

Centricidad del cliente: El crecimiento de la industria solo será posible en centrarse en el cliente

Recalibración regulatoria: Se percibe al año 2018 como una oportunidad para modernizar el cumplimiento normativo y unir si los pilares creados para objetivos de cumplimiento individuales.

Administración de la Tecnología: Para que los bancos sean mas agiles, los CIO deben administrar su portafolio de activos tecnológicos para priorizar actividades que diferenciadoras. Los esfuerzos externos deben enfocarse en funciones genéricas con énfasis en la eficiencia de costos.

Mitigación del riesgo cibernético: El riesgo cibernético es una de las principales preocupaciones de los administradores de riesgos de los servicios financieros.

Fintech y grandes tecnologías: Continúan liderando la innovación en la industria bancaria al enfocarse mas en la experiencia del cliente.

Repensar la fuerza de trabajo: Los bancos deberían considerar repensar la estrategia de su fuerza de trabajo dada la evolución del trabajo, con una mayor automatización y una mayor diversidad en el grupo de trabajo.

Adicionalmente en el reporte presentado se identifican cinco líneas de negocios para la banca:

Banca Retail: Transición a una institución centrada en telefonía móvil y anclada digitalmente.

Banca Corporativa: Priorizar la experiencia del cliente, la tecnología y la orientación al mercado.

Pagos: Optar por proveedores exclusivos de soluciones tradicionales y digitales, y dejar los pagos a las otras fintech y otros.

Gestión de Patrimonio: Las unidades de gestión patrimonial de los bancos deberían centrarse en el cliente.

Mercado de Capitales: Adopción de tecnología líder para la diferenciación competitiva.

Según este reporte, el crecimiento sostenible a largo plazo en la industria bancaria parece solo posible si los bancos se centran en el cliente. Las organizaciones que no han pasado por la transformación centrada en el cliente han colapsado. Afortunadamente, la mayoría de los bancos parece haberse dado cuenta de que las Fintech en realidad puede ser una gran ayuda para servir a sus clientes, tanto a través de la emulación, como por colaboración. Las Fintech, con un foco de atención en el cliente, han demostrado que es posible cumplir, y posiblemente incluso superar, las expectativas del cliente. Pero la tecnología generalmente es solo parte de la solución. El objetivo central para la mayoría de los bancos es lograr agilidad organizacional, y para hacerlo deben considerar adoptar la innovación, administrar el talento de manera diferente, persiguiendo alianzas clave dentro de un sistema más amplio para diseñar y entregar soluciones para los clientes.

Son varias las tendencias a nivel tecnológico que existen, Capgemini identifica diez (10) tendencias tecnológicas, que se presentan a continuación. Es necesario que el personal responsable de ASBANC siempre realice una mirada prospectiva a estos temas, de manera de identificar y proponer los cambios tecnológicos que pueden ser utilizados en el sector bancario del país.

Tabla 4.3: Tendencias de la Banca

Tendencia 1:	**“**Los bancos están utilizando API abiertas para monetizar sus activos y datos digitales”
	Los bancos están colaborando o se están asociando con firmas de Fintech para crear un entorno que nutra la innovación y cumpla con las expectativas en constante evolución de los clientes.
Tendencia 2	**“**Los bancos están utilizando API abiertas para monetizar sus activos y datos digitales”
	Las API abiertas permiten a los bancos integrar sus productos y servicios con aplicaciones de terceros para ofrecer a los clientes una variedad de productos o servicios a través del sistema bancario y que también pueden monetizarse, en muchos casos
Tendencia 3	**“**Hay un cambio en el modelo comercial bancario donde los bancos actuarán como una plataforma para muchas firmas de Fintech”
	“Banks as a Platform” (BaaP) es un cambio completo en el modelo de negocio bancario, que vincula directamente a las Fintech con soluciones innovadoras, lo que les permite proporcionar una ventanilla única para los clientes
Tendencia 4	**“**Con el aumento de las amenazas cibernéticas los bancos están invirtiendo en sistemas de ciberseguridad”
	El aumento de la digitalización y la conectividad ha provocado un aumento en los incidentes de violaciones de datos, obligando a los bancos a fortalecer sus sistemas de seguridad.
Tendencia 5	Los bancos están adaptando cada vez más los servicios públicos en la nube, ya que proporcionan flexibilidad y agilidad.
Tendencia 6	Los bancos están probando la realidad aumentada para proporcionar una mejor experiencia del cliente. Los bancos están invirtiendo en realidad aumentada (AR), ya que les permitirá ofrecer soluciones integrales a los clientes y también brindará una oportunidad para que los bancos destaquen entre la multitud.
Tendencia 7	Los bancos están probando la realidad aumentada para proporcionar una mejor experiencia al cliente

	Los bancos están explorando aplicaciones de tecnología distribuida colaborativa, asociándose con startups o creando incubadoras y laboratorios de innovación.
Tendencia 8	Los bancos están considerando la banca cognitiva para proporcionar una ventaja sobre los competidores. La inteligencia artificial (IA) y la tecnología cognitiva permiten a los bancos acelerar sus iniciativas de digitalización y proporcionar productos y servicios específicos y personalizados.
Tendencia 9	Los bancos están buscando aumentar su eficiencia y productividad al invertir en la Automatización Robótica de Procesos. La automatización robótica de procesos (RPA) es una forma altamente eficiente de ayudar a los bancos a reducir los gastos de TI sin comprometer el aprovisionamiento de servicios.
Tendencia 10	Los bancos están utilizando herramientas de autenticación biométrica para combatir el robo de identidad y el fraude. La autenticación biométrica ayudará a los bancos a combatir el robo de identidad, hacer las transacciones más seguras y mejorar la experiencia del cliente.

Fuente: Capgemini (2017)
Elaboración Propia

4.5 Conclusiones

De lo anteriormente expuesto se detecta una oportunidad potencial en los temas de Ciberseguridad debido a que existen una creciente demanda por parte de los bancos alrededor del mundo de digitalizar sus procesos, lo que viene acompañado de un alto riesgo a los procesos de negocio ya que las amenazas cibernéticas vienen incrementándose desmesuradamente, dicha problemática será desarrollada en el siguiente capítulo.

CAPÍTULO V. EL MERCADO DE CIBERSEGURIDAD

En el presente capítulo se explorará la demanda y oferta de los servicios de ciberseguridad, dando una mirada hacia el futuro sobre los riesgos que se pronostican en los diferentes sectores de la industria, asimismo se explicará acerca de FIRST y su relación con esta estructura de defensa que se ha tenido que realizar para poder hacer frente a estas amenazas cibernéticas que perjudican a las organizaciones tanto económica como reputacionalmente.

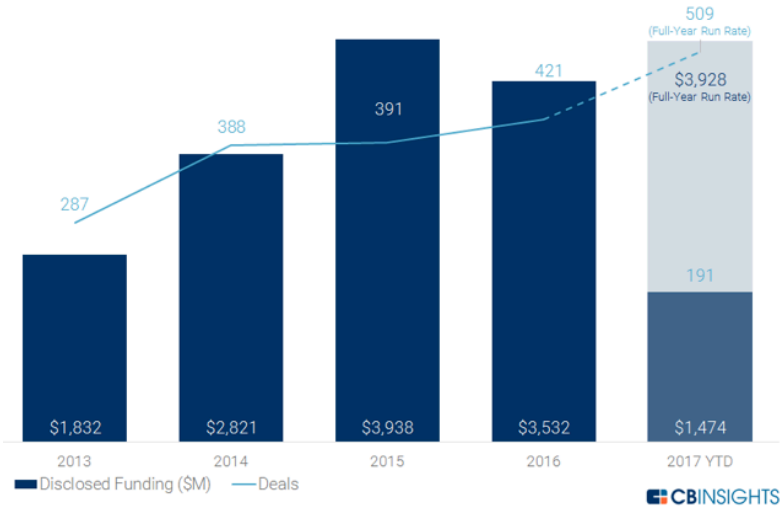
5.1 El mercado de Ciberseguridad

5.1.1 Demanda y tendencia mundial:

En 2017 (Gavilán, 2017), Gartner publicó un informe en la cual se indican que las amenazas dirigidas a las compañías de la **Industria TI** se han mantenido en un nivel elevado "Este sector es el más afectado en temas de ciberseguridad, ya que es el que registra los ataques más violentos", ha declarado al respecto **Neil Mac Donald, VP and distinguished analyst and Gartner Fellow Emeritus**.

El analista también ha explicado que las empresas deben proteger la entrada a las infraestructuras digitales de sus compañías, ya que cada vez los atacantes son más sofisticados. Por esta razón, es importante que quienes lideran dichas empresas evalúen las herramientas disponibles en ciberseguridad y elijan aquellas que proporcionen protección ante amenazas avanzadas, posibilitando una transformación digital más segura por parte de estas compañías, que les permitirá a su vez implementar tecnologías actuales en la nube, lo que se decantará en reducir los costes operacionales, asimismo Nasdaq (Nasdaq, 2018) en su reporte de Ciberseguridad del 2018 indica que las inversiones realizadas por parte de las firmas de riesgo desde el año 2013 han ido en crecimiento constante, cerrando el 2016 con $3.5 billones de dólares, como se observa en la figura 5.1

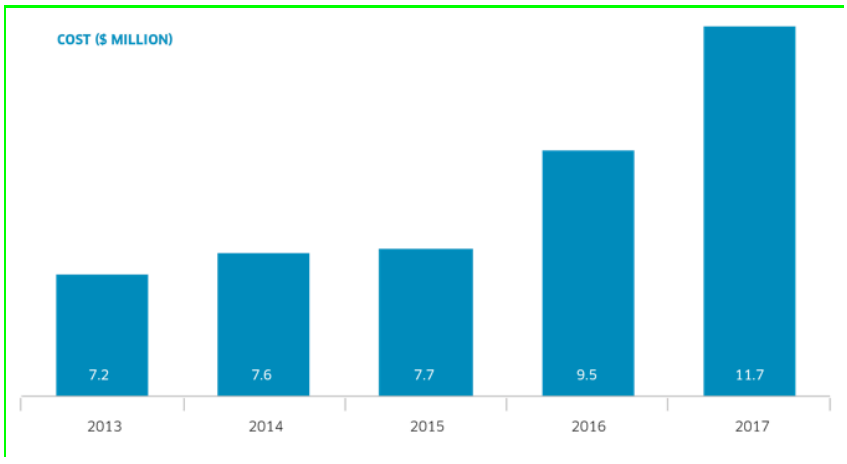
Figura 5.1: Inversiones en Ciberseguridad



Fuente: CBINSIGHTS (2017)

En ese sentido, el banco de inversión Morgan Stanley realizó una encuesta a los principales CIO de las principales corporaciones, donde la mayoría indico que tienen que adquirir al menos 15 tecnologías diferentes las mismas que se han ido en incremento desde el 2013 tal cual se puede observar en la figura 5.2, siendo esto una respuesta al alto grado de sofisticación de los ataques y se ha duplicado en los últimos cinco años.

Figura 5.2: Costo promedio global del Cibercrimen por Organización



Fuente: Morgan Stanley (2016)

Lo mismo es comentado por E&Y en su vigésima edición del Global Information Security Services (EY, 2018), en la que se indica que la mayoría de las empresas considera que el riesgo de sufrir un ciberataque hoy en día es mayor que hace un año, esto principalmente a que las técnicas empleadas por los Ciberdelincuentes son más

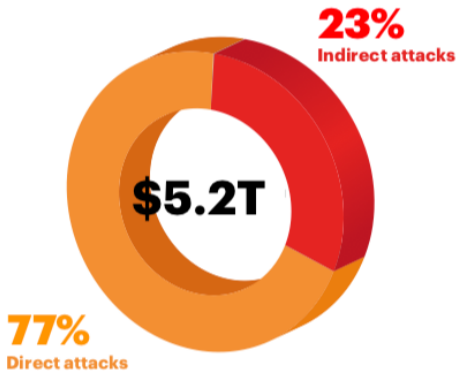
sofisticadas y las empresas están más hiperconectadas que nunca, tanto es así que en la figura 5.3 se puede visualizar esta tendencia respecto al aumento de las inversiones en este tema cada vez mayor, en dicha encuesta se muestra como resultado que el 59% afirma que su presupuesto de inversión ha aumentado en los últimos doce meses, 87% de ellos afirmaron que necesita inclusive hasta 50% más de presupuesto y un 12% espera un aumento de mas del 25% para el 2019.

Figura 5.3: Inversiones como protección frente a ciberataques

Fuente: E&Y (2018)

En el 2018 se realizo un estudio por Accenture (Accenture, 2018) cuyo titulo es Securing the Digital Economy: Reinventig the Internet for Trust, en ella se realizo una encuesta a más de 1,700 CEO y ejecutivos en todo el mundo arrojando una cifra alarmante, ya que las compañías podrían incurrir en costes por más de 5.2 trillones de dólares durante los próximos cinco años, como consecuencia de los ataques cibernéticos afectando la creación de oportunidades de valor desde la perspectiva de la economía digital.

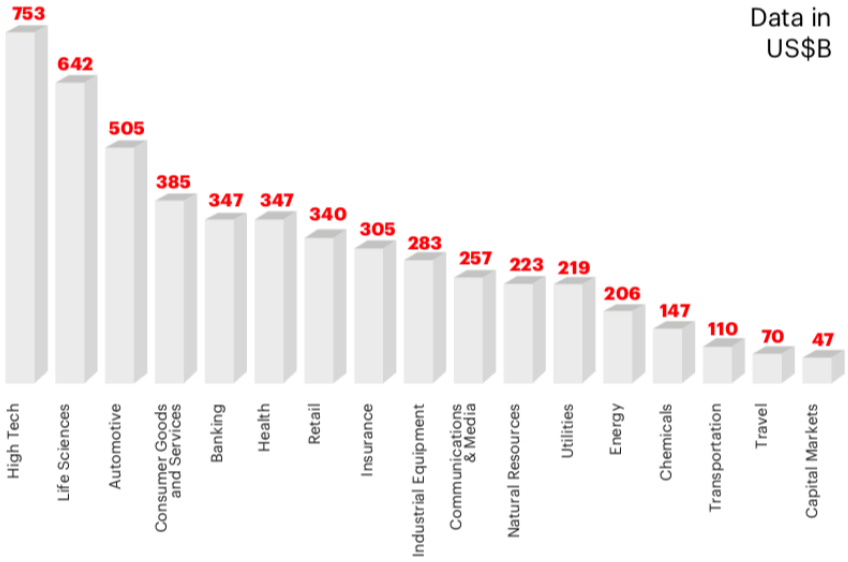
Figura 5.4: Perdida acumulada por ataques cibernéticos en los próximos cinco años



Fuente: Accenture (2018)

Complementando la información anterior, en la figura 5.5 se puede observar que existe un alto riesgo de los diferentes sectores, siendo la más afectada la industria de alta tecnología con un total en pérdidas proyectadas por 753 billones de dólares durante el periodo de 2019 a 2023, estando la banca en quinto lugar con 347 billones de dólares.

Figura 5.5: Valor del riesgo por Industria



Fuente: Accenture (2018)

5.1.2 Demanda y tendencia en Perú:

De acuerdo a un estudio[2] presentado por el fabricante de herramientas de seguridad Fortinet a nivel Perú, indica que la ciberseguridad no es la inversión más importante dentro de los presupuesto de los departamentos de TI, donde el 43% de las empresas o bien invierten de forma personalizada o la consideran como una inversión de baja prioridad, sin embargo este comportamiento no ocurre en otros mercados como el Chileno o Brasilero, en la figura 5.6 se puede observar que existe una tendencia a aumentar esta inversión al menos en un ritmo no menor al 10% anual y también una parte menor de los entrevistados considera la modalidad de Outsourcing como una alternativa interesante.

Figura 5.6: La Ciberseguridad en el Perú

Fuente: CIO Perú (2018)

E&Y su vigésima edición del Global Information Security Services (2018) también realizó una encuesta a los principales ejecutivos, que en la figura 5.8 se indica que esta tendencia al aumento de las inversiones es cada vez mayor, en dicha encuesta arrojó como resultado que el 47% afirma que su presupuesto de inversión ha aumentado en los últimos doce meses, 92% de ellos afirmaron que necesita inclusive hasta 50% más de presupuesto y un 3% espera un aumento de más del 25% para el 2019.

[2] El estudio solo considera información reportada por las empresas.

Figura 5.7: Inversiones como protección frente a ciberataques

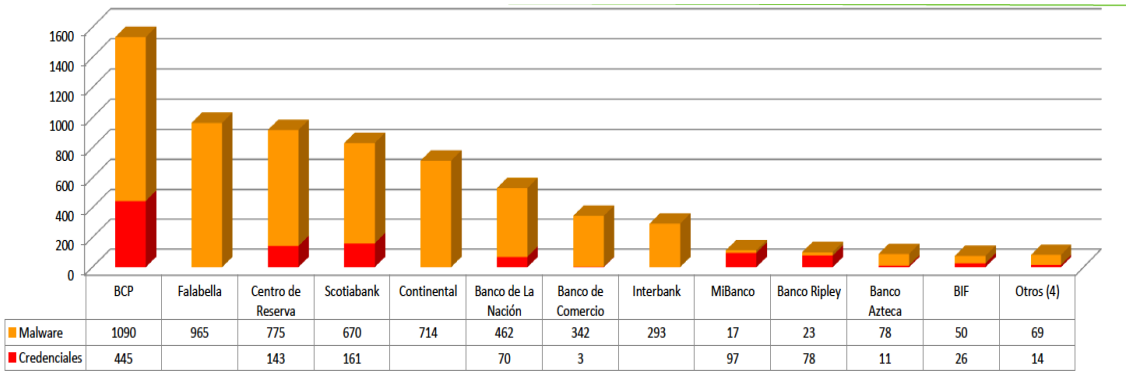
Fuente: E&Y (2018)

De acuerdo con lo indicado por Oscar Chávez Arrieta, vicepresidente de SOPHOS para América Latina (Gestión, 2018), menciona que, al no contar con barreras para detener el Cibercrimen, el Perú se ha vuelto un nicho para los hackers, ya que no se han adoptado las nuevas prácticas de ciberseguridad que existen en el mercado internacional, indicando que para el bicentenario el sector experimentará un crecimiento de hasta 220 millones de dólares.

5.1.3 Estimación de la demanda de servicios de Ciberseguridad en la banca peruana:

Ante un escenario poco alentador, ASBANC encargó la realización de un estudio a la empresa AIUKEN para que pueda realizar un escaneo de los bancos peruanos durante un periodo de 30 días, en febrero 2018, pudiendo encontrar un panorama crítico en los temas de ciberseguridad, como resultado del estudio se encontró 5,548 casos de malware bancario dirigido a robar credenciales, acceder remotamente a la infraestructura interna, extraer datos sensibles y/o manipular dominios web y 1,048 casos de contraseñas corporativas comprometidas que se obtuvieron de la Deep web o que se encuentran almacenadas en el centro de comando y control de Botnets tal como se puede ver en la figura 5.8 donde se muestra una situación general del gremio, como ejemplo se visualiza en la figura 5.9 el detalle del informe sobre lo encontrado en BCP y en la figura 5.10 el detalle de lo encontrado para banco Falabella.

Figura 5.8: Situación General

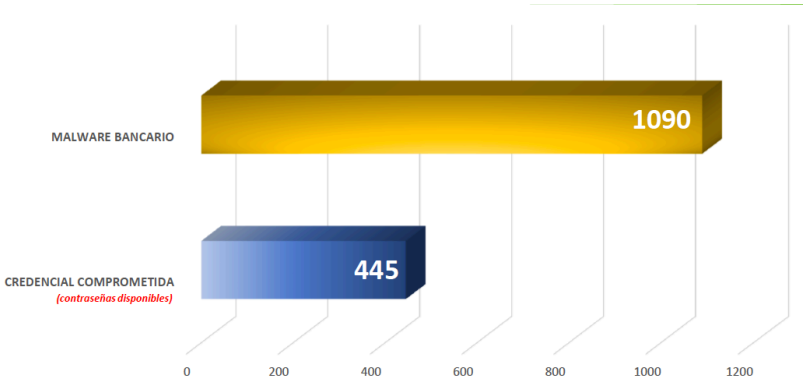


	BCP	Falabella	Centro de Reserva	Scotiabank	Continental	Banco de La Nación	Banco de Comercio	Interbank	MiBanco	Banco Ripley	Banco Azteca	BIF	Otros (4)
Malware	1090	965	775	670	714	462	342	293	17	23	78	50	69
Credenciales	445		143	161		70	3		97	78	11	26	14

Fuente: AIUKEN (2018)

Figura 5.9: Hallazgos BCP

del malware detectado en BCP está diseñado para robar credenciales de usuarios de banca online.



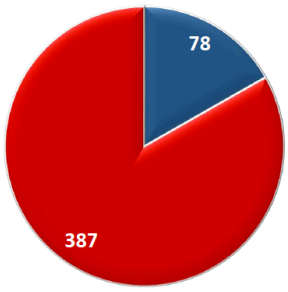
Fuente: AIUKEN (2018)

Figura 5.10: Hallazgos Banco Falabella

Credenciales Corporativas Comprometidas

Remote Access Trojan

Spyware & Malware Avanzado



PUA Troyanos javascript

El malware que afecta a esta entidad es está diseñado para robar credenciales de sus clientes de banca online, además de haber aplicaciones maliciosas que realizan operaciones sobre el dominio del Banco Falabella.

Fuente: AIUKEN (2018)

5.2 Oferta de servicios de Ciberseguridad

5.2.1 Principales servicios ofrecidos.

Para poder brindar un catálogo de servicios adecuado, ASBANC realizó un estudio a nivel macro con Apoyo Consultores con el objetivo de poder relevar quién podría cumplir el rol de aliado estratégico y cuáles serían los principales ofertas de servicio a nivel LATAM, el estudio relevó que entre los principales servicios de Ciberseguridad ofrecidos se encuentran Security Operation Center (SOC), Laboratorios de Inteligencia, Protección de datos, Protección de EndPoint y Auditoría, consultoría e información, la descripción de las mismas puede ser visualizada tabla 5.1 donde se brinda un mayor detalle.

Tabla 5.1: Principales Servicios de Ciberseguridad

Servicio	Descripción
SOC	Security operations center, es el lugar centralizado de donde se supervisa el sistema y el proceso de data
Laboratorios de inteligencia	Detección de vulnerabilidades a través de pruebas como el penetration test que te ayuda a simular ataques para identificar vulnerabilidades del sistema, constante monitoreo de sistema de seguridad para identificación de posibles ataques de Hackers
Protección de datos	Cifrado de datos, autenticación de identidades, recuperación de datos y prevención de fuga de datos
Protección de endpoints	Antivirus y herramientas que permitan bloquear la empresa ante cualquier amenaza externa a través de un end point
Auditoría consultoría e información	Servicios mediante los cuáles verifican operatividad del sistema y brindan recomendaciones de como mejorarlo

Fuente: Apoyo Consultores (2018)

5.2.2 Principales Proveedores con presencia en LATAM

En la tabla 5.2 se muestran las principales empresas de Ciberseguridad a nivel LATAM, entre ellas se selecciono a MNEMO y AIUKEN Cybersecurity para entrar en un proceso de evaluación final, por ello se contrató a un experto del sector[3] el cual realizó las evaluaciones correspondientes en función de las siguientes variables: Certificaciones de calidad, asociación, experiencia, plan de trabajo presentado, precios del servicio y metodología de trabajo, para que se permita comparar las propuestas enviadas por ambos postores y determinar el valor correspondientes de cada una, quedando como ganador del proceso la empresa española AIUKEN Cybersecurity.

[3] Ver Anexo IX

Tabla 5.2: Principales Empresas de Ciberseguridad con presencia en LATAM

Empresa	HQ	Presencia en LatAm	Servicios relacionados a ciberseguridad				
			SOC	Lab de inteligencia	Protección de datos	Protección de endpoint	Auditoría, consultoría y formación
MNEMO		México y Colombia	x	x	x	x	x
Ajuken Cybersecurity		Chile	x	x	x	x	x
ARBOR NETWORKS		-	x		x	x	
enHacke		Perú		x			x
SOPHOS		LatAm	x	x	x	x	x
DIGIWARE		Colombia	x		x	x	x

Fuente: Apoyo Consultores (2018)

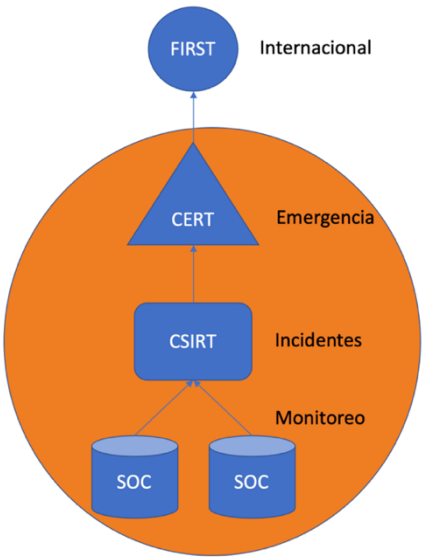
En ese sentido luego de la evaluación realizada, se firmo un contrato entre la española AIUKEN Cybersecurity y ASBANC, donde ASBANC proveía la parte comercial y AIUKEN la parte tecnológica ambas partes acordaban ser socios estratégicos que les permita atender a todo el sistema financiero, los términos de ambas partes se encuentran en el Anexo X donde se detalla los alcances y responsabilidades de cada una de las partes.

5.3 Relación entre FIRST, CERT y CSIRT

Existe una lógica de nivel jerárquico entre Fórum of Incident Response and Security Teams (FIRST) y los Computer Security Incident Response Team (CSIRT), donde FIRST es una Foro internacional que permite que se manejen cooperativamente los incidentes de seguridad informática que afectan las infraestructuras críticas, nuevas vulnerabilidades o ataques de amplio espectro, en ese sentido FIRST promueve programas de prevención a nivel mundial, luego dentro de la cadena existen los Computer Emergengy Response Team (CERT) que son las entidades autorizadas por cada país de poder responder a las emergencias que puedan ocurrir y que afecten a la sociedad de ataques informáticos, luego se encuentra los CSIRT que son los equipos de respuesta ante incidentes, de este último pueden existir varios por país y pueden ser

públicas o privadas y finalmente estas atienden a varias empresas y/o entidades financieras a través de los Security Operation Center (SOC) que son las encargadas de monitorear a nivel de detalle todos los eventos cibernéticos que pudieran ocurrir dentro de una entidad, todo este nivel jerárquico puede observarse en la figura 5.11, donde ASBANC busca implementar un CSIRT que permita monitorear sectorialmente a todos los asociados con el objetivo de poder crear un frente único para la protección cibernética compartiendo información actualizada y en tiempo real sobre estos incidentes que vienen afectando el normal desempeño de las operaciones financieras.

Figura 5.11: Niveles Jerárquicos de un CSIRT



Fuente: Autor de la tesis

5.4 Conclusiones

De lo anteriormente expuesto se puede afirmar que el tema de Ciberseguridad debe de considerar múltiples aspectos, no solo esta relacionado al tema tecnológico sino lo que conlleva un entendimiento de todas las partes involucradas dentro del proceso, es por ello que se ha podido observar que las inversiones en este tema han estado incrementándose de manera sostenible, dicho asunto debe ser tratado a todo nivel dentro de una organización ya que el tema de seguridad cibernética se ha convertido en un tema estratégico que debe ser abordado con la debida prioridad.

VI. EL SERVICIO – CSIRT

En el presente capítulo se busca explicar los servicios ofrecidos por la empresa AIUKEN, multinacional especializada en brindar servicios de Ciberseguridad, cuya matriz se encuentra en Madrid, España con presencia en Medio Oriente, Europa, África y América del Sur con una facturación anual por encima de los € 4MM cuenta con las certificaciones ISO 27001, FIRST, APWG y LEET Security, siendo un factor sumamente importante el tema de la Inteligencia Artificial que le añaden a sus procesos de detección permitiéndole obtener eficiencias operacionales de los servicios ofrecidos y con la cual ASBANC luego de realizar las evaluaciones correspondientes firmaría una alianza comercial para poder comercializar sus servicios.

6.1 ¿Qué es un CSIRT?

Las siglas CSIRT hacen referencia a equipo de respuesta ante incidentes de seguridad informática o conocido también por sus siglas en ingles como Computer Security Incident Response Team, el objetivo de este servicio es poder frenar en tiempo real los ataques cibernéticos que mediante operaciones complejas hacen que las empresas se encuentren expuestas, por ello un CSIRT debe cumplir con una lista de servicios de los cuáles debe estar incorporado dentro de su portafolio de servicios.

ASBANC cuenta con una plataforma de Telecomunicaciones denominada Bancared[4] que es una red desplegada en fibra óptica que opera bajo el protocolo MPLS (Multiprotocol Label Switching) la misma que facilita a todas las entidades financieras se encuentren interconectadas en tiempo real, en ese sentido sobre dicha red permite que se instalen diferentes tipos servicios y de inmediato este se encontraría disponible por parte de los bancos u asociados para poder ser utilizados, para instalar dicho servicio se tendría que configurar que la plataforma de comunicaciones Bancared se conecte con la sede central de AIUKEN en Barcelona o Madrid con el objetivo de poder tener conexión con Delfos que es la plataforma de inteligencia artificial entrenada por expertos de Ciberseguridad durante 4 años, lo que repercute en una reducción de los costos de detección y monitoreo se puedan disminuir a la quinta parte frente a otros proveedores que ofrecen el mismo servicio como se pudo observar en la tabla 5.2 donde se mostraban las principales empresas de Ciberseguridad.

[4] Ver Figura 6.1

Figura 6.1: Estructura lógica de BANCARED

Fuente: Autor de la tesis

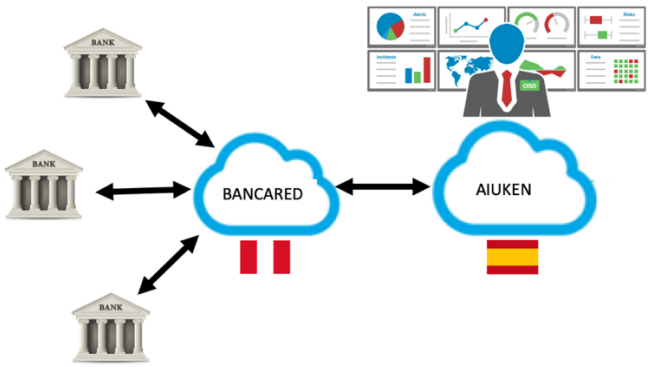
El objetivo de implementar un CSIRT sobre la infraestructura de BANCARED es que permita que cada uno de los asociados de ASBANC puedan acceder a al catálogo inicial de servicios y que forman parte de la lista mostrada en la tabla 6.1 de forma remota hacia los datacenter en España donde se encuentra toda la infraestructura tecnológica y los centros de atención 24x7, por ello se establecerá un canal de comunicaciones dedicado a través de dos fibras ópticas de 100 MB entre España y Perú para poder brindar los diferentes servicios, la topología de la solución se puede visualizar en la figura 6.2

Tabla 6.1: Servicios Ofrecidos por CSIRT

1. Gestión de Incidentes
2. Análisis
3. Protección de la Información
4. Toma de Conciencia del entorno
5. Divulgación y Comunicaciones
6. Capacitación
7. Investigación / Desarrollo

Fuente: First.org
Elaboración: Propia

Figura 6.2: Estructura lógica del servicio



Fuente: Autor de la tesis

6.2 Descripción de los servicios del CSIRT

De acuerdo con los servicios ofrecidos por un CSIRT entre los más demandados se encuentran la gestión de incidentes, el análisis y la protección de la información, por ello, se considera la realización de una alianza comercial con un proveedor internacional cuya propuesta de valor sea brindar un amplio portafolio de servicios de Ciberseguridad.

En vista de ello se ofrecería los servicios de acuerdo a la necesidad específica de cada cliente, comenzando con un catálogo inicial de 10 servicios como parte de la oferta de servicio SasS[5], en la misma se establece que la forma de entrega con cada institución financiera sea a través de BANCARED, en ese sentido las actividades claves principalmente radicarían en la alerta temprana de amenazas, vulnerabilidades y la gestión de medidas preventivas/reactivas ante incidentes de seguridad informática que pudieran ocurrir en otras partes del orbe, el proveedor elegido para realizar dicha alianza fue la multinacional AIUKEN Cybersecurity el mismo que cuenta con una serie de servicios que por fines didácticos se ha categorizado en cuatro grupos:

[5] SaaS: software as a Service es un modelo de distribución de software donde el soporte lógico y los datos que maneja se alojan en servidores de una compañía de tecnologías de información y comunicación (TIC), a los que se accede vía Internet desde un cliente.

6.2.1 Servicio Base:

6.2.1.1 MSS - Managed Security Services:

Servicio orientado a proporcionar los procedimientos, servicios profesionales y conocimiento necesario para defender a la organización del cliente frente a riesgos y amenazas criticas de seguridad sobre la infraestructura TIC. El servicio entrega un equipo multi-disciplinar de recursos para ejercicios de respuesta ante incidentes de seguridad orientado a mitigar riesgos tecnológicos, dicho MSS incluye la conexión a un CSIRT que es un servicio de alerta que se encuentra conectado a FIRST para poder hacer frente a los incidentes de Ciberseguridad.

6.2.2 Soluciones Avanzadas

6.2.2.1 eBanking Security Services:

Detección, análisis y mitigación de ataques provocados por troyanos, phishing y abusos de marca. Servicio de protección de portales de home banking orientado a la defensa de la integridad e identidad de los clientes de la entidad, además de proteger infraestructura bancaria. Evita la manipulación de flujos de datos originados por malware.

6.2.2.2 Gestión de Ingeniería Social:

Servicio para generar conciencia entre usuarios internos y externos sobre amenazas de ingeniería social. Permite el despliegue de ataques controlados por medio de diversos vectores (correo, web, redes sociales, mensajería instantánea, entre otros), medir el comportamiento de los usuarios ante los ataques, ofrecer retroalimentación instantánea a usuarios que cometen errores, y capacitar a los mismos con contenidos personalizados.

6.2.3 Consultorías

6.2.3.1 Cyber Security Consulting Services:

Servicios profesionales que proporcionan experiencia en consultorías de seguridad de alto valor para ayudar al cliente a prepararse y alinearse al cumplimiento normativo, y a protegerse contra ataques y amenazas tecnológicas, además de facilitar una firme adherencia a la innovación operacional en materia de Ciberseguridad.

6.2.3.2 Cyber Security Assessment Consulting:

El servicio está orientado a la clasificación y análisis de activos críticos y de valor desde una perspectiva de seguridad para evaluar el nivel de exposición de riesgos e impacto de los diferentes activos de la organización, abarca ejercicios de auditoría, evaluación y test de la postura de seguridad de la organización.

6.2.4 Auditoria y Testing

6.2.4.1 Ethical Hacking Professional Services:

El servicio tiene como objetivo proveer al cliente de servicios profesionales para la ejecución de auditorías de seguridad sobre activos de información, desde un punto de vista metodológico, partiendo de los marcos de referencia aplicables a la organización y planes de auditoría sistemáticos. El servicio se apoya en algunas tecnologías propias para ejercicios de test de intrusión.

6.2.4.2 Pentesting Services:

El servicio tiene como objetivo proveer al cliente de servicios profesionales y herramientas automatizadas de intrusión para la ejecución de evaluaciones de seguridad sobre activos de información, desde un punto de vista metodológico, partiendo de los marcos de referencia aplicables a la organización y planes de auditoria sistemáticos.

6.2.4.3 Security Code Review:

Servicio orientado al análisis de código fuente estático para la detección y clasificación de vulnerabilidades, debilidades e inconsistencias en el código escrito durante las fases de desarrollo de la aplicación, facilita la remediación o corrección antes del paso a producción eliminando los riesgos de seguridad.

6.2.4.4 Vulnerability Assessment Services:

Servicio integrado por recursos profesionales para administración de tecnologías especificas para la ejecución de ejercicios automatizados de intrusión sobre infraestructuras TIC del cliente.

6.3 Modelo de negocio:

Se plantea que ASBANC apoye a sus asociados en la construcción de una solución cibernética que les permita lograr economías de escala y lograr sinergias entre todos, para ello se realizará una búsqueda a nivel LATAM de la mejor propuesta de servicio, con el objetivo de negociar con ellos la realización de una alianza estratégica de largo plazo, en donde ASBANC proporcioné el acceso mediante las relaciones que mantiene con los bancos, facilitando la llegada a los tomadores de decisiones, en ese sentido ASBANC se desempeñara como un intermediario comercial o canal de comercialización de la empresa que se seleccione para brindar este servicio, la empresa internacional proporcionará su experiencia profesional y su tecnología que permita atender las necesidades de protección cibernética operando directamente con los clientes, dentro del marco de negociación ASBANC será quien lleve la relación contractual con cada banco por cada servicio comercializado, y se encargará de los diferentes procesos administrativos como la cobranza, el pago, entre otros. Cabe precisar que el precio de venta es fijado por ASBANC a sus asociados tomando en cuenta el esquema de costos fijos que se negociaron con el socio de negocio, en ese sentido es muy importante señalar que entre los beneficios que se esperan lograr es diluir tanto los esfuerzos de lado del aliado estratégico como de ASBANC, para que este esquema funcione técnicamente se utilizará la infraestructura de la empresa internacional CenturyLink donde se establecerá el enlace con la sede remota del proveedor, dicha infraestructura sería la cabecera del servicio, en la figura 6.3 se puede observar cada una de los componentes del modelo de negocio para este servicio bajo la metodología de Canvas, por ello se detalla a continuación cada una de las partes que lo describen:

Segmento de Clientes: Los clientes primarios dentro del mercado meta son los jefes y gerentes de seguridad de los bancos asociados a ASBANC.

Propuesta de Valor: Plataforma de Ciberseguridad que tiene capacidades de Inteligencia Artificial que permite detectar oportunamente y a un menor costo cualquier amenaza cibernética que tenga identificado dentro de su catálogo.

Canales de distribución: Se atenderán a los clientes a través de un canal directo haciendo uso de la fuerza de ventas.

Relaciones con el cliente: Servicio personalizado de atención exclusiva a través de una venta consultiva que permite relevar a detalle todos los inconvenientes que surgen.

Flujos de Ingreso: El ingreso será por servicio en función del trafico cursado en GB por cada uno de los servicios adquiridos por parte del banco, donde ASBANC tiene un Revenue entre 10 al 25%.

Recursos Clave: Sistema DELFOS, servicios tecnológicos de Century Link, consultor preventa especializado en los temas de Ciberseguridad, personal de sistemas ASBANC, personal de redes y comunicaciones.

Actividades Clave: Preventa ya que se necesita identificar de manera muy precisa la tipología de amenazas y vulnerabilidades cibernéticas que pudiera existir.

Asociaciones Clave: se tiene una relación comercial con Grupo Microsistemas que es el canal oficial de LATAM para AIUKEN Cybersecurity y también con la empresa Century Link quien provee la Infraestructura para poder alojar los servicios que se vayan comercializando bajo la figura on-premise.

Estructura de Costos: Se presenta dos tipos de costos, en la cual se incurriría para brindar el servicio, los variables compuestos por la comisión de ventas, los estudios de prefactibilidad y los fijos compuestos por los pagos mensuales que se deben de realizar por los servicios ofertados en el catalogo

Figura 6.3: Modelo Negocio Canvas

Fuente: Osterwalder (2010)

6.4 Conclusiones

De lo anteriormente expuesto se puede determinar que dentro del catálogo de servicios ofrecidos se tiene los servicios de consultoría, servicios de auditoria y testing, soluciones de monitoreo avanzado, sobre la base de un servicio base que permitirá tener identificado todas las amenazas que pudieran ocurrir dentro del banco.

Sin embargo, todo ello no seria posible sin tener la infraestructura de telecomunicaciones denominada BANCARED, que permitirá lograr que los servicios puedan ser centralizados para todos sus miembros con lo cual se logra la eficacia esperada en estos temas.

CAPÍTULO VII. ESTUDIO DE MERCADO

Se busca estimar la demanda respecto a la implementación de un CSIRT financiero, por ello se aplicará una metodología que permita analizar los puntos de dolor más relevantes del mercado meta primario, la labor de campo del estudio realizado tiene la particularidad de llegar al 50% de la población objetivo, asimismo se realizará entrevistas a autoridades en la materia que permita brindar una perspectiva global del tema.

7.1 Objetivos, limitaciones y planteamiento del estudio de mercado

7.1.1 Objetivos Generales:

- Estimar la demanda de un nuevo servicio integral de ciberseguridad

7.1.2 Objetivos Específicos:

- Identificar si han tenido inconveniente de incidentes de seguridad informática.
- Identificar qué servicios de seguridad informática tienen
- Conocer que servicios necesitan en su empresa
- Identificar las ventajas y desventajas de no contar con el servicio de ciberseguridad
- Evaluar la aceptación del servicio de ciberseguridad
- Identificar la intención de uso del servicio de seguridad
- Verificación mediante el uso de fuentes secundarias

7.2 Metodología y planteamiento de la investigación

La metodología de investigación realizada permite detectar oportunidades dentro del mercado meta primario utilizando la técnica del focus group, ya que el sector se encuentra concentrado en cuatro bancos (BCP, BBVA, INTERBANK y SCOTIABANK), por ello se pretende determinar una oportunidad de mercado dentro de los bancos pequeños y medianos, por ello se realizará entrevistas a los oficiales de seguridad de la información de los siguientes bancos: Banco Falabella, Banco Ripley,

Banco Interbank, Banco GNB, Banco Cencosud y Banco Azteca, al ser tan pocos participantes dentro del sistema financiero, la muestra a la cual se esta entrevistando es más que representativa, y para poder dar forma a dicha oportunidad se realizará una entrevista en profundidad a la directora de nuevos negocios de Asobancaria quien ha implementado una plataforma de ciberseguridad en Colombia y al Superintendente de tecnología de la SBS para ver los aspectos regulatorios relacionados a los temas de ciberseguridad.

7.3 Investigación cualitativa mediante focus group

A continuación, se presenta la ficha metodológica que resume la ejecución del focus group, en la cual se indica todas las partes

Tabla 7.1: Ficha Metodológica

Técnica	Cualitativa, a través de focus group
Público Objetivo	Oficiales, analistas y jefe de gobierno de control de los bancos.
Número de participantes	06 participantes
Reclutamiento	Realizado por ASBANC
Instrumento	Para la recolección de información se uso una guía de pautas[6].

Fuente: Autor de la tesis

[6] Ver Anexo I

7.3.1 Análisis de Resultados

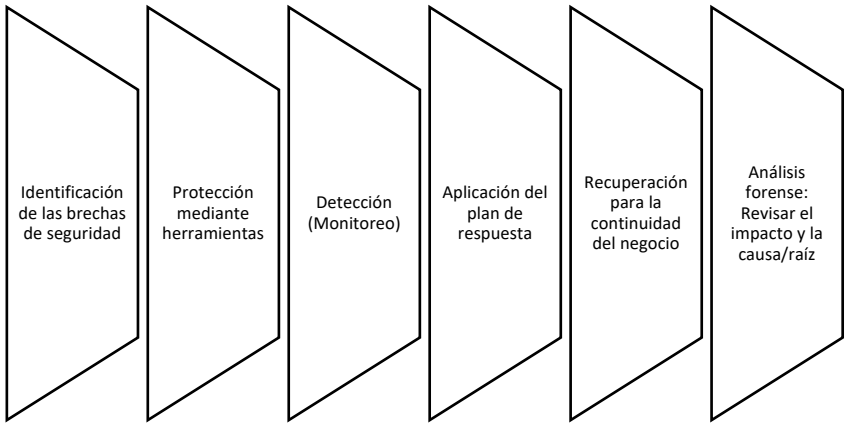
7.3.1.1 Sobre la Ciberseguridad

A los participantes se les plantearon cinco grandes preguntas siendo el resultado el siguiente:

¿Sienten que hay una cultura preventiva?

- En general, perciben que no hay concientización en las organizaciones acerca de los riesgos y consecuencias de los Ciberataques.
- Comentan que esta situación se presenta a pesar de contar con planes de capacitación a los usuarios (Trimestral, semestral y anual) y monitoreos continuos, por lo que sienten que estas actividades son insuficientes.
- Esta actitud indiferente se percibe a través de las diversas posiciones jerárquicas del banco. En algunos casos indican que presentan dificultad para coordinar entre áreas (IT).
- En general ¿Qué conocen de los ciberataques?
- Se presenta mayor conocimiento a nivel teórico (Conceptos) pues de manera práctica no intervienen con la frecuencia deseada a pesar del incremento de los ataques, así como la sofisticación de estos en los últimos años.
- ¿Qué hacen cuando se les presenta el día cero?
- La consulta de fuentes
- Las páginas web podrían ser usadas para determinar el tipo de ataque, su origen, la forma de administrarlo y de evitar su propagación. El uso de este medio sería en el caso de personal con poco conocimiento y recursos.
- Comunidades virtuales de seguridad con personas que por lo general tienen conocimientos básicos o del mismo nivel. Sería usado principalmente como un medio informativo más no para encontrar soluciones.
- Manuales o Procedimientos

Figura 7.1: Pasos para el resguardo de la seguridad Informática



Fuente: Autor de la tesis

¿Y sienten que cuentan con los recursos necesarios?

- La mayoría siente que no cuenta con los recursos necesarios para prevenir y defenderse antes los problemas de seguridad de la información, los que en su mayoría son ataques a nivel internos (No internacionales)

A nivel Interno:

¿Que sienten que les falta?

- Concientización a nivel de usuarios para disminuir los riesgos a los ataques.
- Programas especializados para problemas de cyberseguridad por ejemplo SOC. (muy pocos cuentan con esa herramienta. Entre ellos, el banco Interbank)
- Oportunidad de asistir a capacitaciones o conferencias referentes a temas de seguridad.

A nivel Externo:

- Productos ajustados a la realidad de sus problemas: Ataques internos y no provenientes del extranjero (en la mayoría de los casos)
- Falta de orientación por parte de los proveedores, pues se percibe que solo se preocupan por concretar la venta más no por resolver dudas o compartir conocimientos. Esto genera desconfianza hacia el proveedor

- Personal especializado y con experiencia en temas de seguridad de la información. No sólo conocimientos teóricos, sino principalmente a nivel de implementación.
- Comunidades con asesores externos que puedan brindar soporte ante consultas o dudas.
- Falta de oferta académica que incluya propuestas prácticas a nivel de implementación.

7.3.1.2 Experiencias con la Ciberseguridad

En los últimos años se ha dado un incremento significativo en la cantidad y nivel de sofisticación de los ataques cibernéticos, en consecuencia, se dan ataques en vulnerabilidades que antes lo hackers no detectaban fácilmente.

Los rápidos avances tecnológicos hacen que toda implementación de seguridad informática posea algún grado de vulnerabilidad, algunos en pequeña escala, otros en grandes proporciones, Por tanto, varios declaran que ninguna entidad tiene un nivel seguridad ideal.

7.3.1.3 Principales Necesidades Identificadas:

Del focus realizado se pudieron recoger las siguientes necesidades de los potenciales servicios que se podría brindar, por ello se ha clasificado en tres grandes tipos:

Servicios Reactivos:

- Alertas y advertencias
- Tratamiento de incidentes
- Análisis de incidentes
- Apoyo a la respuesta a incidentes
- Coordinación de la respuesta a incidentes
- Respuesta a incidentes in situ

Servicios Proactivos

- Comunicados
- Observatorio de tecnología
- Desarrollo de herramientas de seguridad

- Servicios de detección de intrusos
- Difusión de información relacionada con la seguridad

Manejo de Instancias:

- Análisis de solicitudes
- Respuesta a las solicitudes
- Coordinación de la respuesta a las Solicitudes

Gestión de la Calidad de la Seguridad

- Análisis de riesgos
- Consultoría de seguridad
- Sensibilización
- Educación / Formación

7.4 Investigación de fuentes primarias

7.4.1 Asobancaria:

En junio del 2018, la Asobancaria lanzó el primer CSIRT financiero, ya que buscaba atender a los bancos del sector financiero en temas de incidentes cibernéticos como los que ocurren en los temas de ATM, POS, Phishing, Pharming, entre otros, para hacer frente a estos temas realizaron una alianza estratégica con la empresa MNEMO (El Economista, 2018), esta empresa es una multinacional especializada en dar servicios de ciberseguridad al sector financiero, su centro de operaciones se encuentra en México y es dueña de uno de los cuatro equipos de respuesta en ciberseguridad certificados por FIRST en el país.

Por ello se realizo una entrevista a la doctora Ángela Vaca[7], que es la directora de nuevos negocios de la Asobancaria , quien comento que se vienen trabajando estos temas de forma gremial, ya que los riesgos vienen aumentando día tras día haciendo mención que los mayores riesgos lo encuentran en la parte de ciberseguridad

[7] Ver Anexo IV

sobrepasando al tema de delitos informáticos y de fraude, esto principalmente se debe a la evolución que ha tenido la banca en los temas de transformación digital y esta nueva línea de negocios ha traído nuevos riesgos, es por ello que desde Asobancaria se hace un seguimiento de cómo evoluciona las transacciones financieras, sobre todo ahora que más de la mitad de ellas se ejecuta vía internet y/o a través de medios electrónicos, cayendo cada vez cae más en desuso el tema de las oficinas físicas generando nuevos riesgos asociados a la operativa bancaria, es por ello que ya se tenía este proyecto en mente desde hace cuatro años, la importancia de contar con un centro de respuesta ante incidentes es sumamente importante y va teniendo vital importancia en el desarrollo de los negocios realizados por los bancos colombianos, sobre todo al ser una tendencia internacional el contar con una protección sectorial, tanto es así que ya se han suscrito al servicio 15 bancos de los 23 en menos de un año.

La ventaja que ofrece Asobancaria es que al ser parte del gremio, no lo perciben como un proveedor de servicios sino como alguien neutral a quien pueden entregarle una información, siendo más sencillo que el banco entregue a una entidad gremial que no tiene ningún interés particular, sino que es de preocupación de todos ya que la información que ellos entregan la realizan bajo un marco de colaboración y confianza que permite que tengan las mejores herramientas para la toma de decisiones y luego poder anticiparse ante los ataques o riesgos cibernéticos que sucedan dentro de los asociados, es por ello que se han dimensionado cuatro servicios principales que ofrecerá Mnemo: Servicio de Inteligencia de amenazas externas, Servicio de gestión de respuesta ante incidentes externos, Observatorio de seguridad para el Sector financiero y Servicios complementarios.

En la entrevista también se hizo mención que existe un tema regulatorio acerca de los CSIRT sectoriales en el CONPES 3854-2016 en la cual se establecen los lineamientos para los temas de ciberseguridad, dicha regulación facilito la implementación de este CSIRT.

7.4.2 Aspecto Regulatorio:

Para poder abordar los temas regulatorios en el Perú acerca del CSIRT, se realizó una entrevista al señor Magno Condori[8], Intendente de Supervisión de Sistemas de Información y Tecnología de la SBS para explorar si existe alguna normativa específica sobre el tema de Ciberseguridad que los bancos tengan que cumplir y poder gestionar el riesgo al cual se ven expuestos, este indico que no existe una normativa especifica a la fecha sin embargo parte de este tema se recoge en la circular G140-2009 en la cual se establece el marco normativo de seguridad de la información que las empresas deben de cumplir haciendo referencia por empresas a los bancos, financieras, cajas, aseguradoras y AFP, también mencionó que existen otras normas relacionadas al tema de ciberseguridad como la resolución 272-2017 en el cual se establece el reglamento de gobierno corporativo y gestión integral del riesgo, allí se establece que el proceso de gestión de riesgos es responsabilidad del directorio, la gerencia y las diversas unidades haciendo hincapié que estos entes son los responsables de hacerse cargo de identificar el riesgo al que se expone el negocio y su gestión, en ese reglamento se indica los riesgos de crédito, los riesgos de mercado y los riesgos operacionales, pero también menciona que esa lista no es limitativa, eso quiere decir que en verdad la regulación puede no necesitar que se especifique el riesgo de ciberseguridad, pero al ser un riesgo al que esta expuesto el negocio bancario las entidades sin necesidad de la existencia de una regulación especifica hoy en día deberían tomar medidas al respecto sobre el riesgo de ciberseguridad.

Es por ello que viendo que todavía existen muchas brechas por cerrar, la SBS si va a sacar una regulación especifica en el tema de ciberseguridad en ella se establecerán los requisitos mínimos dentro de la gestión de riesgos, es por ello que en el plan operativo de la Superintendencia 2019 se tiene como objetivo implementar una plataforma de ciberseguridad para monitorear la actividad de los participantes del sistema financiero, sin embargo existen en el mercado una serie de autoridades que sacan sus propias normativas entre ellas están el Banco Central de Reserva, la Superintendencia de Mercado de Valores, la SBS y se esta evaluando quién debe tener dicha plataforma para lograr un esquema más eficiente. Sin embargo, la mayor parte de servicios que pueden ser afectados se encuentran en los bancos y otra parte dentro de la

[8] Ver Anexo VI

administración pública como el LBTR que esta a cargo del Banco Central, entonces la plataforma de ciberseguridad puede tener la finalidad de mantener informados y a la vez reutilizar la información compartida entre los que se encuentren interconectados con el objetivo de que al existir un ataque cibernético se tome las acciones correspondientes.

7.5 Conclusiones:

En el focus group realizado, todos los participantes mostraron interés en el tema y todos son consientes de la importancia de su desarrollo, con lo cual evidencian que no existe ninguna duda que poder hacerlo ya que todos mostraron una gran predisposición a su realización, en ese sentido de acuerdo a lo que viene sucediendo en Colombia donde existe un alto índice de adopción del servicio y el aspecto regulatorio que la Superintendencia de Banca y Seguros impulsará a través de una normativa específica se puede inferir que existe un mercado potencial para implementar un CSIRT financiero, el mercado potencial asciende a 5 millones de dólares anuales , esperando captura 1.8 millones de dólares del mercado meta en el tercer año.

CAPÍTULO VIII. PLAN DE MARKETING

El presente capítulo tiene como finalidad explorar el marketing mix del servicio, considerando las estrategias adecuadas para poder captarlo, retenerlo y fidelizarlo, en ese sentido también se definirán los indicadores claves que se deben de alcanzar para la ejecución del plan.

8.1 Objetivos de Marketing:

- Generar un ingreso de $230K en el primer año.
- Que el servicio sea adquirido por el 50% del mercado objetivo dentro los dos primeros años
- Comercializar 05 servicios base, 3 servicios de eBanking protection y 3 servicios de ingeniería social.
- Lograr un posicionamiento en el primer año con un porcentaje de reconocimiento del 20% y luego ir aumentando.

De acuerdo a lo indicado por Schumpeter (1934) “La innovación se extiende como un proceso de destrucción creativa, que permite que la economía y los agentes económicos evolucionen; asimismo, es la forma en que la empresa administra sus recursos a través del tiempo y desarrolla competencias que influyen en su competitividad”, en base a lo anteriormente expuesto se puede definir en función de la estrategia empresarial de ASBANC, la misma que se materializa dentro de la perspectiva SF1 del plan estratégico, y que puede ser visualizada en la figura 8.1, donde se indica que se debe contribuir a mejorar la competitividad del sistema financiero, en ese sentido se establecerá la ejecución de un plan de acción que permita materializar en brindar un servicio de plataforma de Ciberseguridad con lo cual se plantea lograr de ingresos en el 2019 alrededor de $250K

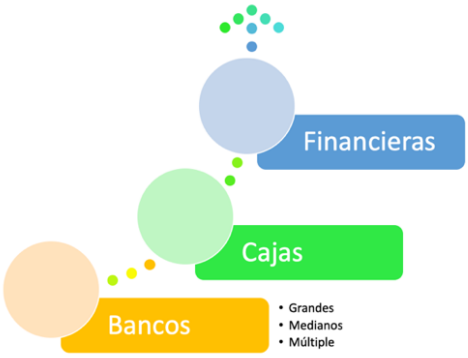
Figura 8.1: Objetivos de Marketing

Fuente: Autor de la tesis

8.2 Segmentación:

El mercado al cual se dirige la presente propuesta de tesis es a instituciones bancarias el mismo que puede ser visualizado en la figura 8.2 donde se realiza una microsegmentación definiendo tres grandes grupos: Bancos, Cajas y Financieras de Perú, ya que la solución ofrecida debe ser customizada de acuerdo con cada segmento, ya que la problemática en temas de ciberseguridad es distinta.

Figura 8.2: Segmentación del Sistema Financiero



Fuente: Autor de la tesis

8.3 Mercado Meta

Se establece a continuación, el mercado meta primario y el mercado meta secundario al cual se le debe comunicar la propuesta de valor.

8.3.1 Mercado Meta Primario:

Bancos con una participación de mercado menor al 0.03% y 18% y que no pertenezca a la banda de segundo piso, donde los roles de decisión sean los oficiales de seguridad de la información de los bancos.

8.3.2 Mercado Meta Secundario:

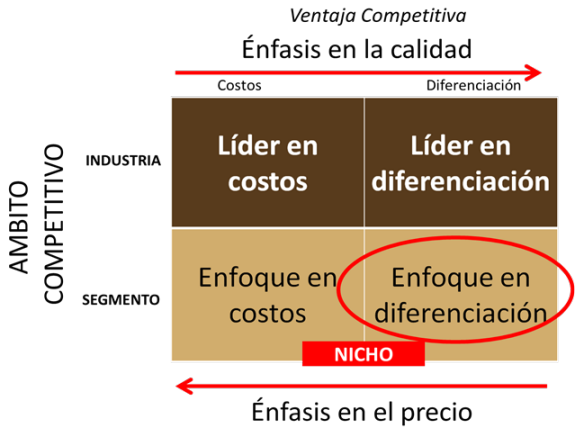
Bancos que tengan una participación de mercado mayor al 18% y que no sea banca de segundo piso, donde los roles de decisión se concentran en los gerentes y responsables de seguridad de la información de las áreas de TI, Cash Management.

8.4 Posicionamiento:

De acuerdo con lo indicado por Salcedo y Maguiña (2013:95) definen el posicionamiento como un proceso para establecer un lugar distintivo en el mercado para una organización y/o sus ofertas de servicio individuales, en un mercado competitivo donde una "posición" refleja la forma en la cual los consumidores perciben el desempeño del servicio en atributos específicos en la relación a sus competidores.

Analizando a los competidores desde la perspectiva de Michael Porter (1979), respecto al tipo de producto que ofrecen se ha optado por una estrategia de posicionamiento con enfoque en la diferenciación, que corresponde a un liderazgo en producto ofreciendo la mejor relación de valor, producto y precio, la misma que se observa en la figura 8.3.

Figura 8.3. Ventaja Competitiva



Fuente: Jiménez & Mezarina (2018)

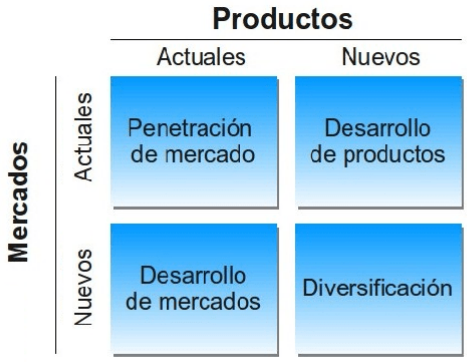
En ese sentido el mercado para la implementación de un CSIRT financiero aún es virgen dentro del mercado peruano, ya que no existen bancos suscritos a este tipo de servicios, lo que permitirá que se posicione como la plataforma integral de Ciberseguridad para el sistema financiero dentro de los bancos con una participación de mercado entre el 0.03% y 18% ofreciéndoles servicios personalizados si que tengan altos costos de inversión y acceder a un amplio catálogo de servicios en nube de acuerdo a la demanda de cada uno, por ello se comercializará a precios igual que los competidores y se manejará una política de precios agresivas para desarrollar negocios.

8.5 Estrategias del Marketing Mix de Servicios (8Ps)

8.5.1 Elementos del Producto

Del análisis realizado, se ha determinado de acuerdo a la matriz de Ansoff[9] que en el cruce en una relación de nuevo producto y mercado actual, se encuentra ante una estrategia de desarrollo de productos, es por ello que puede evidenciarse dentro del producto claras ventajas competitivas como el uso de la inteligencia artificial para la detección de ciberamenazas, lo que reduce sustancialmente los costos operacionales, es por ello que en la figura 8.5 se puede observar la flor de servicios la misma que describe Lovelock (2009) para hacer referencia a los servicios en general, donde inicialmente existe un producto base que estaría compuesto por los servicios MSS & CSIRT que son los componentes fundamentales para la detección de las ciberamenazas, en ese sentido dicho servicio puede hacer uso de otros servicios suplementarios como las consultorías, soluciones avanzadas y auditoria & pentesting, finalmente cabe precisar que todos lo antes mencionados utilizaran los mismos pétalos de la flor ya que son actividades transversales que se realizan.

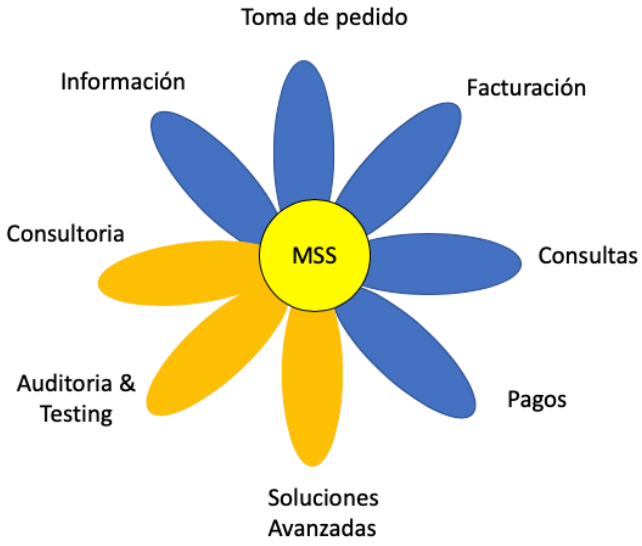
Figura 8.4: Matriz de Ansoff



Fuente: Nicole (2017)

[9] La Matriz de Ansoff es también conocida como matriz Producto/Mercado o Vector de crecimiento. Su objetivo principal es servir de guía a las empresas que buscar crecer ya sea en el mercado en el que actualmente participan como también en otros mercados aun no explorados.

Figura 8.5: Flor de servicios



Fuente: Lovelock & Wirtz (2002)

8.5.1.1 Servicio base:

Se define el uso del servicio MSS que tiene los componentes base que brindará la inteligencia de poder actuar en contra de las amenazas cibernéticas que aparecieran dentro de la organización, los mismos que serán en cumplimiento de lo exigido por la regulación que la Superintendencia de Banca y Seguros normará como requisito mínimo.

8.5.1.2 Pétalos principales

8.5.1.2.1 Servicios de soluciones avanzadas:

Este tipo de servicios el dimensionamiento tecnológico dependerá de los activos críticos que posea la organización, teniendo en cuenta su tipología y las capacidades tecnológicas que este posea.

8.5.1.2.2 Servicios de auditoria y testing:

Este tipo de servicios garantiza que la organización se encuentra en un buen estado de salud, referente a los ataques cibernéticos recibidos, lo que implica que existe una

política dentro de la organización que permite ejecutar este tipo de auditorias con cierta frecuencia.

8.5.1.2.3 Servicios de consultoría:

Servicios orientados al acompañamiento para el cumplimiento de temas normativos y contra los ataques cibernéticos que ocurren dentro y fuera de las organizaciones.

8.5.1.3 Pétalos complementarios:

8.5.1.3.1 Información:

Se le brindara al cliente, instructivos sobre el uso de la plataforma de Ciberseguridad, los horarios de atención, las condiciones de venta

8.5.1.3.2 Toma de pedidos:

Las solicitudes se realizarán a través de la fuerza de ventas, la misma que establece el proceso de atención en el Capítulo VII donde se encuentra el flujo correspondiente.

8.5.1.3.3 Facturación:

Se le enviara a fin de mes un estado de cuenta periódico, en la que figure los servicios contratados y las transacciones realizadas el presente mes.

8.5.1.3.5 Consulta:

Para hacer uso de los servicios de consulta especializada fuera de los ofrecido dentro del servicio base, debe de haber contratado los servicios Cybersecurity Consulting Services y/o Cybersecurity Assessment Consulting.

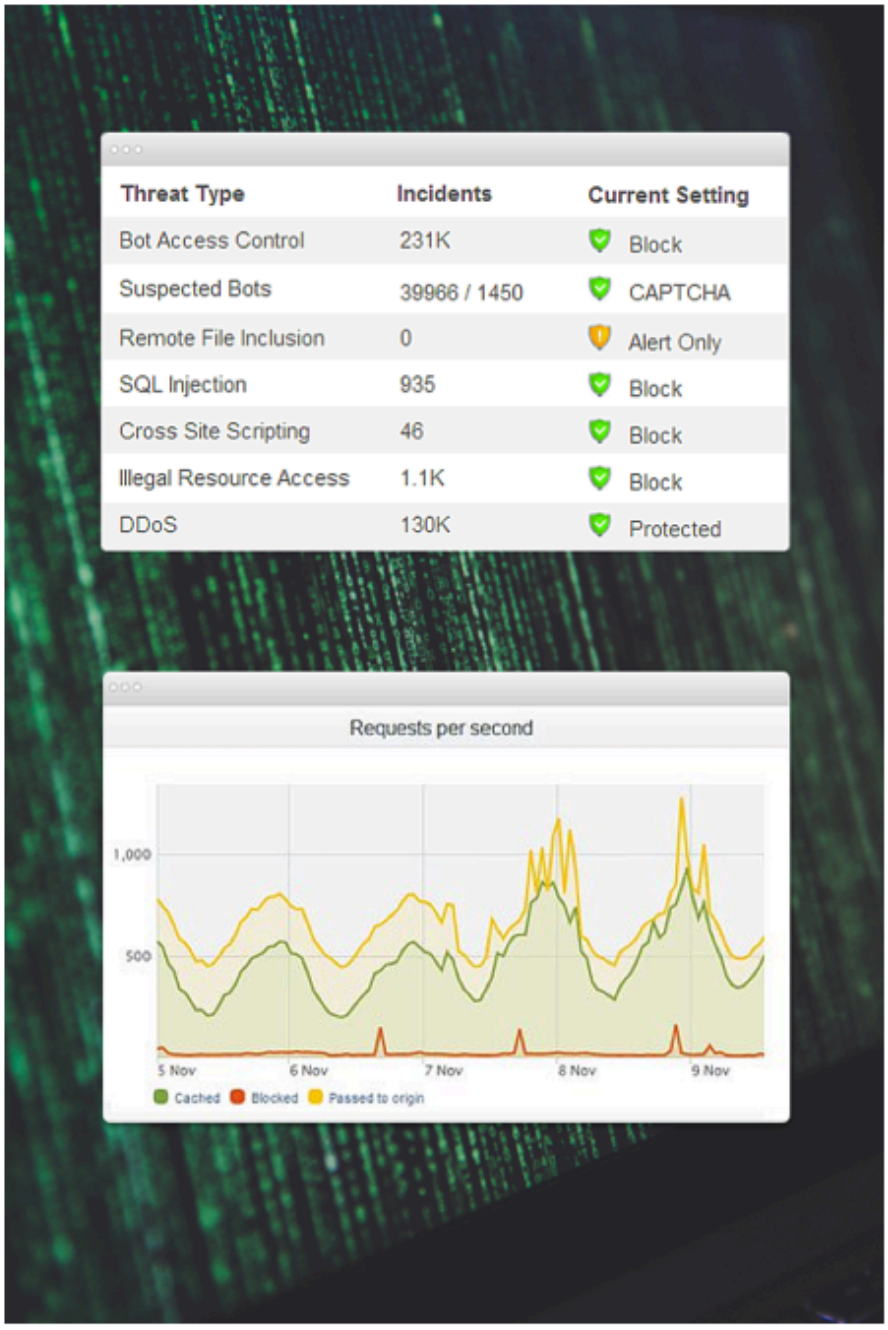
8.5.1.3.4 Pagos:

Se realizará vía transferencia electrónica de fondos, en las siguientes cuentas: Cta. Cte. Dólares en el Banco de Crédito del Perú 191-1016947-1-00 o a la cuenta de transferencia interbancaria CCI: 00291910010169471005 9

8.5.1.2 Diseño de la plataforma de ciberseguridad:

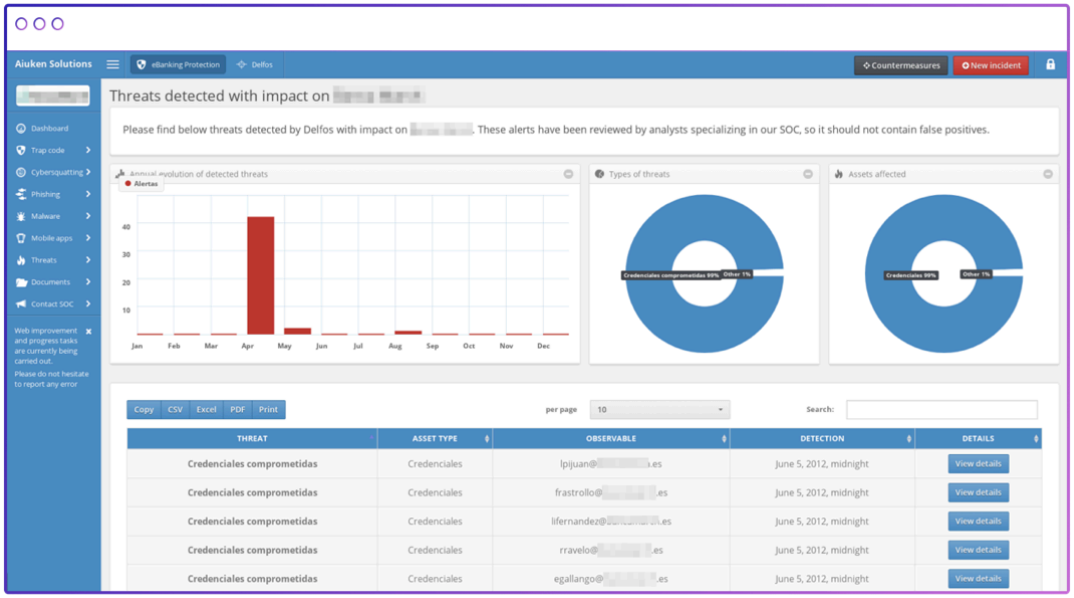
A continuación, se define los diseños para las plataformas de acceso para los principales servicios ofrecidos: MSS & CSIRT, eBanking Protection y Pentesting Services y Gestión de la Ingeniería Social.

Figura 8.6: Visor del Pentesting Services



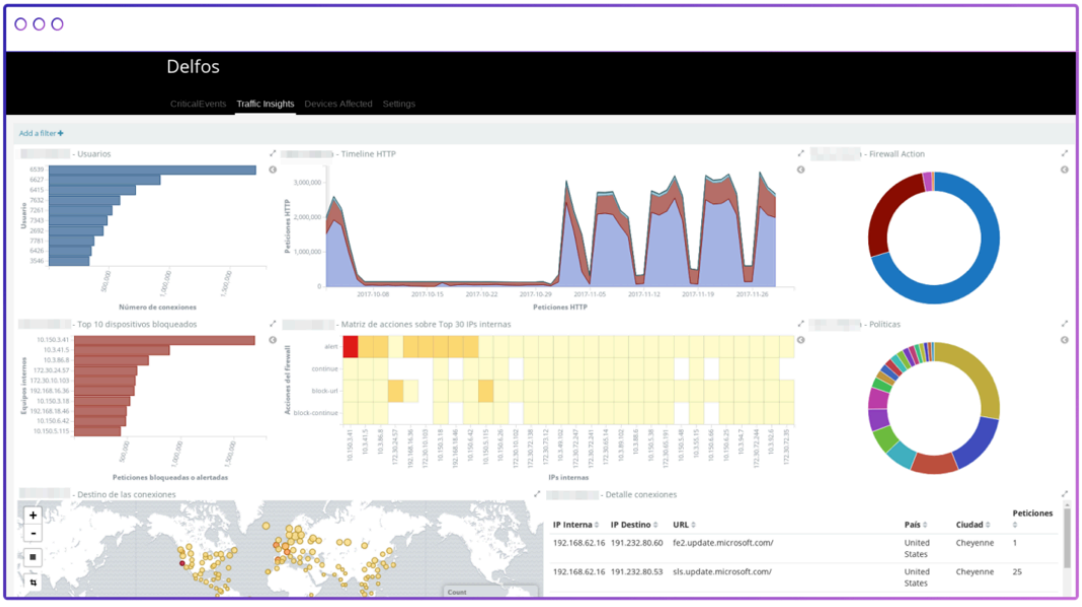
Fuente: AIUKEN (2019)

Figura 8.7: Detección Amenazas MSS



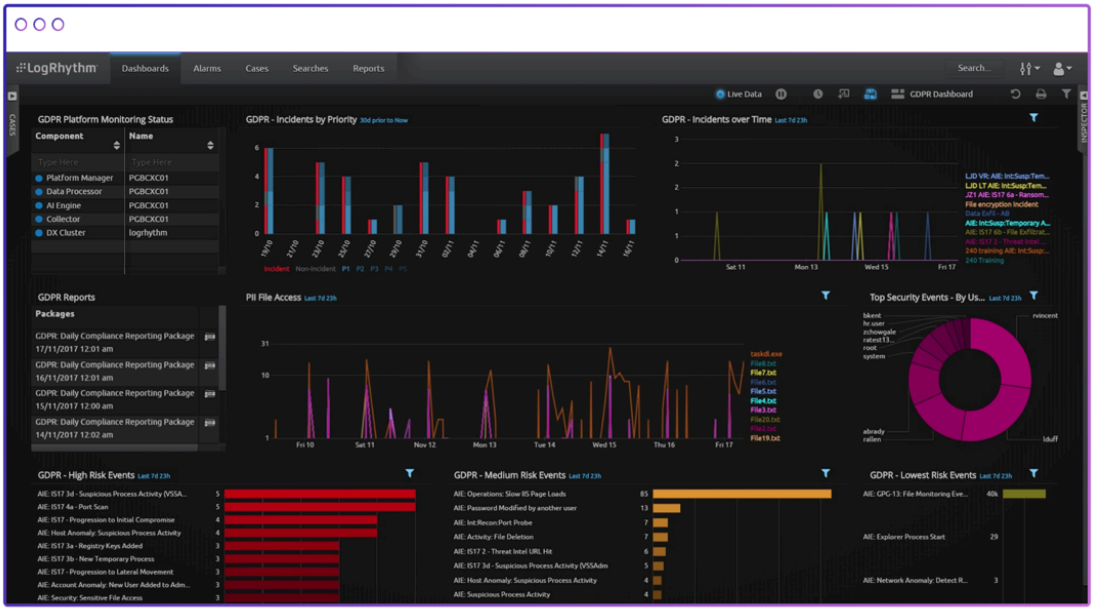
Fuente: AIUKEN (2019)

Figura 8.8: Información de Tráfico MSS



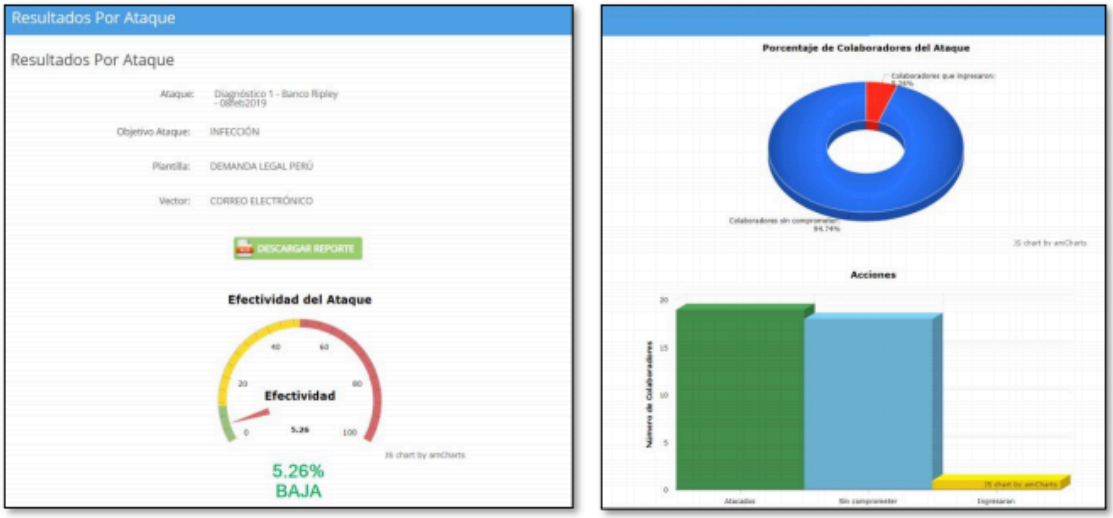
Fuente: AIUKEN (2019)

Figura 8.9: eBanking Protection



Fuente: AIUKEN (2019)

Figura 8.10: Gestión de la Ingeniería Social



Fuente: AIUKEN (2019)

8.5.2 Precio y otros costos para el usuario

Capturar el nivel más alto de precio de mercado, basándose en una estrategia de paridad en el precio del servicio, el cual debe su exclusividad al uso de una inteligencia artificial entrenada en la detección de patrones de malware, fishing durante cuatro años en el mercado europeo de Bancos, garantizando que el servicio responda en tiempo real a cualquier ataque cibernético que provenga de cualquier parte del orbe hacia el sistema financiero peruano, siendo la relación de precios la siguiente:

Tabla 8.1: Precios de Lista (sin IGV)

Categoría	Servicios	Mensual
Base	Managed Security Services	$15,000
Consultoría	Cyber Security Consulting Services	$21,394
Consultoría	Cyber Security Assessment Consulting	$9,169
Soluciones Avanzadas	eBanking Security Services	$18,337
Soluciones Avanzadas	Ethical Hacking Professional Services	$17,319
Soluciones Avanzadas	Gestión de la Ingeniería Social	$8,150
Auditoria & Testing	Pentesting Services	$9,169
Auditoria & Testing	Security Code Review	$9,169
Auditoria & Testing	Visibility Analytics Services	$7,131
Auditoria & Testing	Vulnerability Assessment Services	$6,113

Fuente: Autor de la tesis

A precio de lista se va a colocar igual que el competidor usando paridad de precio de acuerdo a lo que se puede visualizar en la tabla 8.1, pero al momento de negociar se va a considerar el precio de introducción que se muestra en la tabla 8.2 ya que por penetración de mercado y dado que el segmento son bancos pequeños se realizarán un descuento de 57% por año y estos se mantendrán durante tres años hasta lograr el objetivo de lograr 6 clientes, posteriormente a los siguientes se les cobrará los precios de lista, para efectos de simulación sólo se ha colocado los precios de introducción para el servicio base el cual comienza en $9,500 y el precio máximo puede llegar a $26,250 correspondiente a la venta de un servicio de eBanking Protection y Gestión de la Ingeniería Social los que se encuentran dentro de la categoría de soluciones avanzadas.

Tabla 8.2: Precio de Introducción (sin IGV)

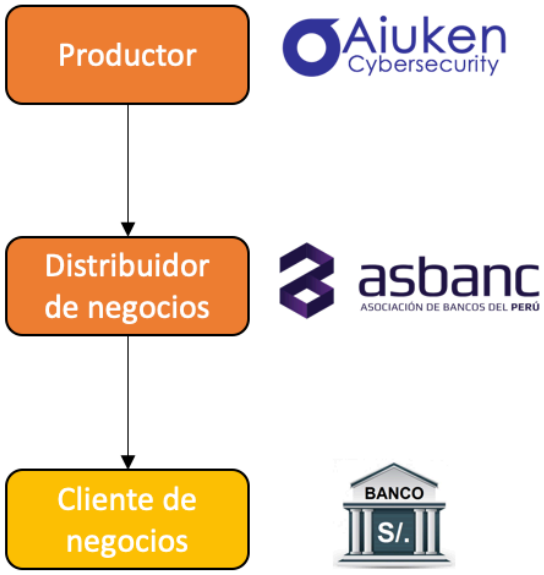
Categoría	Servicios	Mensual
Base	Managed Security Services	$9,500
Consultoría	Cyber Security Consulting Services	$13,125
Consultoría	Cyber Security Assessment Consulting	$5,625
Soluciones Avanzadas	eBanking Security Services	$11,250
Soluciones Avanzadas	Ethical Hacking Professional Services	$10,625
Soluciones Avanzadas	Gestión de la Ingeniería Social	$5,000
Auditoria & Testing	Pentesting Services	$5,625
Auditoria & Testing	Security Code Review	$5,625
Auditoria & Testing	Visibility Analytics Services	$4.375
Auditoria & Testing	Vulnerability Assessment Services	$3,750

Fuente: Autor de la tesis

8.5.3 Lugar y tiempo

El tipo de distribución utilizada para este tipo de canal seria del tipo indirecta para negocios, en la cual se permite operaría con un solo distribuidor de negocios permitiendo así un mejor control sobre la entrega del servicio, por ello en la figura 8.11 se puede observar el flujo de la misma, siendo la mecánica de comercialización del servicio a través de una venta consultiva[10], acompañados de expertos internacionales en Ciberseguridad de la empresa AIUKEN, ya que el objetivo de la misma será relevar mediante un assesment o cuestionario los principales problemas que ocurren en los clientes.

Figura 8.11: Distribución indirecta de negocio



Fuente: Kotler (2012)

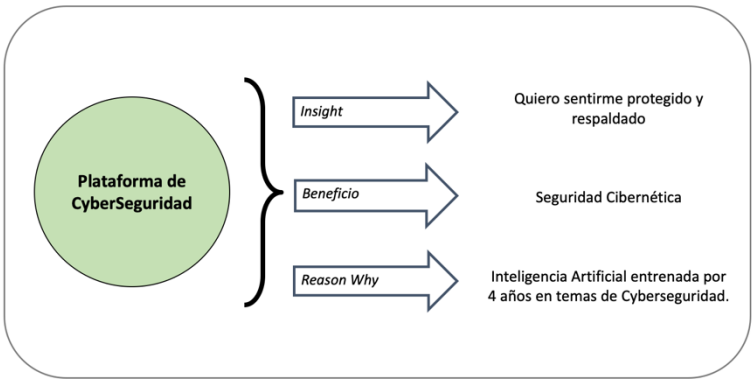
[10] El proceso comercial de la fuerza de ventas se detalla en el capítulo IX

8.5.4 Promoción y Educación

Se disponen de varias herramientas promocionales entre las que se tiene: marketing directo, relaciones publicas, ventas personales y promoción de ventas, para ello se abordaran a continuación cada una de estas herramientas, que permita llegar a nuestro publico objetivo de manera rápida y efectiva.

El marketing directo sería a través de mailing, catálogo informativo, marketing telefónico, al ser un servicio sumamente complejo solo se evidenciará la comunicación del Insight del servicio "Quiero sentirme protegido y respaldado", para ello se usará las bases de datos que tiene ASBANC sobre sus asociados, a los jefes, gerentes, oficiales de seguridad de la Información.

Figura 8.12: Insight del servicio



Fuente: Autor de la Tesis

En referencia al insight del servicio, se determina que entre los principales pains se encuentran que los problemas de no contar con un servicio de este tipo afecta los temas políticos, costos, reputacionales y de compliance, por ello el compelling event relacionado a este pain son los juegos panamericanos[11] a realizarse en julio próximo, donde la pérdida de no tener implementado este servicio haría realidad los puntos de dolor indicados anteriormente, los beneficios o gain asociados son que en todo momento podrán proteger los activos críticos de su infraestructura evitando las pérdidas tanto económicamente como a nivel de imagen.

[11] Los Juegos Panamericanos de 2019, oficialmente los XVIII Juegos Panamericanos, serán un evento multideportivo internacional que se celebrará entre el 26 de julio y el 11 de agosto de 2019 en Lima.

En las relaciones publicas, se planifica la participación en eventos especializados como el SEGURINFO[12] que permita evidenciar la potencia de nuestra solución con demos en línea y que permitirá generar una buena imagen corporativa dentro del sector financiero como lideres en soluciones de Ciberseguridad.

Para incentivar al mercado meta en la adquisición de los servicios, se utilizará una promoción de ventas, que consiste en probar durante un mes los siguientes servicios mostrados en la tabla 8.3, con el objetivo de poder conocer cuales son los diferenciadores claves del servicio.

Tabla 8.3. Lista de Promociones

Análisis de vulnerabilidades	- IP's públicas y privadas sin límite. - No se incluye reporte de recomendaciones.
Un mes de inteligencia de eBanking Protection	- Cuentas comprometidas. - Vulnerabilidades en activos informáticos públicos.
Diagnóstico de ingeniería social	- 03 ataques personalizados sobre vector de correo electrónico. - Reporte ejecutivo.

Fuente: Autor de la tesis

Para las ventas personales, se realizarán las visitas a cada uno de los clientes del mercado meta con el objetivo de poder conocer sus necesidades de primera mano, ya que existe un mayor entendimiento de ambas partes cuando y se tiene una mayor efectividad, sobre todo porque construye una relación de largo plazo con el cliente permitiendo que esta actividad sea vista mas como una inversión en la relación de vida con el cliente.

Siendo esta definición de las herramientas a utilizar en esta parte del servicio, se elegirá la estrategia de empuje que de acuerdo a Kotler (2012) la define como el impulso que recibe un servicio a través de los canales de marketing hacia los consumidores finales a través del canal, que este caso es el distribuidor de negocios que impulsara con estas técnicas a sus clientes finales utilizando las herramientas de ventas personales, promoción comercial, entre otras, donde el flujo puede ser observado en la figura 8.13

[12] SEGURINFO, es uno de los principales congresos anuales de seguridad de la información que incluye un intensivo programa con sesiones de seguimiento y actualización para reunirse con colegas y proveedores de la industria al cual los miembros de la banca participan de manera anual.

Figura 8.13: Estrategia de empuje

Fuente: Kotler (2012)

Finalmente, también a los clientes que cierren un contrato con ASBANC durante el primer año de lanzamiento del servicio, se les llevara a Madrid a visitar el SOC de la empresa AIUKEN, el objetivo es poder vivir la experiencia de los servicios que este ofrece y también escuchar el comentarios de otros clientes a quienes vienen atendiendo, todo este traslado, movilidad y costes de permanencia serán asumidos por AIUKEN Cybersecurity.

8.5.4.1 Estrategia de Fidelización:

En vista que se cuenta con una ventaja competitiva de alrededor de 5 años, se buscará crear con el cliente una relación de largo plazo, que permita fidelizar al mercado meta creando las barreras necesarias que haga frente a una posible competencia, entre las actividades que se realizará de manera regular es otorgar capacitaciones gratuitas a los clientes, quienes son los responsables de administrar el servicio dentro de la organización

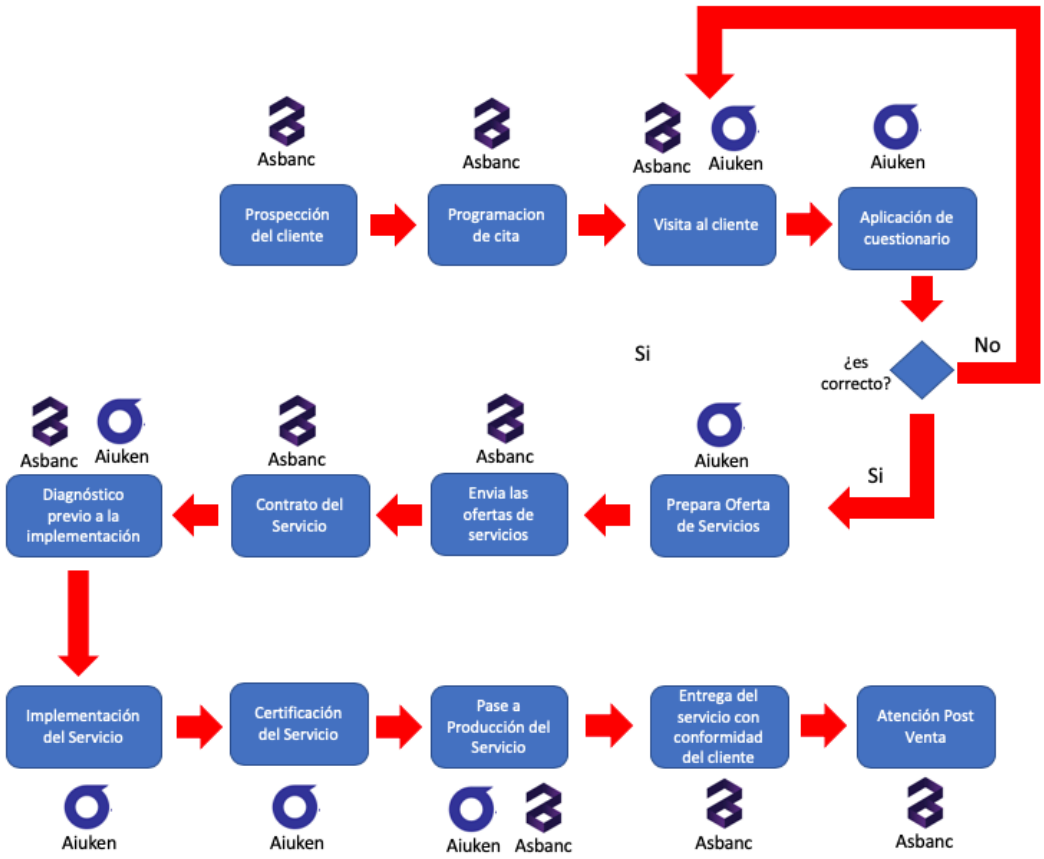
Asimismo, también se enviará información actualizada sobre los temas de Ciberseguridad como boletines semanales, informes técnicos del sector, tendencias mundiales, y la estrategia más importante de todas es utilizar los patrones predictivos de todo el sistema para poder brindar un diferenciador especial frente a terceros, en la cual la data analizada arroje los patrones predictivos de fraude pero esto sobre la base de conocimiento almacenado durante cinco años, todo esto acompañado de expertos internacionales como Antonio Ramos, Juan Miguel Velasco, entre otros.

8.5.5 Proceso

Para poder brindar el servicio, se ha diseñado el siguiente proceso que gráfica toda la ruta que seguiría la atención de un nuevo cliente, comenzando por la etapa de prospección del cliente, la que es realizada por ASBANC en función de la información que se dispone dentro de la organización respecto a los asociados, como los componentes de su infraestructura, número de incidencia anuales, entre otros datos que son compartidos dentro de los comités de seguridad física y electrónica, que se organizan mensualmente, para ello una vez realizada la prospección pasaría a programarse una cita para visitarlo, esta tarea es realizada por el área comercial a través del call center, luego que se procede con la visita para ello la empresa AIUKEN participa ya sea remotamente vía Skype, Webex u otra herramienta remota el acompañamiento a la fuerza comercial para poder escuchar las necesidades del cliente y también cruzar con la información proporcionada por ASBANC, es por ello que AIUKEN procede con la aplicación de un cuestionario que permite tener identificado la situación del prospecto, si este cuestionario no identifica dicho assesment este deberá ser repetido hasta que se encuentre totalmente correcto, posteriormente AIUKEN tiene hasta 2 semanas como máximo para preparar una oferta de servicios que contemple todas estas necesidades que serian atendidas de manera inicial por el CSIRT, por ello una vez terminada se envía la propuesta de servicios al cliente, esta tarea es realizada por ASBANC y una vez aceptada la propuesta ASBANC gestiona el contrato de servicios.

Para asegurarse de la calidad de los servicios a implementarse, se realiza un diagnóstico previo dentro del cliente, este es ejecutado por AIUKEN y supervisado por ASBANC, para que en la etapa de implementación no ocurra ningún imprevisto que anteriormente no se haya identificado, luego de esta etapa se procede con las pruebas de certificación y se concluye con el pase a producción realizado entre AIUKEN y ASBANC para dar fe de que el proceso se concluyo correctamente se le solicita al cliente que firme un acta de conformidad del servicio realizado, esta tarea es realizada por ASBANC y si todo es conforme pasa al área comercial para que se le brinde el servicio post venta correspondiente.

Figura 8.14: Proceso de atención del servicio



Fuente: Autor de la tesis

8.5.6 Entorno físico

Lovelock (2002) indica que los entornos de servicio se relacionan con el estilo, la apariencia del ambiente físico y otros elementos que experimentan los clientes en los sitios donde se entregan los servicios, el entorno y la atmósfera que lo acompañan afectan el comportamiento del comprador de tres maneras importantes: como medio que crea mensajes, como medio que llama la atención y como medio que crea afecto.

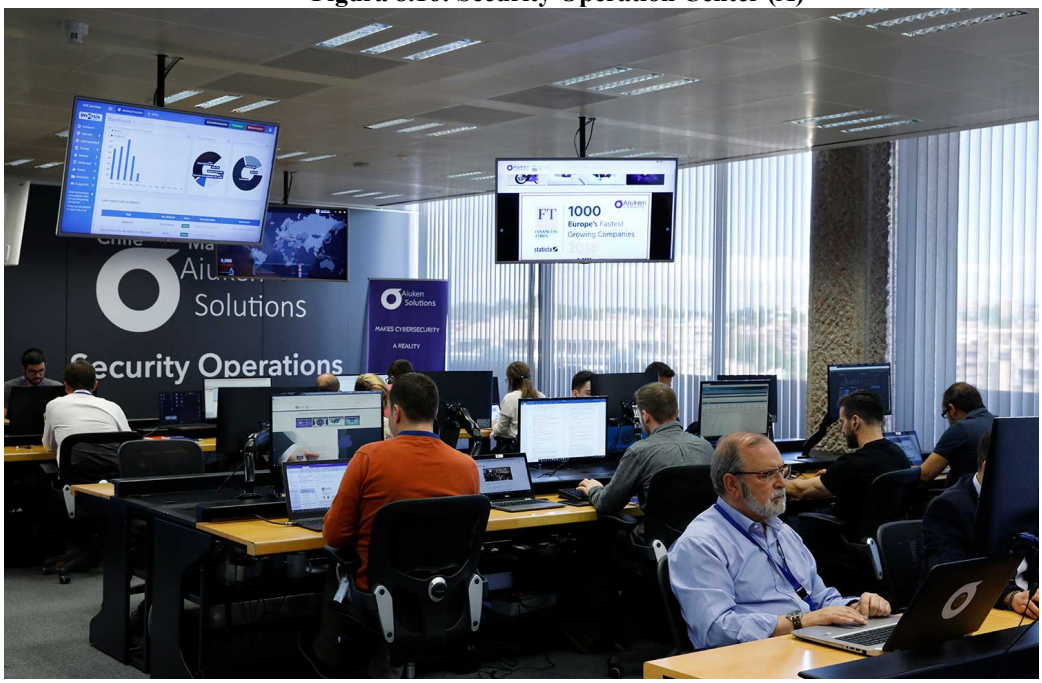
Es por ello que la empresa AIUKEN ha situado su Centro de Operaciones a la entrada de un hotel de lujo, en este caso el Hilton vemos en la figura 8.15 que el ambiente se encuentra preparado para indicarle al mercado meta que comunica una calidad distintiva de experiencia en el servicio.

Figura 8.15: Entrada de AIUKEN

Fuente: AIUKEN (2017)

Asimismo, los ambiente donde se brindan los servicios, se le denomina los ambientes de showroom, se puede observar a los operadores de primer, segundo y tercer nivel que brindan los servicios de monitoreo avanzado del servicio, estos lugares son exhibidos para las visitas para que puedan conectar con el cliente y crear esa conexión para atraer a los clientes que contraten el servicio.

Figura 8.16: Security Operation Center (A)



Fuente: AIUKEN (2018)

Figura 8.17: Security Operation Center (B)

Fuente: AIUKEN (2018)

8.5.7 Personal

Heskett & Sasser (2010), hace referencia a que la satisfacción del cliente es el resultado del logro de mayores niveles de valor que los competidores y el valor se crea por medio de empleados satisfechos, comprometidos, leales y productivos, por ello de acuerdo a la naturaleza de este servicio el personal post venta tendrá poco contacto con el cliente, la interacción se dará mayormente a través de correo electrónico o teléfono, sin embargo para los momentos de la comercialización existirá un mayor contacto, siendo estos momentos los fundamentales para la construcción de valor con el cliente, es por ello muy importante que este personal tenga las competencias[13] blandas necesarias para poder atender al cliente de la mejor forma, por ello se le pedirá al área de recursos humanos que pueda seleccionar al grupo de personas que tengan las siguientes competencias para la atención del servicio:

Atención post venta:

Tabla 8.4: Perfil de atención post venta

		A	B	C	D
Competencias Genéricas	Innovacion			X	
	Compromiso		X		
	Integridad		X		
	Orientacion al cliente	X			
Competencias Específicas	Orientacion a resultados		X		
	Comunicación	X			
	Empowerment			X	
	Aprendizaje continuo		X		

Fuente: Autor de la tesis

Ejecutivo de Ventas:

Tabla 8.5: Perfil de ejecutivo de ventas

		A	B	C	D
Competencias Genéricas	Innovacion			X	
	Compromiso		X		
	Integridad	X			
	Orientacion al cliente	X			
Competencias Específicas	Orientacion a resultados	X			
	Comunicación	X			
	Empowerment	X			
	Aprendizaje continuo		X		

Fuente: Autor de la tesis

8.5.8 Productividad

[13] Ver la descripción de las competencias en el Anexo XI

De acuerdo con lo expresado por Lovelock (2002), menciona que el mejoramiento de la calidad del servicio y el aumento de su productividad a menudo son dos lados de la misma moneda, pues ofrecen un potencial poderoso para incrementar el valor para los clientes y la empresa, por ello un desafío fundamental para cualquier negocio de servicios es entregar resultados satisfactorios a sus clientes, en forma que estos sean rentables para la empresa.

Es por ello que de acuerdo a lo expuesto anteriormente para poder producir mejores resultados a nivel de la productividad del servicio ofrecido, se seguirá una estrategia basada en la automatización de procesos para que sistemas expertos puedan reemplazar los procesos operativos actuales, es por ello que servicios como los de auditoria y testing podrían ser mejorados con el uso de una tecnología basado en inteligencia artificial, con ello ya no se necesitaría de profesionales expertos que realicen estas labores sino que se desplegaría una serie de herramientas que permitan que estos procesos sean cada vez más exactos, es por ello muy importante estar midiendo los gaps e ir incorporándolos dentro del entrenamiento de esta tecnología que va aprendiendo y resolviendo poco a poco, es importante precisar que esta es una tendencia en los últimos años sobre todo porque se busca reducir los costos operacionales y también buscar una mayor rapidez en los tiempos de respuesta hacia el cliente.

8.6 Plan de acción

Dentro de el roadmap para ejecutar todas estas acciones comienzan en agosto 2018 y se terminan en marzo 2019, en la cual se establecen los pasos para poder lograr el objetivo de lograr una meta comercial de US$230K en el 2019

- Realización Joint Venture con empresa internacional (febrero 2018).
- Lanzamiento del Servicio (noviembre 2018).
- Campaña de diagnóstico gratuito a los asociados (enero – marzo 2019).
- Visita guiada a las Estaciones SOC (Madrid – Barcelona) con los asociados que muestren interés por el servicio (marzo 2019).

8.7 Calendarios y KPIs

Se establece un calendario para el 2019, donde se establecen las metas comerciales para el servicio.

Tabla 8.6: Indicadores Clave y Calendario

Key Performance Indicators					
Launch KPIs		3 months	6 months	12 months	Measure
1	Margen de Contribución del servicio	20	35	50	%
2	Ingresos del Periodo	50,000	100,000	250,000	US$
3	Coverage	10	20	30	%

Fuente: Autor de la tesis

8.8 Conclusiones

De lo anteriormente expuesto se concluye que el mercado meta son los bancos que mantienen una participación de mercado menor al 30%, esto se debe a que los bancos grandes ya tienen algún servicio de ciberseguridad mientras que los bancos medianos y pequeños no lo tienen, esto también se pudo relevar dentro de la etapa de estudio de mercado realizado.

CAPÍTULO IX. PLAN COMERCIAL

El presente capítulo tiene como finalidad determinar cuales son los objetivos del plan de ventas, el proceso y la estructura del área comercial y cual seria la proyección que se estima para la venta del servicio.

9.1 Objetivos comerciales

- Lograr $230K de ingresos el primer año de operación
- Suscribir al servicio a 2 entidades bancarias durante el primer año de operación
- Contar con una cartera de 5 clientes al tercer año de operación

9.2 Estrategia Comercial

La venta del servicio Base será el servicio Managed Security Services y el modulo de CSIRT, sin embargo, este servicio detectara de manera adecuada los incidentes, amenazas que sucedan dentro de la organización, sin embargo, el objetivo es generar cross-selling, a lo largo del servicio, este mismo es variable ya que dependerá de cada institución que servicio a demanda puede tomar.

9.3 Fase de Preventa

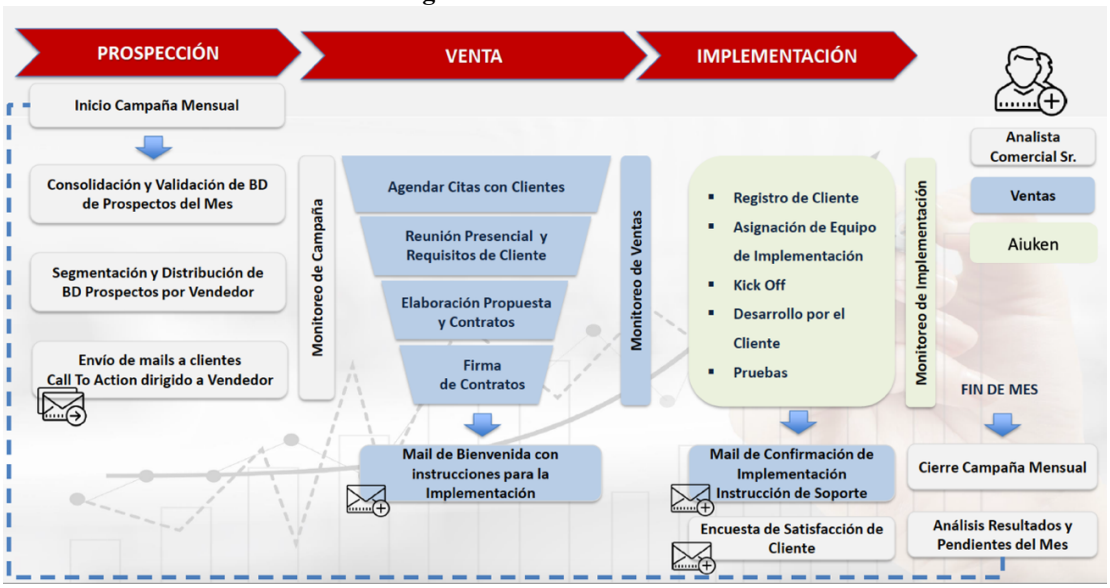
Antes de iniciar el proceso comercial el gerente de operaciones debe hacerse cargo de participar como parte de la preventa del servicio, a través de las relaciones que mantiene con los bancos en los comités operativos donde este participa, en dichas reuniones la información que se debe de comunicar a los participantes es que ASBANC se encuentra comercializando un servicio de ciberseguridad, en alianza estratégica con la empresa internacional AIUKEN, cabe precisar que el rol que el gerente de operaciones desempeña en ASBANC es la de un influencer[14] ya que tiene una participación activa en los medios de comunicaciones y es ampliamente reconocido por todo el sector financiero respecto a los temas de seguridad informática ya que tiene más de 20 años de experiencia nacional e internacional.

[14] Influencer: Es una persona que cuenta con cierta credibilidad sobre un tema concreto, y por su presencia e influencia en redes sociales puede llegar a convertirse en un prescriptor interesante para una marca.

9.4 Proceso Comercial:

Dentro del proceso comercial se establecen que ASBANC se encarga de la facturación, cobranza y pagos de los servicios contratados por cada uno de los clientes, así como también de su comercialización, por ello se establece que la fuerza de ventas haga una prospección adecuada de los servicios de Ciberseguridad, por ello en la figura 9.1 se establece el flujo del proceso comercial de inicio a fin que permitirá contar con una propuesta ad-hoc para cada cliente a implementar, es por ello que dentro de la prospección realizada por el analista comercial senior en conjunto con los vendedores definen el perfil del servicio a través una venta consultiva, es por ello que se requiere la participación de la parte técnica que asista al personal de ventas para poder generar las propuestas comerciales correspondientes, los mismos que deben calzar dentro de los gastos comerciales del servicio ofrecido y que se muestra en la figura 9.2.

Figura 9.1: Proceso Comercial



Fuente: ASBANC

9.3.1 Fase de prospección:

Un analista comercial de ASBANC, se encarga de monitorear toda la campaña, prospectando la base de datos y tomando como referencia la lista de contactos que ASBANC posee, para este servicio en particular la preventa es realizada por el gerente de operaciones y la venta es realizada por el ejecutivo comercial de ASBANC con el gerente de negocios, para ello realizaría una segmentación de acuerdo al mercado meta indicado en el Capítulo VIII, luego esta prospección sería enviada al vendedor para que luego pueda realizar el proceso de ventas correspondiente, Finalizando la fase de implementación del servicio con una encuesta de satisfacción al cliente y el análisis mensual de los resultados de la campaña.

9.3.2 Fase de venta:

El ejecutivo comercial agenda una reunión con el cliente capturado a través de la base de datos enviada en la fase de prospección, y luego lo ingresa en el pipeline de ventas, elabora una propuesta y el contrato y gestiona la firma de estos, cuando cierra la venta envía un email de bienvenida con instrucciones para la implementación, al finalizar la implementación se le envía al cliente un email para la confirmación de los trabajos realizados seguido de las instrucciones de soporte.

9.3.3 Fase de implementación:

La empresa AIUKEN registra al cliente en su sistema de trabajo, recibiendo por parte del ejecutivo comercial de ASBANC que inicien los trabajos, en la cual se le asigna un equipo de trabajo, para luego programar el inicio del proyecto a través de un "Kick Off", luego pasa a la fase de desarrollo por lado del cliente y se termina con las pruebas de certificación del servicio y pase a producción.

9.5 Perfil del Equipo de ventas

Los Key Account Manager o Ejecutivos Comerciales de ASBANC liderarán la apertura de canales de comunicación hacia los clientes, aprovechando el relacionamiento institucional que ASBANC tiene con los mismos, entre sus responsabilidades se encuentran indicadas en la tabla 9.1

Tabla 9.1: Funciones y Responsabilidades del Ejecutivo Comercial

Apoyar en la comunicación y convocatoria para cualquier iniciativa de mercadeo Aportar a la actualización constante de la base de datos de contactos de clientes Realizar prospección de los clientes, comunicándose con ellos vía correo, llamadas y visitas con la frecuencia que determinen las gerencias de proyecto Realizar presentaciones y exposiciones de soluciones y servicios de ciberseguridad Coordinar visitas a los ejecutivo preventa, gerentes de proyecto y/o directores, según sea el caso Generar un pipeline de oportunidades calificadas por montos que cumplan los hitos establecidos en el plan de trabajo Generar facturación de ASBANC a los clientes por montos que cumplan los hitos establecidos en el plan de trabajo.

Fuente: Autor de la tesis

9.6 Sistema de incentivos:

El sistema de comisiones se establece como un 5% de la venta realizada, sin embargo, este es el driver que se usa para la proyección financiera, por ello posteriormente se detallará como se compondría este sistema de incentivos, ya que el Key Account es un parte muy importante dentro del proceso de gestión comercial.

9.5.1 Tipos de incentivos

En función del objetivo comercial planteado, se ha considerado dos tipos de incentivos, en función del logro de meta de ventas propuesto alineado al objetivo comercial de lograr en el primer año una venta de $230K, cabe precisar que el Key Account comercializará también otros servicios del portafolio de servicios mostrados en la tabla 8.1, estos incentivos están calculados de acuerdo con el esquema comisional que se muestra en la tabla 9.2.

Tabla 9.2: Esquema comisional

	1 cuota 9K	**2 cuota 18K**	**3 cuota 27K**	**Bono Logro**
KAM	$400	$400	$400	$600

Fuente: Autor de la tesis

9.6 Capacitación sobre la venta

La empresa AIUKEN proveerá de clases virtuales al personal de ventas de ASBANC, con el objetivo de poder conocer a mayor detalle sobre los servicios y funcionalidades brindadas por cada uno de ellos, todas estas capacitaciones servirán de base para poder conocer el portafolio de servicios que se explicaron en el capítulo VI, ya que este tiene un alto componente técnico, donde las capacitaciones ayudarán a que estas se ejecuten de manera adecuada.

9.7 Gastos Comerciales:

A continuación, se muestra en la tabla 9.3 los costos comerciales asociados al proceso de venta, en donde se especifica el esquema de comisiones por cada servicio vendido y los drivers de costo administrativos que incurre ASBANC por dicha línea de servicio, cabe resaltar que al ser este un servicio tercerizado requiere del apoyo permanente de la empresa AIUKEN para poder dimensionar correctamente la propuesta comercial.

Tabla 9.3: Gastos Comerciales

Comisiones del vendedor	5%	Ventas
Marketing	$7,716	Anuales
Sueldo del vendedor	$5,556	Anuales
Beneficios sociales del vendedor	$3,333	Anuales
Sueldo de personal operativo	$15,926	Anuales
Beneficios sociales del personal operat	$9,556	Anuales
Gastos Administrativos	2%	Ventas

Fuente: Autor de la Tesis

9.8 Proyección de ventas:

De acuerdo con el mercado meta, se establece que la población objetivo son 5 instituciones financieras, es por ello por lo que se puede observar en la tabla 9.4 que la cantidad de clientes suscritos al servicio finaliza con dos clientes el primer año, luego ingresan dos instituciones más durante el segundo año y se finaliza el tercer año con 05 clientes en cartera respecto a la comercialización de los productos base.

Tabla 9.4: Demanda de los Servicios

Periodo	Año 1	Año 2	Año 3	Año 4	Año 5
- Productos Base	2	4	5	5	5
- eBanking	1	2	3	3	3
- Ingeniería	1	3	3	3	3

Fuente: Autor de la Tesis

9.9 Conclusiones

Se puede concluir que al finalizar el proyecto se espera contar con el 50% del mercado objetivo, sin embargo, esto no excluye que se pueda realizar la venta de otro tipo de servicios.

CAPÍTULO X. PLAN DE TECNOLOGIA DE INFORMACION

En el presente capitulo se explica el plan de tecnología que cubre los aspectos relacionados al hardware y software necesarios para que los clientes que se conecten al servicio puedan operar de manera continua.

10.1 Plataforma de Comunicaciones:

Para que el servicio se brinde de manera adecuada se dispone de una plataforma de comunicaciones propiedad de la ASBANC, es por ello que la empresa América Móviles conocida comercialmente con el nombre de CLARO se encarga de operar dicha plataforma desde el año 1998, siendo la disponibilidad de la misma por encima del 99.98%, el detalle de las características técnicas contratadas se detallan en el Anexo XII.

A continuación se listan las principales características del servicio:

- Un enlace principal en el nodo central.
- Un enlace de respaldo en el nodo alterno.
- Equipos de comunicaciones y demás dispositivos necesarios para el funcionamiento del enlace a la red
- Servicio de administración, configuración, operación, mantenimiento y soporte del nodo remoto constituido para el cliente,
- Información en línea que le permita conocer el nivel en que se utiliza el ancho de banda del enlace conectado al nodo remoto mediante el cual se le preste el servicio Bancared materia de este contrato.

10.2 Servicio de Administración:

ASBANC brinda el servicio de administración de la plataforma de comunicaciones a través del área de conectividad que opera dentro de la gerencia de operaciones, la misma que se encargará de realizar las siguientes tareas:

- Implementación, administración, configuración, operación, mantenimiento, soporte, renovación tecnológica, disponibilidad y seguridad de los nodos centrales y alternos.

- Todos los programas (software) puestos a disposición de los clientes para que el monitoreo de su enlace sea a través de Internet.
- Mantener una disponibilidad del 99.98% de disponibilidad del servicio.

10.3 Requerimientos de infraestructura y tecnología

Al acceder a una red remota como la de AIUKEN que nos permita acceder a su catálogo de servicios a demanda, se requiere que cada cliente que vaya a contratar el servicio nos brinde la siguiente información a nivel fisco y a nivel lógico con dicha información se podrá dimensionar el alcance de los recursos:

10.3.1 Físico:

Características técnicas de los dispositivos que posee, número de dispositivos, tipo de red, ubicación y conectividad a la red de activos TI, equipos de sobremesa, servidores, dispositivos de red, dispositivos móviles, sistemas tercerizado, servicios en la "nube".

10.3.2 Lógico:

Topología de red, conectividad física y lógica, límites que separan las diferentes zonas de confianza y conexiones externas, etc.

10.4 Conclusiones:

Para poder hacer uso de la plataforma se necesita que el cliente se conecte a la red de CLARO para poder hacer uso de la plataforma de comunicación, cabe precisar que esta red es privada y todo el tráfico que se cursa en ella se encuentra asegurada de inicio a fin.

CAPÍTULO XI. PLAN DE RRHH

En el presente capitulo se describe la organización que seguirá el servicio a nivel de personas, en ella se detallarán los roles que desempeñará cada uno de los integrantes del equipo del servicio tanto de lado de ASBANC como de AIUKEN.

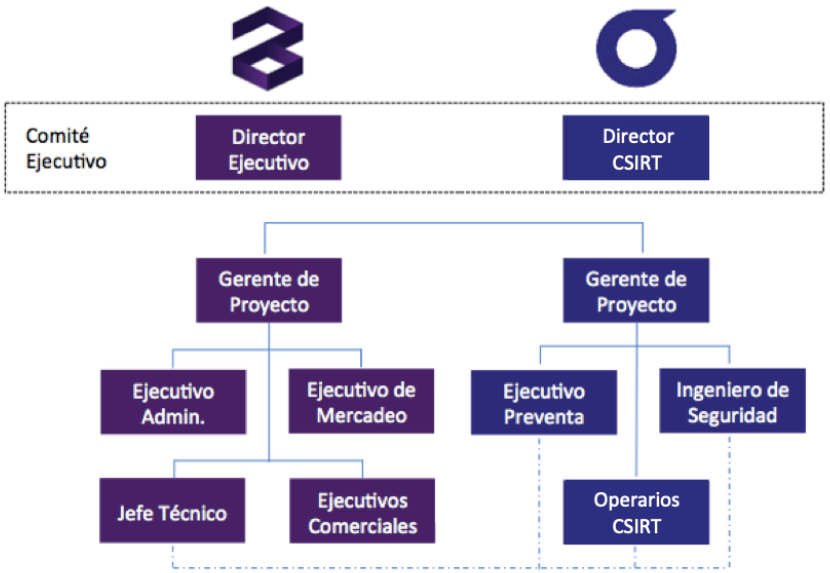
11.1 Estrategias de organización y recursos humanos en ASBANC

Al ser un servicio tercerizado se requiere una mínima planta operativa para atender el servicio por parte de ASBANC, lo que no ocurre con la parte comercial que requiere personal preventa especializado, para poder aterrizar las necesidades de los bancos que se requieran en los temas de ciberseguridad, ejecutivos comerciales, Jefe Técnico y Ejecutivo de administración, cabe precisar que se utilizarán recursos propios de la organización para no incurrir en gastos mayores a los presupuestados, como se puede visualizar en la figura 11.1.

11.2 Estrategias de organización y recursos humanos en AIUKEN

La parte organizacional y de recursos humanos que estaría proveyendo la empresa AIUKEN se puede en la figura 11.1, y el detalle de como opera el CSIRT se explica en la figura 11.2 en la cual se detalla las áreas de análisis y respuesta, escaneo y evaluación y ciclo de vida de sistemas.

Figura 11.1: Organigrama ASBANC - AIUKEN



Fuente: Autor de la tesis

11.3 Descripción de los Roles y Funciones

A continuación se describen los roles que desempeñarían cada uno de los miembros del equipo entre ASBANC y AIUKEN, y que forman parte del servicio.

Tabla 11.1: Posiciones y perfiles

Posición	Perfil	Funciones
Comité Ejecutivo	El Comité Ejecutivo es el máximo responsable del éxito del servicio, sus miembros en conjunto tomarán las decisiones estratégicas y de asignación de recursos de sus respectivas organizaciones para asegurar el cumplimiento de los mismos	- Evaluar la gestión de los gerentes de proyecto y demás cargos establecidos en el equipo de trabajo, encaminar dicha gestión y, de ser necesario, realizar cambios en la asignación de los distintos recursos. - Aprobar toda nueva versión tanto del equipo de trabajo como del plan de trabajo.
Director Ejecutivo ASBANC	El Director Ejecutivo de ASBANC deberá ser un alto ejecutivo con la autoridad necesaria para asignar recursos de ASBANC y de representar los intereses de la organización ante el Comité Ejecutivo.	- Responsable de cada una de las responsabilidades específicas detalladas para el Comité Ejecutivo. - Realizar la preventa del servicio, gracias al alto grado de relacionamiento que mantiene con los clientes.
Director CSIRT AIUKEN	El Director CSIRT será responsable de las acciones estratégicas para generar la venta de servicios CSIRT ofrecidos por ASBANC	- Participar en la evaluación la demanda de los servicios que entrega el mercado local y establecer el modelo de comercialización para los nuevos servicios no catalogados
Gerente de Proyecto ASBANC	El Gerente de Proyecto ASBANC será el responsable directo de la ejecución de actividades del plan de trabajo por parte del equipo de ASBANC	- Supervisar y direccionar el trabajo de los demás integrantes del equipo de ASBANC en relación al objeto del contrato marco
Gerente de Proyecto AIUKEN	Lidera la gestión de la entrega de los diferentes servicios CSIRT aprovisionados a los clientes de ASBANC	- Se ocupa del gobierno en todas las áreas de sus servicios, incluyendo - Generar y/o supervisar los informes de servicio
Ejecutivo Administrativo ASBANC	Recopilador de Informacion.	- Recolectar y administrar toda la documentación que se desprenda del Contrato Marco
Ejecutivo de Mercadeo ASBANC	El Ejecutivo de Mercadeo será el responsable de manejar la comunicación comercial hacia los CLIENTES	- Establecer un plan de marketing con la aprobación de los Gerentes de Proyecto
Jefe Técnico ASBANC	El Jefe Técnico será la contraparte a la interna de ASBANC para manejar la comunicación con el Ingeniero de Seguridad y los Operarios SOC de AIUKEN	- Apoyar como nexo en la comunicación técnica entre AIUKEN, y los bancos
Ejecutivos Comerciales ASBANC	Los Ejecutivos Comerciales ASBANC liderarán la apertura de canales de comunicación hacia los CLIENTES	- Aportar a la actualización constante de la base de datos de contactos de CLIENTES - Realizar presentaciones y exposiciones de soluciones y servicios de CIBERSEGURIDAD

Ejecutivo Preventa AIUKEN	Ser de nexo entre los Bancos y ASBANC	- El Ejecutivo Preventa apoyará en la elaboración y diseño de propuestas de solución de servicios CSIRT,
Ingeniero de Seguridad	Aplicación técnica de los diseños del Ejecutivo Preventa	- Analizar, solucionar problemas e investigar anomalías de los sistemas de información relacionados con la seguridad sobre la plataforma de seguridad, tráfico de red, archivos, alertas basadas en seguridad y registros.
Operarios CSIRT	Los Operarios CSIRT son los ingenieros de primer, segundo y tercer nivel, como también sus supervisores y gerentes	- Las funciones se detallan en los puntos 11.3.1, 11.3.2 y 11.3.3

Fuente: Autor de la tesis

11.3.1 Análisis y Respuesta:

Tier 1: Se ocupa de recibir las llamadas de los usuarios afectados (tickets) y la captura de alertas y advertencias en el SIEM u otra consola (s) de sensores en tiempo real.

Tier 2: Se ocupa de la intervención de Ciberincidente, empleando el tiempo que requiera para eliminar la amenaza.

Tendencias: En este modelo de CSIRT existe un grupo de operación que se encarga del análisis y tendencias de Ciberinteligencia y además de la observación de actividad de la red y de estudiar las táctica, técnicas y procedimientos de los atacantes.

11.3.2 Escaneo y Evaluación:

Escaneo: Se refiere a un grupo de operación con una serie de capacidades que realiza escaneos rutinarios en la red y se ocupa de investigar las posibles vulnerabilidades en los sistemas de la circunscripción., esta tarea a menudo aparenta ser la más ambigua porque a los analistas se les requiere que realicen una búsqueda de amenazas no estructuradas de composición abierta que no son visibles por el radar.

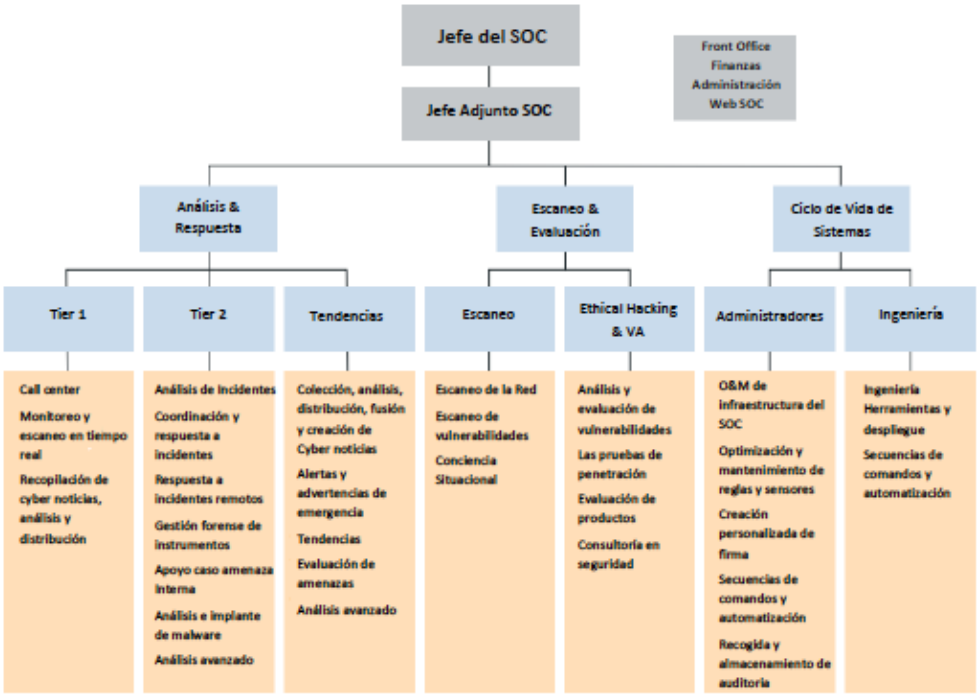
Ethical Hacking & VA: Este grupo de intervención está compuesto por recursos con mayor iniciativa, habilidades y capacidades analíticas que los demás analistas del SOC.

11.3.3 Ciclo de Vida de Sistemas:

Administradores: En el equipo de recursos de administración de los sistemas, es probable que se deba asignar a una o dos personas dedicadas a cada uno de los paquetes de sensores y reglas más importantes del SIEM, asimismo, aunque no todas las organizaciones integran en su catálogo de servicios SOC el mantenimiento de los dispositivos de protección perimetral, esto puede ser incluido en el marco del ciclo de vida de los sistemas como un tercer equipo con funciones de soporte técnico

Ingeniería: El grupo de ingeniería debe mantenerse al tanto de los principales retos del grupo de operaciones y de los "puntos débiles" para aprovechar ágilmente las soluciones aplicadas

Figura 11.2: Organigrama del CSIRT



Fuente: AIUKEN (2018)

11.4 Conclusiones:

Se describio el funcionamiento a nivel organizacional del servicio, en el mismo es importante resaltar la figura de los directores que son los responsables de administrar los recursos.

CAPÍTULO XII. PLAN DE OPERACIONES

En este capítulo se explicará la mecánica de operación del servicio que ASBANC realizaría, intermediando entre los bancos y el partner de negocios, en el capítulo VI se graficó que dentro del modelo de negocios la parte comercial sería ofrecida por ASBANC, mientras que la parte tecnológica y operativa la proveería la empresa AIUKEN basando la ejecución del servicio en los procesos de atención de incidentes y agilidad de respuesta que un CSIRT posee.

12.1 Estrategia de operaciones:

Al ser un servicio operado por un tercero, ASBANC reduce el nivel de inversión que necesita para poder operar sin embargo el presente capítulo pretende explicar cual sería la lógica de funcionamiento del servicio ya que implica una conexión hibrida entre dos infraestructuras, la poseen los bancos y la del CSIRT ubicado en España donde se encuentran los servicios de Ciberseguridad que tiene la empresa AIUKEN.

12.2 Procesos operativos clave:

Dentro de los procesos operativos planteados para dar el servicio se platean básicamente dos niveles el comercial y el proceso operativo, donde el proceso comercial será operado íntegramente por ASBANC y el proceso operativo por la empresa AIUKEN, sin embargo, ambas empresas deben estar expresamente coordinadas para poder brindar el servicio.

Figura 12.1: Procesos Clave

Fuente: Autor de la tesis

12.2.1 Proceso captar y mantener al proveedor:

Este proceso es una parte critica de la operación, ya que el servicio es de propiedad de la empresa AIUKEN, es por ello por lo que debe existir un alto nivel de relacionamiento entre ambas partes para que la sociedad se consolide ante discrepancias con la competencia dentro del mercado financiero, es por ello que ante el surgimiento

de problemas que pongan en peligro dicha alianza comercial se mantengan unidas las partes por el alto grado de compromiso que deba existir.

12.2.2 Proceso comercial:

Este proceso se explicó dentro del capítulo IX, en donde se indicaron las actividades que conlleva la parte comercial y como se interrelaciona con el proveedor de servicios, en este caso la empresa AIUKEN.

12.2.3 Proceso Operativo:

Cuando existe algún inconveniente con los servicios, los bancos tendrán que comunicarse al número 612-3390 para comunicarse bajo la modalidad 24x7 en la cual seria atendido inicialmente por el centro de atención telefónica, y que luego este derivaría las atenciones a Chile donde se encuentran los equipos de respuesta, por ello se puede ver en la figura 8.3 los principales grupos de trabajo operativos que soportarían la atención con los bancos.

12.2.3.1 Atención de Incidentes:

El principal enfoque del CSIRT será utilizar la tecnología y herramientas para la detección preventiva de eventos de seguridad, operando servicios de forma gestionada y prevaleciendo su capacidad de reacción, al ofrecer un CSIRT con cierta madurez de circunscripción y con mayor número de recursos, se puede aprovechar los métodos y mejores prácticas para detectar incidentes de forma autónoma, con sondas, recolectores, sensores y una plataforma SIEM donde el equipo de analistas cualificados de AIUKEN recopile datos de apoyo, realice análisis y pueda responder inconvenientemente considerando la creciente sofisticación y opacidad de los ataques, un CSIRT está obligado a considerar todo el ciclo de vida del ciberataque, el mismo que se detalla en la tabla 12.1.

Por ello ante un incidente el CSIRT se esforzará por detectar y responder al Ciberdelincuente, no sólo cuando manifiesta su ataque sobre un objetivo concreto, sino durante todo el ciclo de vida de la ofensiva, desde el reconocimiento e identificación de cualquier presencia no autorizada en los sistemas bajo el control del CSIRT.

Gestionando y utilizando el conocimiento del ciclo de vida integral del Ciberataque permitirá a los recursos del CSIRT desarrollar un enfoque más holístico para la detección y análisis de cualquier tipo de evidencia maliciosa o no autorizada bajo la circunscripción del CSIRT, en ese sentido el CSIRT deberá reconocer que la realidad de los ataques podría iniciarse en múltiples segmentos de su arquitectura tecnológica sobre la red de BANCARED.

Tabla 12.1: Fases del Ciclo de Vida del Ciberataque

Fase del Ciclo de Vida	Descripción	Síntoma
Reconocimiento	El adversario identifica e investiga los objetos	Web mining contra sitios web corporativos y lista de asistentes de conferencias en línea.
Weaponize (militarizarse)	El conjunto de herramientas de ataque se empaqueta para la entrega y ejecución en ordenador o red de la víctima.	El adversario crea un documento a troyanizado en formato portátil (PDF), y el archivo contiene sus instrumentos de ataque.
Deliver (entrega)	La herramienta avanzada o instrumentos de ataque envasados hacen diana.	El adversario envía un correo electrónico de phishing que contiene el archivo troyanizado a su lista de objetivos.
Exploit	El ataque inicial en el destino se materializa.	El usuario abre el archivo troyanizado y se ejecuta el software malicioso.
Control	El adversario comienza a dirigir el sistema victima y ejecutar acciones.	El adversario instala herramientas adicionales en el sistema victima.
Execute	El adversario emprende el cumplimiento de sus requisitos y materializa su misión	El adeversario comienza a obtener los datos deseados, a menudo utilizando el sistema de la victima como un punto de acceso a otros sistemas interno y a la red.
Maintain	Se lográ acceso a largo plazo.	El adversario ha conseguido puertas traseras ocultas en la red de destino que le facilita el reingreso regularmente.

Fuente: Autor de la Tesis

Utilizando el conocimiento de todo el ciclo de vida ataque cibernético mostrado en la tabla 8.2, permitiría adoptar un enfoque más holístico para la detección y análisis. La instrumentación de sensores de redes de la circunscripción no sólo debe proporcionar indicaciones de reconocimiento y de actividad de explotación, sino también debe revelar la presencia de herramientas de acceso remoto que se deben utilizan en el control y ejecución de las fases. Por otra parte, la evidencia de un exploit puede ser difícil de descubrir, teniendo en cuenta que puede ser no conocido (ataque "0-day") o puede ser

no percibido en la red.

El CSIRT debe comprender que el origen de los ataques puede ocurrir en varias partes a través de tráfico de red, o en la BIOS del sistema huésped, firmware, disco duro, medios extraíbles, software a nivel de sistema y aplicaciones en la memoria, etc.

Este reconocimiento facilita la comprensión por parte de los operadores de cuándo y cómo estos sensores implementados pueden ser ineficaces, inválido o simplemente esquivado. El CSIRT deberá desplegar y desarrollar una diversidad de técnicas para englobar la comprensión y capacidad de defender su circunscripción durante todas las fases del ciclo de vida del ciberataque

12.2.3.2 Agilidad de Respuesta

Por principio conceptual un CSIRT debe invertir muchísimo esfuerzo sólo para mantener la capacidad de evolucionar al mismo ritmo de progreso que sus adversarios.

ASBANC deberá tener en cuenta cuestiones como el diseño de las infraestructuras, el proceso de control de cambios, conocimientos ambiguos, responsabilidades contradictorias, el bajo rendimiento de la arquitectura de red, los controles descentralizados e incluso la aplicación de políticas y procedimientos laboriosos que socavan la capacidad del CSIRT para detectar y repeler los ciberataques con mayor velocidad, y saber conjugar su autoridad para para intervenir con libertad cuando la falta de agilidad sea un obstáculo para la consecución del objetivo.

La gestión proactiva del ciberriesgo es de importancia crítica para la sostenibilidad y la competitividad de cualquier CSIRT. Al exponer a ensayos y validación los equipos de ciberseguridad, y luego aumentar la resiliencia organizacional para desarrollar la interacción con la gestión de crisis corporativa, la gestión de riesgos, las comunicaciones y los equipos y sistemas de continuidad del negocio permitirá a ASBANC desarrollar una capacidad de ciberrespuesta ágil.

El CSIRT podrá destacar por varias razones, pero una capacidad de operación ágil y resolutiva debe ser uno de sus desempeños más destacados. Aunque los recursos del

CSIRT de ASBANC pudieran, sigue existiendo un distanciamiento entre la rapidez de movimiento de un atacante y la agilidad con la cual el defensor decide el mejor enfoque de respuesta y con qué rapidez puede bloquearlo.

Desarrollar inteligencia sobre las intenciones y motivaciones de hacktivistas, delincuentes organizados, los gobiernos malintencionados de ciertos y otros especialistas permitirá a ASBANC posicionar el ciberriesgo como una consideración de negocio para implementar un proceso de gestión de ciberamenazas proactiva y reactiva. Esto también sirve como ejemplo de que la ciberseguridad es la responsabilidad de todos los recursos de ASBANC.

Desarrollar métodos de respuesta rápida y efectiva de incidentes es fundamental durante las primeras horas de un ataque y asegura la correcta toma de decisiones, influye positivamente en el resultado de la investigación y minimiza el riesgo de mala reputación.

Para que el equipo de respuesta se sienta con la libertad de actuar en el caso de un ciberincidente el CSIRT debe tener un proceso gestionado, repetible, robusto y que sea abierto y transparente, conociendo el quién, cómo y por qué de un ciberataque permitirá brindar una respuesta que conviene contra la amenaza y mantendrá la seguridad, integridad y disponibilidad de los activos críticos.

Es importante resaltar que la respuesta a un ciberataque implica analizar más allá de la respuesta técnica. Todo el personal asignado a responder deberá estar preparado para trabajar con los medios de comunicación, cooperar con las autoridades nacionales, conocer la manera de cumplir con las obligaciones legales relativas a la divulgación de información confidencial del cliente interno o externo como consecuencia de un ataque.

12.2.4 Costos de Operación:

Al ser un servicio tercerizado, ASBANC los costos de operación de los servicios son menores, es por ello por lo que en la tabla 12.2 se pueden ver los costos mensuales y/o anuales de los diferentes servicios ofrecidos, así como también los pagos únicos a realizarse ya sea por temas de licenciamiento o despliegue y/o configuración.

Tabla 12.2: Costos de Operación

	Pago Único		**Pago Recurrente**	
Cyber Security Consulting Services	-	-	mensual	$10,500
			anual	$115,500
Cyber Security Assessment Consulting	Licencia	$3,200.00	mensual	$4,500
	Despliegue y Configuración	$12,000.00	anual	-
eBanking Security Services	Despliegue y configuración	$12,000.00	mensual	$9,000
			anual	$99,000
Ethical Hacking Professional Services	Despliegue y configuración	$3,000.00	mensual	$8,500
			anual	$82,500
Gestión de la Ingeniería Social	Despliegue y configuración	$5,000.00	mensual	$4,000
			anual	$44,000
Managed Security Services	Despliegue y configuración	$9,000.00	mensual	$3,000
			anual	$33,000
Pentesting Services	Despliegue y configuración	$9,000.00	mensual	$4,500
			anual	$49,500
Security Code Review	Despliegue y configuración	$9,000.00	mensual	$4,500
			anual	$49,500
Visibility Analytics Services	Licencia	$3,200.00	mensual	$3,500
	Despliegue y configuración	$13,500.00	anual	$38,500
Vulnerability Assessment Services	Licencia	$22,160.00	mensual	$3,000
	Despliegue y configuración	$5,000.00	anual	$33,000
CSIRT	-	-	mensual	$300
			anual	$3,600

Fuente: Autor de la tesis

Asimismo, en la tabla 9.1 se puede observar los gastos relacionados al proceso comercial que se ha dimensionado para poder realizar la venta del servicio.

12.3 Aspectos legales y societarios:

Al establecer una relación societaria con la empresa AIUKEN, se establecen una serie de pautas las mismas que se explican en el Anexo X, en la misma se establecen las responsabilidades, alcances y formas de pago.

12.4 Conclusiones

De lo anteriormente se puede concluir que la parte critica del servicio radica en el lado de la empresa AIUKEN ya que ellos son los que proveen el servicio de CSIRT, la relación que ASBANC mantiene es básicamente la de un reseller ya que tiene los contactos y las relaciones con el mercado meta.

CAPÍTULO XIII. EVALUACION ECONOMICA Y FINANCIERA

En este capítulo se determinará la viabilidad económico-financiero del proyecto con un horizonte de evaluación de 5 años, en la que se calculan los flujos de caja de forma mensual y se determina el Valor Presente (VAN), asimismo se realizará un Análisis de Sensibilidad que permitirá determinar la resistencia del modelo financiero ante cambios en los costos, precio de venta y cantidad demandada.

Cabe señalar que la tasa de descuento aplicada al flujo económico contempla la tasa exigida por la gerencia general de ASBANC que asciende al 20% para la evaluación de los nuevos servicios.

13.1 Supuestos

- Se asume que existe no existe una tendencia al incremento del tipo de cambio.
- Se asume que no existe un ajuste de precios por inflación anual.
- El financiamiento del proyecto es sustentado al 100% con capital propio.
- El pronóstico del crecimiento de la contratación de los servicios de Ciberseguridad será moderado.
- La facturación de los servicios se realiza de forma mensual y los bancos cancelan estos servicios dentro del mes de servicio ofrecido.
- Los accionistas no retiran las utilidades generadas en el periodo del proyecto.
- Se evaluará el flujo económico descontándolo a una tasa anual en función de lo exigido por la organización.
- Los cálculos se realizan sin incluir el IGV

13.2 Inversión inicial

El total de la inversión para el presente proyecto asciende a US$14,080, dicha inversión se encuentra distribuida de la siguiente manera: Realización de Focus Group, Contratación de Experto Ciberseguridad, Lanzamiento del Servicio, Presentación a Gerentes Generales.

Tabla 13.1: Inversión Inicial

Focus	$1,080	dolares
Consultor	$2,000	dolares
Lanzamiento	$8,000	dolares
Presentacion a GG	$3,000	dolares

Fuente: Autor de la tesis

13.3 Estado de Resultados

A continuación, se muestra en la Tabla 13.5 el Estado de Resultados del proyecto expresado en dólares americanos los cuales tienen las siguientes componentes que se explican a continuación, las cifras mostradas corresponden a flujos mensuales del primer año de evaluación para los costos de ventas y gastos operacionales, las ventas y el estado de resultados se muestran de forma anualizada, el detalle de todas estas cifras mostradas se muestra en el Anexo XIII.

a) Ventas: referida a la cantidad de servicios MSS y SOC contratado por cada una de las entidades las cuales se muestran en la Tabla 13.2 donde se encuentra la proyección de ventas realizadas por la duración del proyecto.

Tabla 13.2: Proyección de ventas anual

Periodo Anual	0	1	2	3	4	5
Ventas		232,750	720,750	929,500	1,045,000	1,045,000

Fuente: Autor de la tesis

b) Costo de Ventas: compuesto por los costos variables asociados a la venta de los servicios correspondientes a la instalación del SOC, la instalación del SIEM y el servicio del SIEM propiamente dicho, dichos cálculos pueden ser visualizados en la tabla 13.3

Tabla 13.3: Costo de ventas mensual primer año

	Jul	Ago	Set	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun
SOC	-	3,000	3,000	3,000	3,000	3,000	6,000	6,000	6,000	6,000	6,000	6,000
CSIRT	-	300	300	300	300	300	600	600	600	600	600	600
eBanking Protection	-	-	-	-	-	-	-	-	-	9,000	9,000	9,000
Ingeniería Social	-	-	-	-	-	-	4,000	4,000	4,000	4,000	4,000	4,000
Instalacion SOC	-	9,000	-	-	-	-	9,000	-	-	-	-	-
Instalacion SIEM	-	9,000	-	-	-	-	9,000	-	-	-	-	-
SIEM	-	1,000	1,000	1,000	1,000	1,000	2,000	2,000	2,000	2,000	2,000	2,000
Instalación eBanking	-	-	-	-	-	-	-	-	-	12,000	-	-
Instalación Ingeniería Social	-	-	-	-	-	-	5,000	-	-	-	-	-
Coste de Ventas	-	22,300	4,300	4,300	4,300	4,300	35,600	12,600	12,600	33,600	21,600	21,600

Fuente: Autor de la tesis

c) Gastos de operación: Compuesto por gasto de personal, el cual incluye el costo fijo del vendedor, sus comisiones, sus beneficios sociales, el sueldo de un personal operativo, los gastos administrativos asociados al proceso de facturación del servicio y los gastos de marketing.

Tabla 13.4: Gastos de operación mensual primer año

	Jul	Ago	Set	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun
Gastos de Personal	2,864	3,339	2,864	2,864	2,864	2,864	3,339	2,864	2,864	2,864	2,864	2,864
- Sueldo de vendedor	463	463	463	463	463	463	463	463	463	463	463	463
- Comisión del Vendedor	278	278	278	278	278	278	278	278	278	278	278	278
- Beneficios sociales del vendedor	1,327	1,327	1,327	1,327	1,327	1,327	1,327	1,327	1,327	1,327	1,327	1,327
- Sueldo de personal operativo	796	796	796	796	796	796	796	796	796	796	796	796
- Beneficios sociales del personal operativo	1,286	1,286	1,286	1,286	1,286	1,286	1,286	1,286	1,286	1,286	1,286	1,286
Marketing	0	190	190	190	190	190	505	505	505	730	730	730
Gastos Administrativos	0	0	190	190	190	190	190	505	505	505	730	730
Total	2,864	3,529	3,244	3,244	3,244	3,244	4,034	3,874	3,874	4,099	4,324	4,324

Fuente: Autor de la tesis

Sobre el análisis del Estado de Resultados se observa que el proyecto es rentable a partir del primer año con una utilidad operativa positiva, la cual se incrementa considerablemente dentro del periodo de evaluación.

Tabla 13.5: Estado de Resultados

Periodo	0	1	2	3	4	5
Clientes Producto Base		2	4	5	5	5
Clientes eBanking		1	2	3	3	3
Clientes Ingeniería Social		1	3	3	3	3
Inversion Inicial	14,080					
Ventas		232,750	720,750	929,500	1,045,000	1,045,000
SOC + CSIRT		161,500	357,000	442,000	467,500	467,500
eBanking Protection		33,750	213,750	281,250	371,250	371,250
Ingenieria Social		37,500	150,000	206,250	206,250	206,250
Costo de Ventas		177,100	461,700	610,600	665,500	665,500
SOC		51,000	117,000	156,000	165,000	165,000
CSIRT		5,100	11,700	15,600	16,500	16,500
eBanking Protection		27,000	162,000	225,000	297,000	297,000
Ingeniería Social		24,000	92,000	132,000	132,000	132,000
Instalacion SOC		18,000	9,000	9,000	-	-
Instalacion SIEM		18,000	9,000	9,000	-	-
SIEM		17,000	39,000	52,000	55,000	55,000
Instalación eBanking		12,000	12,000	12,000	-	-
Instalación Ingeniería Social		5,000	10,000	0	-	-
Utilidad Bruta		**55,650**	**259,050**	**318,900**	**379,500**	**379,500**
Gastos de Personal		35,320	35,320	34,845	34,370	34,370
- Sueldo de vendedor		5,556	5,556	5,556	5,556	5,556
- Comisión del vendedor		950	950	475	-	-
- Beneficios sociales del vendedor		3,333	3,333	3,333	3,333	3,333
- Sueldo de personal operativo		15,926	15,926	15,926	15,926	15,926
- Beneficios sociales del personal operativo		9,556	9,556	9,556	9,556	9,556
Marketing		15,432	15,432	15,432	15,432	15,432
Gastos Administrativos		4,655	14,415	20,095	22,800	22,800
Utilidad Operativa		**243**	**193,883**	**248,528**	**306,898**	**306,898**
Impuesto a la renta (30%)		11,841	46,910	82,973	102,419	102,419
Utilidad Neta		**-11,598**	**146,972**	**165,554**	**204,478**	**204,478**

Fuente: Autor de la tesis

13.4 Flujo de Caja Económico

- Ingresos operativos, correspondientes a las ventas realizadas en el periodo del proyecto.
- Egresos operativos, correspondientes a los costos de ventas y de operación relacionados al Estado de resultados.

Tabla 13.6: Flujo Caja Económico

Periodo	0	1	2	3	4	5
Flujo Operativo						
- Ingreso Operativo		232,750	720,750	929,500	1,045,000	1,045,000
- Egreso Operativo		-244,348	-573,778	-763,946	-840,522	-840,522
FC Operativo		-11,598	146,972	165,554	204,478	204,478
Flujo Inversiones						
- En Gastos Preoperativos	-14,080					
FC Inversiones	-14,080					
Flujo de Caja Económico	**-14,080**	**-11,598**	**146,972**	**165,554**	**204,478**	**204,478**

Fuente: Autor de la tesis

13.4.1 Horizonte de Evaluación

El horizonte de evaluación es de 5 años.

13.4.2 Indicadores Financieros

13.4.2.1 Costo del Accionista (ke)

Se considera una tasa de retorno del 20% anual (ke), el cual es exigido por el accionista de acuerdo con la política para el desarrollo de nuevos servicios en la empresa.

13.4.3 Evaluación Económica Financiera

13.4.3.1 Indicadores de Rentabilidad

Utilizando la información del Estado de Resultados de la Tabla 13.7 se pueden determinar los siguientes indicadores de rentabilidad, bajo un escenario esperado:

Tabla 13.7: Márgenes de rentabilidad (dólares americanos)

	1	2	3	4	5
Utilidad Bruta	55,650	259,050	318,900	379,500	379,500
Utilidad Operativa	243	193,883	248,528	306,898	306,898
Utilidad Neta	-11,598	146,972	165,554	204,478	204,478
Margen Bruto	**23.91%**	**35.94%**	**34.31%**	**36.32%**	**36.32%**
Margen Operativo	**0.10%**	**26.90%**	**26.74%**	**29.37%**	**29.37%**
Margen Neto	**-4.98%**	**20.39%**	**17.81%**	**19.57%**	**19.57%**

Fuente: Autor de la tesis

a) Margen Bruto: permite definir que se cubre el costo de producción que incluye los costos variables del proyecto, el promedio que arroja el proyecto es 33.36%.
b) Margen Operativo: se determina que el promedio se encuentra en 22.50% que cubre los costos operativos, obteniéndose una rentabilidad a este nivel.
c) Margen Neto: se determina que el promedio se encuentra en 14.47% que cubre los costos operativos, obteniéndose una rentabilidad a este nivel.

13.4.3.2 Valor Actual Neto

Para determinar el Valor Actual Neto del proyecto se utiliza la información de del flujo de caja económico (ver Anexo XIII), utilizando la tasa del accionista correspondiente al 20% anual, obteniéndose una rentabilidad de US$ 354,911

13.4.3.3 Punto de Equilibrio

El punto de equilibrio se logra con 3 Clientes que permite cubrir los costos fijos y variables del proyecto.

13.5 Análisis de Sensibilidad

De acuerdo con la investigación en campo y a la naturaleza propia del negocio se realizó un análisis unidimensional y bidimensional, los que permitirán determinar la sensibilidad del proyecto ante variaciones del precio de venta, los costos de ventas y el aumento de los gastos operativos.

13.5.1 Análisis Unidimensional

Este análisis se caracteriza porque se sensibiliza el modelo respecto de una variable, en el presente acápite se analizará los cambios porcentuales de las variables económicas que son el precio de venta, el costo de producción y el tipo de cambio, determinando si los cambios impactan de forma directa sobre la rentabilidad del proyecto.

a) El Precio de Venta

Se puede observar en la Tabla 13.8 el precio de venta es una variable muy crítica pues tiene un gran impacto sobre los flujos, afectando de manera directa la rentabilidad del proyecto y ésta se ve afectada de variables no controlables tanto de lado de la oferta, como de la demanda, se observa que el precio de venta se afecta más allá del 20%.

Tabla 13.8: Análisis Unidimensional Precio

		VAN
Variacion % Precio		354,911
	-40.00%	-307,635
	-35.00%	-202,190
	-30.00%	-100,363
	-25.00%	-22,008
	-20.00%	55,204
	-15.00%	131,356
	-10.00%	207,040
	-5.00%	281,392
	0.00%	354,911
	5.00%	428,104
	10.00%	500,899
	15.00%	573,645
	20.00%	645,985
	25.00%	718,297
	30.00%	790,609
	35.00%	862,921
	40.00%	935,234

Fuente: Autor de la tesis

b) El Costo de Ventas

De los cálculos realizados se observa que el costo de producción del servicio afecta de manera directa la rentabilidad del proyecto cuando se incrementan los costos mas allá del 30%, tal como se puede observar en la Tabla 13.9.

Tabla 13.9: Análisis Unidimensional Costo de Ventas

		VAN
Variacion % Costo		**354,911**
	-40.00%	743,959
	-35.00%	695,556
	-30.00%	647,153
	-25.00%	598,750
	-20.00%	550,348
	-15.00%	501,945
	-10.00%	453,126
	-5.00%	404,191
	0.00%	**354,911**
	5.00%	305,368
	10.00%	255,273
	15.00%	204,395
	20.00%	153,344
	25.00%	101,787
	30.00%	49,630
	35.00%	**-2,811**
	40.00%	**-55,614**

Fuente: Autor de la tesis

c) La Demanda

De los cálculos realizados se observa que la cantidad demandada no afecta de manera directa la rentabilidad del proyecto como se observa en la Tabla 13.10

Tabla 13.10: Análisis Unidimensional de la Demanda

		VAN
Variacion % Demanda		**354,911**
	-40.00%	279,745
	-35.00%	298,617
	-30.00%	315,276
	-25.00%	334,086
	-20.00%	352,442
	-15.00%	376,294
	-10.00%	392,524
	-5.00%	408,753
	0.00%	**354,911**
	5.00%	367,836
	10.00%	380,761
	15.00%	393,685
	20.00%	406,610
	25.00%	419,535
	30.00%	432,459
	35.00%	445,384
	40.00%	458,309

Fuente: Autor de la tesis

13.5.2 Análisis Bidimensional

En este análisis se realiza el cálculo del VAN mediante la variación de dos variables, lo cual permite determinar la sensibilidad del precio ante variaciones ocurridas de los costos y el tipo de cambio.

a) Variación del precio vs el costo

Se observa en la tabla 13.11 que la rentabilidad del proyecto se ve afectada ante variaciones en el precio reduciéndose 20% y aumentando los costos en 5%.

b) Variación del precio vs la cantidad demandada

Según se observa 13.12 se puede determinar que el proyecto es viable mientras que la cantidad demandada no baje del 35%, y el precio de venta no baje más allá del 20%.

Tabla 13.11: Variación precio vs costo

	Variacion % Costo																	
	354,911	-40%	-35%	-30%	-25%	-20%	-15%	-10%	-5%	0%	5%	10%	15%	20%	25%	30%	35%	40%
Variacion % Precio	-40.00%	162,340	111,798	60,532	8,518	(44,087)	(98,064)	(166,640)	(237,138)	(307,635)	(378,133)	(448,631)	(519,128)	(589,626)	(660,124)	(730,621)	(801,119)	(871,617)
	-35.00%	236,120	186,565	136,174	84,950	33,254	(19,127)	(72,114)	(131,883)	(202,190)	(272,688)	(343,186)	(413,683)	(484,181)	(554,679)	(625,177)	(695,674)	(766,172)
	-30.00%	309,597	260,284	210,789	160,487	109,368	57,990	5,732	(46,969)	(100,363)	(167,243)	(237,741)	(308,239)	(378,736)	(449,234)	(519,732)	(590,229)	(660,727)
	-25.00%	382,398	333,696	284,447	234,952	184,800	133,786	82,520	30,468	(22,008)	(74,812)	(133,095)	(202,794)	(273,291)	(343,789)	(414,287)	(484,784)	(555,282)
	-20.00%	454,710	406,307	357,582	308,538	259,116	209,110	158,204	106,938	55,204	2,945	(49,850)	(102,887)	(168,109)	(238,344)	(308,842)	(379,340)	(449,837)
	-15.00%	527,022	478,619	430,217	381,468	332,452	283,172	233,335	182,622	131,356	79,892	27,681	(24,890)	(77,693)	(134,326)	(203,648)	(273,895)	(344,392)
	-10.00%	599,334	550,932	502,529	454,126	405,354	356,365	307,085	257,417	207,040	155,774	104,489	52,417	71	(52,732)	(105,553)	(169,138)	(239,188)
	-5.00%	671,647	623,244	574,841	526,438	478,035	429,240	380,278	330,998	281,392	231,210	180,192	128,926	77,153	24,894	(27,772)	(80,574)	(135,557)
	0.00%	743,959	695,556	647,153	598,750	550,348	501,945	453,126	404,191	354,911	305,368	255,273	204,395	153,344	101,787	49,630	(2,811)	(55,614)
	5.00%	816,271	767,868	719,465	671,062	622,660	574,257	525,854	477,012	428,104	378,824	329,343	279,335	228,563	177,512	126,349	74,366	22,107
	10.00%	888,286	840,180	791,777	743,375	694,972	646,569	598,166	549,759	500,899	452,018	402,738	353,318	303,398	252,730	201,679	150,628	99,015
	15.00%	960,295	912,337	864,090	815,687	767,284	718,881	670,478	622,076	573,645	524,785	475,925	426,651	377,293	327,375	276,898	225,847	174,796
	20.00%	1,032,304	984,346	936,388	887,999	839,596	791,193	742,791	694,388	645,985	597,531	548,671	499,811	450,564	401,268	351,351	301,066	250,015
	25.00%	1,104,312	1,056,355	1,008,397	960,311	911,908	863,505	815,103	766,700	718,297	669,894	621,417	572,557	523,697	474,477	425,197	375,326	325,138
	30.00%	1,176,321	1,128,363	1,080,406	1,032,448	984,220	935,818	887,415	839,012	790,609	742,207	693,804	645,303	596,443	547,583	498,390	449,110	399,301
	35.00%	1,248,330	1,200,372	1,152,414	1,104,457	1,056,499	1,008,130	959,727	911,324	862,921	814,519	766,116	717,713	669,189	620,329	571,469	522,304	473,024
	40.00%	1,320,339	1,272,381	1,224,423	1,176,465	1,128,508	1,080,442	1,032,039	983,636	935,234	886,831	838,428	790,025	741,622	693,075	644,215	595,355	546,217

Fuente: Autor de la tesis

Tabla 13.12: Variación precio vs demanda

	Variacion % Demanda																	
	354,911	-40%	-35%	-30%	-25%	-20%	-15%	-10%	-5%	0%	5%	10%	15%	20%	25%	30%	35%	40%
Variacion % Precio	-40.00%	(234,162)	(232,074)	(229,987)	(227,899)	(225,811)	(215,770)	(216,278)	(216,786)	(307,635)	(312,660)	(317,685)	(322,710)	(327,735)	(332,760)	(337,786)	(342,811)	(347,836)
	-35.00%	(152,295)	(147,251)	(142,206)	(137,162)	(132,118)	(119,110)	(116,661)	(114,212)	(202,190)	(204,263)	(206,335)	(208,408)	(210,496)	(212,655)	(214,815)	(216,974)	(219,134)
	-30.00%	(72,006)	(64,006)	(56,095)	(48,353)	(40,611)	(25,061)	(19,980)	(15,121)	(100,363)	(100,140)	(99,980)	(99,849)	(99,766)	(99,773)	(99,791)	(99,809)	(99,828)
	-25.00%	(7,512)	2,083	10,752	19,867	28,841	44,721	50,932	57,143	(22,008)	(19,673)	(17,338)	(15,003)	(12,668)	(10,333)	(7,998)	(5,673)	(3,370)
	-20.00%	51,689	62,578	72,045	82,935	93,824	111,063	119,340	127,617	55,204	59,795	64,387	68,954	73,507	78,060	82,613	87,066	91,462
	-15.00%	108,994	121,971	132,853	145,830	158,807	177,404	187,748	198,092	131,356	138,115	144,874	151,628	158,207	164,785	171,364	177,942	184,521
	-10.00%	166,299	181,178	193,660	208,726	223,791	243,746	256,156	268,566	207,040	215,890	224,637	233,381	242,126	250,870	259,615	268,359	277,104
	-5.00%	223,113	239,897	254,468	271,621	288,174	310,088	324,564	338,832	281,392	292,245	303,098	313,951	324,803	335,656	346,509	357,362	368,214
	0.00%	279,745	298,617	315,276	334,086	352,442	376,294	392,524	408,753	354,911	367,836	380,761	393,685	406,610	419,535	432,459	445,384	458,309
	5.00%	336,377	357,337	375,866	396,288	416,422	442,142	460,408	478,675	428,104	443,126	458,101	473,075	488,049	503,023	517,997	532,971	547,945
	10.00%	393,008	416,056	435,992	458,108	480,224	507,989	528,293	548,596	500,899	517,949	535,000	552,050	569,101	586,152	603,202	620,253	637,304
	15.00%	449,640	474,151	495,721	519,874	544,026	573,836	596,177	618,518	573,645	592,758	611,844	630,929	650,014	669,100	688,185	707,271	726,356
	20.00%	505,989	531,843	555,450	581,639	607,829	639,683	664,061	688,439	645,985	667,125	688,265	709,406	730,546	751,686	772,826	793,967	815,107
	25.00%	561,678	589,535	615,179	643,405	671,631	705,531	731,946	758,361	718,297	741,492	764,687	787,882	811,077	834,272	857,468	880,663	903,858
	30.00%	617,334	647,227	674,908	705,171	735,434	771,378	799,830	828,283	790,609	815,859	841,109	866,359	891,609	916,859	942,109	967,359	992,609
	35.00%	672,989	704,920	734,637	766,936	799,236	837,225	867,715	898,204	862,921	890,226	917,531	944,836	972,140	999,445	1,026,750	1,054,055	1,081,359
	40.00%	728,645	762,612	794,366	828,702	863,038	903,072	935,599	968,126	935,234	964,593	993,953	1,023,312	1,052,672	1,082,032	1,111,391	1,140,751	1,170,110

Fuente: Autor de la tesis

13.6 Análisis de Escenarios

En el presente acápite se analiza la variación de distintas variables que podrían interactuar antes variaciones que ocurriesen en la cantidad exportada de mangos, precio de venta y los costos de ello se determinan 03 escenarios, obteniéndose el valor presente para cada escenario y se muestra en la Tabla 11.13.

Se puede apreciar que ante un escenario pesimista la VAN del proyecto arroja una proyección de - US$332,921 en el esperado US$354,911 y en el optimista US$ 965,049.

Tabla 13.13: Escenarios Financieros

	Pesimista	Esperado	Optimista
Costo	40%	0	-20%
Demanda	-20%	0	40%
Inversion	50%	0	0
Precio	-20%	0	15%
VAN	-332,921	354,911	965,049

Fuente: Autor de la tesis

13.7 Conclusiones

El proyecto es viable, y resiste variaciones en la demanda, costo, pero es sensible ante cambios en el precio de ventas cuando este se disminuye más allá del 25%.

CAPÍTULO XIV. CONCLUSIONES Y RECOMENDACIONES

14.1 Conclusiones:

Se concluye que existe viabilidad financiera, operativa y comercial para implementar un CSIRT para el sistema financiero.

Se determina que el mercado meta es de 10 bancos, sin embargo el mercado potencial son 16 bancos.

Se empleará un modelo de negocios bajo la figura de alianza estratégica con una empresa internacional, que pueda brindar el respaldo y el posicionamiento adecuado para la atención de los clientes bancos a un precio competitivo.

Se determina que la rentabilidad del proyecto es de US$ 70,000 anuales para la organización, se cubre el costo de la tasa de descuento de 20% exigida para los proyectos presentados.

14.2 Recomendaciones

Dado que existe una oportunidad se recomienda implementar el proyecto de acuerdo a lo planificado en el plan de tesis, lo cual implica:

- Seleccionar al partner de negocio.
- Realizar el lanzamiento del servicio.
- Se asigne la función al personal operativo de ASBANC.
- Que se monitoree con la Superintendencia la publicación de la normativa respecto al tema de ciberseguridad a fin de facilitar la venta del servicio.

La empresa AIUKEN realice una evaluación de riesgo-impacto y pueda ser cuantificado el riesgo actual de no contar con un servicio de este tipo.

Anexo I – Guía de pautas - CSIRT

Encuadre: (5 minutos)

1. Opinión Personal – Toda opinión es válida – no hay respuestas buenas ni malas.
2.
3.
4. Finalidad de la reunión: ser un grupo que aporte ideas que permitan contribuir a las mejoras de la empresa.
5. Micrófono / Grabadora (Confidencialidad)
6. Breve presentación de cada uno

OBJETIVO:

El objetivo es indagar los siguientes aspectos:

CIBERSEGURIDAD Conocimiento del nivel riesgos al que está expuesto la entidad financiera, tipos de ataques que reciben y tipos de soluciones que conocen.

TEMAS:

ESFERA COGNITIVA, AFECTIVA Y CONDUCTUAL EN TEMAS DE SEGURIDAD Y MEDIO AMBIENTE

Dinámica (15 minutos)

Vamos a hacer un jueguito. Tengo acá unos papelógrafos y nos vamos a reunir en 2 grupos y vamos a trabajar el tema de Ciberseguridad.

Explicación sobre la dinámica:

Acá tenemos 2 imágenes de 2 personas en la entidad financiera (se enseña dibujo de un monigote, sin rostro para no sesgar). Al parecer son iguales, pero lo que los diferencia es su relación con el tema que vamos a tratar (Ciberseguridad)

El primero de ellos es una persona que es muy consciente del nivel de riesgo, el segundo de ellos es una persona que es poco consciente del nivel de riesgo que está expuesto la entidad financiera.

Para Ciberseguridad:

El tema para trabajar es: Conocimiento del nivel riesgos al que está expuesto la entidad financiera, tipos de ataques que reciben y tipos de soluciones que conocen.

El primer equipo va a trabajar este tema en función a la persona que están conscientes del nivel de riesgo de Ciberseguridad (se les entrega el papelógrafo):

- En la primera parte escribirán acerca de qué sabe esta persona con respecto del tema.
- En la segunda parte escribirán (y/o dibujarán) aquello que esta persona siente con respecto de este tema.
- En la tercera parte escribirán, en qué momentos del día a día aplica este tema y cómo así los aplica.

El segundo equipo va a trabajar el tema en función a la persona que están poco consciente con el nivel de riesgo de seguridad y a veces no es tan conscientes (se les entrega los papelógrafos)

- En la primera parte escribirán acerca de qué sabe esta persona con respecto del tema.
- En la tercera parte escribirán, en qué momentos del día a día aplica este tema y cómo así los aplica y en qué momentos no los aplica y por qué.

Una vez que terminen de trabajar los papelógrafos cada grupo procede a exponer Se explica que los demás equipos pueden aportar en las respuestas mencionadas por los otros equipos. Se procede a escribir todos los hallazgos relevantes en la pizarra.

Nivel cognitivo (8 minutos)

- ¿qué puso el primer grupo acerca de lo que sabe? ¿qué puso el segundo? ¿qué diferencias hay entre los 2 personajes? ¿por qué podrían existir ese tipo de diferencias? ¿qué puede estar pasando que hace que tengan diferente tipo de información?

Nivel conductual (8 minutos)

- ¿qué puso el primer grupo acerca de cómo lo aplica en el día a día? ¿qué puso el segundo acerca de en qué casos lo aplica y en qué casos no? ¿por qué creen que podrían existir ese tipo de diferencias? ¿a qué se deberá? ¿qué influye a ello?

Escenario de confluencia (15 minutos)

Ok, ahora vemos que todos ellos trabajan en el mismo lugar, es decir en una entidad financiera A. Entonces, imaginemos un día cualquiera, los 2 están trabajando en la misma área y se presenta una situación donde el tema debe tomarse en cuenta.

- ¿qué puede suceder?... ¿qué tipo de escenario es el más probable que suceda? ¿por qué? ¿cómo será la interacción entre estos 2 personajes? ¿cuáles son los issues positivos y negativos? ¿por qué? (se hace el mismo ejercicio con el otro escenario)

EXPERIENCIA PROPIA. TODOS (15 minutos)

(Ahora me gustaría preguntarle a Ud. Directamente).
¿Cómo viven el tema de Ciberseguridad en su actividad diaria? ¿Les resulta fácil o difícil contrarrestar ataques? Por qué Profundizar
Que es lo más difícil de cumplir Por qué Profundizar
¿Cómo detectan un incidente interno?
¿Cómo diferencian las operaciones normales de un ataque en cubierto? ¿Les resulta fácil o difícil diferenciar? Por qué Profundizar
¿Tienen visibilidad de sitios, perfiles de redes sociales o aplicación que usen de manera indebida el nombre de su empresa? ¿Es oportuna y suficiente la información que tienen sobre el uso indebido del nombre de su empresa? Por qué Profundizar
¿Han tenido oportunidades de usar nuevas soluciones de Ciberseguridad para salvaguardar la información comprometida? ¿Cuales?

PLAN DE SUGERENCIAS DE MEJORA (15 minutos)

Ahora nos vamos a conversar acerca de las sugerencias y oportunidades de mejora que se pueden tener para el tema que hemos trabajado hoy (Ciberseguridad).
Empecemos con el primero:
¿Qué sugerencias se podría dar para que todos conozcan de este tema y que lo apliquen (se pregunta lo mismo para el siguiente tema)
¿Cómo le gustaría trabajar para contrarrestar los ataques diarios? ¿Qué servicios o equipos tendría que tener para reducir el nivel de riesgo frente a un ataque encubierto (operaciones normales de un ataque encubierto)?

PRESENTACIÓN DEL PRODUCTO (15 minutos)

(Preguntas libre sobre el servicio. Carlos Álvarez)

En general, ¿Qué les parece este servicio de CSIRT? ¿Por qué? ¿Qué es lo que más le impacto de lo que acaba de mostrar?
¿Habían oído hablar de un sistema similar anteriormente? ¿Dónde? ¿Qué les parece este servicio?
¿Cómo agruparía estos servicios? ¿Por qué?
¿A usted le acomodaría usar este servicio? ¿Qué beneficio les parece que le traería este servicio?

Para finalizar, más allá de que sea una alternativa real de compra para Uds., o no, ¿qué aspectos de este servicio les resulta especialmente atractivos o positivos?, ¿algún otro?, ¿por qué?
Ahora, ¿Si tuvieran que adquirir algunos de los servicios mencionados, seria a corto, mediano o largo plazo?

Anexo II: Transcripción Focus Group

CSIRT

Bueno señores, muchas gracias, muy agradecido por el tiempo y por estar aquí, yo soy Angelina y quiero darle unas pautas para que la reunión salga lo mejor posible y luego nos presentamos, creo que algunos nos hemos estado conociendo, me parece que Víctor ha estado conversando. Si no nos vamos presentando para conocernos un poco y luego empezamos la dinámica.
Yo sólo quería darles un par de pautas que para mí son indispensables, la primera en la que ver con su sinceridad, apelo a ello al máximo, eso quería decir que si algo no saben, no conocen o no les gusta, critiquen con toda confianza, justamente en base a eso es que nosotros hacemos todas las programaciones y si sacamos al mercado productos que consideran que están buenos y no están tan buenos, se arruina todo, entonces por eso es que les pediría que seamos los más críticos y así los posibles y lo otro tiene que ver con lo mismo, es básicamente su individualidad ¿Qué implica? No importa si tienen a todo el grupo en contra, ustedes defiendan su posición hasta el final, no tratemos de convencernos unos a otros, la idea es rescatar información, eso es lo que yo necesito de ustedes, la información que pueda.
Entonces lo que les estaba diciendo básicamente es que defendamos su posición hasta el último momento, así tengan el grupo que piense diferente ¡No importa! Ustedes, su posición hasta el final.
Muy bien, vamos a presentarnos un poquito, para saber quiénes están frente a nosotros, comenzamos con Carlos, Carlos buenos días.

- Buenos días.

Carlos, cuéntanos un poquito, cuéntanos a que te dedicas, donde trabajas, cuéntanos un poco tu vida familiar quizás.

- Soy el oficial de seguridad de información de Banco Falabella, creo que me conoce la mayoría que está acá.

¿Mucho tiempo, cuánto tiempo en el puesto?

- Sí, ya 9 años.

¡Ah, bastante, uno de los pocos que dura tanto! Ya hoy en día la gente no dura en su trabajo tantos años.

- Sobre todo, los millennials.

Si, sobre todo los millennials, ¡Así es Carlos"!

- Sí, yo soy casi un millennials, porque ando con mi celular, con mis aplicaciones y todo el día trato de estar muy al día en esto porque es parte del día a día de mi trabajo y también soy casado, tengo 2 hijas universitarias.

¿Y te siguen los pasos o hacer otras cosas?

- No, hacen otras cosas.

OK, gracias Carlos, muy amable, pasó con Ángel ¿Qué me dices?

- Buenos días con todos, mi nombre es ángel Chávez como yo trabajo en el banco Ripley, soy analista de seguridad de la información, estoy encargado de diversos proyectos, incluyendo el tema de ASA, el tema de PCI, el tema de líderes personales dentro del banco, de hecho, recién esté trabajando en banca, antes venía trabajando en una de pagos, que era Leocast.

¿Y en puestos similares o hacías otra cosa?

- Puestos similares, de hecho, ahí venía implementando PCI, Leocast es una empresa que le da servicios a 15 o 16 entidades financieras, incluyendo bancos, como banco Ripley, BBVA, Scotiabank, diversos bancos y los procesos son los mismos, digamos que el esfuerzo si es mayor, porque implementar una empresa pequeña a un banco es un reto enorme.

O sea, estás en pleno reto.
- Si.

¿Ángel, que me dices de tu vida personal, estas casado, tienes hijos, soltero?
- Soltero, estoy ahorita dedicado netamente a los temas profesionales, ahorita tengo una proyección con mi novia, pero todavía no se da.

César, buenos días ¿Qué me dices César?
- Soy, jefe de gobierno de control, de seguridad de información en el banco Interbank, veo todo lo que tenga que ver con gobierno, riesgo y cumplimiento, sobre temas de seguridad del banco, en el banco tengo más de 8 años.

¿En lo mismo o hacías otras funciones?
- En seguridad, 8 años, por varias funciones, como jefe de gobierno y control 5 años, anterior estaba en otra jefatura, pero dentro de seguridad de información que es una subgerencia en Interbank.

¡Que se llama seguridad de información!
- Claro, pero seguridad tengo como 15 años, antes he trabajado en seguridad, pero en el tema de telecomunicaciones, en una empresa de telecomunicaciones que ya fue fusionada y ahora una sola y es mexicana.

Gracias César.
¿Qué nos puedes contar de tu vida personal?
- Soy casado, todavía no tengo hijos.

¿Carmen, cuéntame?
- Soy Carmen Goyzueta, estoy como oficial de seguridad de información, en el banco GNV, en el banco ya tengo 4 años, dentro de los cuales estoy como oficial, la labor es que todos mis compañeros han ido mencionando y respecto a mi vida familiar, soy casada, tengo una bebé de un año y un mes.

Todavía tus noches están críticas.
- ¡Uy sí, todavía! Pero feliz, me encantó.

Muy bien Carmen, muchas gracias.
¿Cuéntanos Víctor?
- Yo soy Víctor Isa, trabajo en un banco Cencosud, hace más de 2 años, son las mismas funciones que todos venimos realizando, con los proyectos y las regulaciones vigentes, en mi vida personal soy soltero y sin hijos.

¿Víctor, en Cencosud cuánto tiempo tienes?
- Más de 2 años, 2 y medio.

¿Y antes trabajabas en funciones similares o eran otras cosas?
- Sí, en funciones similares en Falabella.

Muy bien, gracias Víctor, John, buenos días ¿Qué nos comentas?

- Como está, buenos días, mi nombre es John Alvarado, soy el oficial de banco Azteca, dentro del paquete también veo el tema de Elektra e Itálica, que son parte del grupo corporativo, estoy alrededor de casi 3 años en el banco Azteca, anteriormente he estado como oficial también en Diners Club, y bueno, soy casado, tengo 3 hijos, el primero ya tiene 15 años y la segunda 7.

Muchas gracias John.
Yo soy Angelina, y me dedico a esto, a hacer investigación de mercados, soy sicóloga, entonces del área de ustedes se muy poco, así que lo que les pediría es que ustedes como expertos me instruyan a mí, tal cual yo fuera una criatura de escuela, así, de primer grado, así, porque eso son mis niveles a nivel de lo que ustedes hacen, entonces, eso es básicamente la función, que es lo que les quería pedirle, tengan en cuenta que a mí me van a tener que explicar las cosas básicas, desde lo elemental, porque pueda que hablemos en diferentes términos ¡Pueda no, voy a estar seguro! Entonces, por eso esa paciencia les pido y esa nitidez en su explicación para yo poder ir entendiendo algunas cosas que van quedando al aire.

ESFERA COGNITIVA, AFECTIVA Y CONDUCTUAL EN TEMAS DE SEGURIDAD Y MEDIO AMBIENTE

Dinámica (15 minutos)

Vamos a empezar con una pequeña dinámica, se las voy a explicar bien, vamos a dividirnos en 2 grupos, 3 para un lado y 3 para el otro, 3 van a estar trabajando sobre ese monigote, yo les voy a pasar unos papelógrafos y van a escribir en los papelógrafos, y los otros 3 sobre este monigote ¿Cuál es la diferencia de ambos monigotes? El tema básico del día de hoy es la Ciberseguridad, me imagino que algo de eso se imaginaban ustedes mismos por los perfiles que tenemos acá; entonces este monigote de acá es el experto en Ciberseguridad ¿Qué implica que sea experto? Implica básicamente el que es más consciente de todos los niveles de riesgo que existe, el que tiene mejores recursos, el que tiene más capacidad de maniobra en todos los aspectos, ese es ese monigote, que lo vamos a dividir entre ustedes 3 van a está trabajando sobre ese monigote, y ustedes 3 van a trabajar sobre este monigote ¿Qué características tiene este monigote? No es tan conocedor, ni tan experto como el de allá, por lo tanto, no sabemos qué es primero, el huevo o la gallina, pero tampoco tiene tan buenos recursos, o sea, las entidades donde laboran, no le brinda la totalidad de recursos que necesita, por lo tanto, tiene algunos desperfectos, tiene algunas ventanas abiertas y no es tan consciente de los niveles de riesgos a los cuales puede ser expuesto.
Ahora ¿Qué vamos a trabajar en base a estos monigotes? Vamos a trabajarlo a nivel de 3 aspectos que se los voy a ir diciendo y repitiendo, para que no se vayan a olvidar, primero ¿Qué tanto saben cada uno de sus monigotes? Luego, que siente el monigote, porque puede sentir mucho orgullo o mucha frustración, dependiendo de que tanto sabe y, por último, que es lo que hace, como lo hace, con que cuenta cada uno de sus monigotes.
Entonces hagamos espacio para pasar de los papelógrafos y los pulmones y si podemos dividirnos.
Tienen 15 minutos para llenar el papelógrafo.
Entonces, repito, primero, que sabe, acuérdense del rol de cada uno, este es el no tan experto y este es el totalmente experto, que sabe, que siente y luego es que hace, como lo hace y qué recursos tiene.

- Una consulta, ¿Y tenemos que ponernos en la posición del monigote? con las deficiencias que tiene cada uno.

Exacto, ustedes representan a su monigote. Éste es más eficiente y este se supone que es el que más conoce, y que hace, como lo hace y con que cuenta, porque acordémonos que ustedes están

enganchados a los recursos, a la tecnología, entonces lo que yo sé, tengo que suplantarlo con toda la tecnología que hay detrás.
(Participantes realizan ejercicio)

Vamos señores a seguir, entonces vamos a comenzar por este grupo, Ángel, Carmen y Carlos, cuéntenme un poco, expóngame un poco, que tal está este monigote, cuéntenme del monigote, ustedes 3, sobre todo para que ellos vayan después a ir refutando, porque se supone que ellos manejan al monigote conocedor, por lo tanto, ustedes van a estar ahorita en desventaja, pero comiencen a contar.
¿Carmen?

- A ver, nuestro monigote ¿Qué hace? Estamos considerando, primero que sabe, tiene criterios muy básicos de seguridad, conoce los estándares, pero a nivel conceptual, o sea, sumamente básico.

¿Cuál es el ABC que conoce?

- Puede conocer la norma, por decir, ¿Sabes qué? En la ISO 27001, en el anexo A, hay tales y tales controles, pero no sabe cómo implementarlos, entonces sabe la teoría hasta cierto nivel, no tan profundo, después conoce de tipos de ataques, pero a nivel de conocimiento, no ha hecho en algún momento algún ejercicio, de evitar hacking interno.

Te voy a poner ejemplos, este señor sufre un ataque, ¿Qué tipos de ataque me paso por ahí?

- Ingeniería social o Ransomware que fue el año pasado.

¿Y qué hace este monigote?

- En ese momento, intenta buscar en internet me imagino, como es que ha pasado, porque se le eliminó la información o porque se infectaron los archivos en la PC del usuario que le acaban de comunicar, es más, ya sabe que es Ransomware, puede inferir, porque como participa en comunidades de seguridad, sabe que hay estar alerta, pero no en profundidad, entonces en ese momento recién se va a empapar de saber qué tipo de ataque es, como fue, cuál fue el origen y como administrarlo y evitar la propagación.

¿Ángel, algo ibas a decirnos?

- Sí, básicamente complementando lo que dice Carmen, al no saber mucho, no podría detectar rápidamente las características de un ataque Ransomware o características de un phishing o los 5 pasos que son esenciales que se debe seguir ante un ataque.

Vamos a hacer un paréntesis, el mismo ataque sufre ese monigote ¿han escuchado del ataque?

- El Ransomware (varios)

¿Qué hace su monigote?

- El monigote ya está preparado y ya dio sus charlas de concientización, dado que este ataque generalmente ingresa por correo o envío electrónico para que otra persona no pueda recibir los correctos electrónicos con anticipación.

Eso ya sucedió, pero ¿Que hizo el monigote de ustedes para evitar que suceda esto? Yo retrocedo la pregunta ¿Qué hace su monigote para evitar que suceda eso?

- Para este tipo de ataque, lo que tiene que tener es, como indica John, concientización para evitar que las personas abran algún enlace o algún link que pueda infectar a la red de la empresa, otro punto es que este tipo de ataque se aprovecha de vulnerabilidades que tienen los sistemas que no han sido debidamente parchados, que debe ser, actualizados.

Por lo que yo entiendo, su monigote tiene todo parchado.

- Tiene un proceso de parchado.

¿Y qué tiene, qué recurso tiene para hacer ese parche?
- Varios recursos, porque los sistemas pueden variar, hay una herramienta que tiene Microsoft que usa para parchar las estaciones de trabajo, que se llama WSUS.
- ¡Eso es para el parchado en sí una vez que hay que subsanarlos! También hay parchados virtuales que ni bien se detecta algo, lo parcha.

Todo lo que me dices Víctor, es cuando ya detectaron.
- Si.

¿Pero en la parte preventiva?
- El fabricante dice, ha salido una nueva actualización y uno tiene que revisar, ver a qué máquinas le afecta, que sistemas y procesa a parchar periódicamente, y cuando viene el Ransomware para expandirse busca vulnerabilidades dentro de la red, que no han sido parchadas, pero si han sido detectadas, puede ser que no haya sido ni detectada, pero hasta ahorita no ha sido el caso de los que ha habido en el mercado, entonces si tú quieres un poco parcharlo, es encontrar la vulnerabilidad en esas máquinas, y una manera de evitar es que la persona haga clic a algo que viene de una fuente desconocida, para este tipo de ataques.

¿Y ahí?
- Concientización.

Lo que decía yo "No abran los correos, el día de hoy nadie".
- No, es un plan de capacitación, no es el día de hoy, sino todo el año.
- Hay un programa que se le hace a todos los colaboradores y en la cual dentro de ese programa está ese título.

¿Y ese programa, tiene una periodicidad específica?
- Al menos, anualmente.
- Depende de la organización también, más o menos vas conociendo tus usuarios y en función a eso con esas "Sabes qué, lo hacemos trimestral, lo hacemos semestral" ¡Y de cajón la anual!

Ahora si vamos, el segundo ¿Qué saben, más o menos?
- Porque por ejemplo hemos puesto que el monigote sabe, los temas relacionados por comunidad, por ahí el tema de LinkedIn, Cybersecurity.

¿Y el de ustedes también está en esas comunidades?
- Claro, es una asociación de auditores y la cual también pertenece seguridad de información y personal que maneja riesgos.

Entonces, ahí no hay mucha diferencia, los 2 están al mismo nivel. Porque lo que tú me estás hablando es información teórica de seminarios, cosas y comunidades.
- Incluso, el nuestro está especializado.

¿Como el de ustedes está especializado?
- Lo que pasa que, para el tema de Ciberseguridad, necesitas capacitación continua, y con el tema de monitoreo tú ya vas aprendiendo poco a poco y se van presentando nuevas amenazas en el mercado.
- La diferencia sería, que nuestro monigote sabe de las normas, del PCI, del COBI, pero por ahí asistió a la conferencia, pero hasta ahí.

- Y ha asistido, hay eventos en Estados Unidos donde directamente se ven temas de seguridad y todas las normas o le han pagado también para que pueda asistir a ver PCI.

Pero hasta ahí es conocimiento teórico.

- Es conocimiento.
- Pero de repente ahí puede estar asociado a una comunidad más especializada.

Justo eso iba a preguntar ¿Esas comunidades son como un asesor o simplemente todos están al mismo nivel? Una comunidad, con una empresa que me asesora.

- No.
- Todo es al mismo nivel.

Todos tienen el mismo problema, todos tienen la enfermedad.

- Pero es informativo, de agrupación, tú vas, participas y ahora, obviamente dentro de los que participan, hay gente que tiene conocimientos básicos, como gente que tiene conocimientos mucho más.

Claro, pero la nutrición es de ustedes, a lo que voy es que se nutren entre ustedes, no hay un profesor, ni un experto, ni nada.

- No. Depende mucho de cada profesional de seguridad de que comienza a profundizar cada uno de los temas en función a sus intereses y en función a los procesos que en su organización lleven.
- Por ejemplo, en el tema en particular, tienen unas charlas mensuales que son para todos, pero aparte hay cursos que ya son pagados, que son varios días de información; y el que tiene menos recursos, no va.

Voy a ponerles un escenario, ataque en día cero ¿Qué hace este?

- Acá lo sorprende totalmente, no sabe definir en ese momento, se va a poner a buscar en internet de qué se trata el tema, qué cosas puede hacer y en casos graves va a tener que decirle a la gente que se vaya a su casa, apaguen la computadora y eso lo que sucedió el año pasado; y en ese momento recién va a reaccionar, se va a dar cuenta de que habían cosas que no tenía previstas, no las había previsto y que en ese momento va a tratar de encontrar algún parche, alguna medida, nutriéndose especialmente por Internet, porque no tiene un consultor que esté cercano a él. Y lo que va a tener que hacer es apagar todo.

Supongo, que todo se desenchufa para que no entre más.

- En realidad, cuando identificas un equipo así, lo que te queda es desconectarlo, sacarlo de la red, para evitar la propagación.

¿Y ustedes que hacen, los expertos, que me dicen, Víctor, Carlos, que hacen ustedes? Ataque a cero ¿Qué hacen?

- Primero existen elementos para detectar ciertas anomalías dentro de la red, en la cual es software se identifica que está pasando en las redes, si es que hay alguna cuenta que está navegando y está ingresando a ciertos servidores que no debería ingresar y que no está autorizado su ingreso, que está intentando ingresar a otras máquinas.

¿Y cómo lo hace, que tiene, qué herramientas?

- Tiene herramientas, tiene un equipo preparado, tiene un equipo de respuesta de incidentes cuando suceden estas cosas, se juntan y son multidisciplinarios y entonces preparan el tipo de ataque, si necesitan notificar hacia arriba todo esto.

Primero, antes de la notificación hacia arriba, quiero saber que tienen en casa ¿Qué tienen? Tú me dices herramientas, háblame un poquito de las herramientas.

- Claro, hay rentas como el UTM Fortinet, que es una tecnología que ya incluye varios softwares ahí y en la cual te manda reportes y tú puedes hacer un análisis en ese instante para ver qué máquinas o hacia dónde está yendo este software malicioso.

¿Qué otras herramientas tienen? Acuérdense que éste sabe todo y tiene todo.

- Tiene IPS, que son sistemas que van en el perímetro de la empresa, que trata de contener tipos de ataque que puedan venir desde fuera de la compañía, por Internet, hackear la compañía.
- Sólo es en la red que tenga comportamientos anómalos.

Varios sensores ¿Algunos nombres específicos?

- Como el IPS, WA, 100.
- 100, que es la tecnología, un ejemplo es un (no se entiende) un fabricante.
- Claro, están poniendo nombre de soluciones, no están poniendo marcas, porque marcas hay "N".

Claro, esto es como la plataforma.

- La tecnología.
- Ahora, esto es para ayudar a protegerte, y también es replicarlo en un laboratorio para intentar ver qué vulnerabilidades tiene o de que se está aprovechando para propalar esto.
- Me hace acordar que el monigote no tiene un equipo para la respuesta de incidentes, ante un ataque y acero, que tiene que ponerse a buscar, tener alguien que lo ayude.

Son 2 cosas que yo veo, primero, tener todos estos equipos, digamos que no son equipos, son plataformas, pero que tenemos y segundo, además de eso un equipo de atenciones.

- Claro.
- Y no sólo eso, sino también procesos que integren dentro de la tecnología y las personas, porque ya tiene que haber una secuencia preestablecida.

Tiene un protocolo que hay que seguir cuando ocurre esta etapa. 2 necesito nuevas plataformas o los productos, luego este protocolo y luego un equipo de gente.
¿No es cierto?

- Si.

Y eso lo tiene aquí el señor monigote, el que está acá.
¿Cuál de todas las plataformas, estos productos que estamos hablando, cuál es el más eficiente ante un ataque del día cero o todos?

- Depende del ataque.
- Es que día cero, es muy general, día cero, es que viene el ataque, pero las herramientas dependiendo de por dónde viene, lo que indican, puede ser más eficiente para ese tipo de ataques, si viene desde afuera de la red, podemos hablar de un IPS, un WA u otro tipo de herramienta que te ayuda a contener algún ataque volumétrico, te estoy poniendo un ejemplo, pero en sí, el que más trabaja dentro de la red, es el que está tratando de propalar un ataque dentro de las máquinas.
- Si hablamos del más importante, yo creo que sería el SOC, que no es un aplicativo, es un grupo de aplicativos y es un servicio que te brindan.
- Y otro punto que es importante que el monigote, de este lado, no tiene un consultor, una buena consultoría que esté constantemente, que le diga "Oye, mira, acaba de ocurrir este ataque, en el Perú, en tal parte, entonces es posible que te esté llegando, en

Colombia o en tal sitio", entonces antes de que te llegue, ya tienes el aviso del consultor que te está diciendo.

- ¡Y estos servicios SOC, hacen eso!

Ya te entendí, lo detecta en el camino.

- Claro.
- En lo que ocurrió con el (no se entiende) el año pasado y el Ransomware que ocurrió primero en España, entonces todo el mundo sabía que estaba viviendo, porque 7 horas antes ya había ocurrido y se ha podido tomar las acciones y los que tenían las herramientas o recursos, ya podían tomar todas las precauciones.

O sea, ellos se salvaron de este ataque; y ustedes no.

- No.

¿Así, más o menos, así fue el escenario en este ataque?

- Claro.
- Y también para la respuesta, porque para la respuesta el consultor de dice: "Mira la vulnerabilidad es exactamente esto de aquí y tu balsa tal parte, tal cosa y vas a poder salvarte", en cambio el que no tiene, está buscando en internet, está viendo y buscar la información cierta, falsa.
- Es el que está más aislado, porque necesariamente el que parcha, no es el de seguridad, es otra área ¡Y hasta que vaya a convencerlo!
- Hasta que coordines con él, hasta que ellos prioricen, porque también tienen su prioridad.

¿Y porque no parcha seguridad?

- No es parte de sus funciones.
- Ahora, no es parte de las funciones el parchado, pero si el asegurarse de que se cumpla, por ejemplo, una de las labores bien importantes y bien interesante de seguridad es justamente coordinar con la gente de tecnología para que haga los despliegues, para que anticipadamente, en TI es el que parcha, TI es el que tiene la parte operativa y nosotros somos los que les damos los lineamientos.
- Eso es lo que te ayuda a tener un equipo de respuesta incidente, porque hay cabezas del TI que están ahí y ya saben su rol y cuando viene un día cero se reporta ahí y cada uno toma su función y hace lo que le toca hacer; acá yo entiendo que un ataque día cero, si no lo tienes documentado y está medio aislado, tienes que ir a convencer hacia arriba, a tu jefe, entonces eso también puede tomar tiempo.

¿Algo más acá, de lo que saben?

- No.

Yo quiero entender con que cuenta él, que cosas básicas tiene ¿Qué hace?

- Con buenas intenciones (risas)

¡No es suficiente!

- ¡Ah no!

¿Qué hace Carmen?

- Mira, tiene procedimientos, tiene control o ha diseñado controles que son manuales, que son muéstrales, que se basa en el uso de herramientas, tipo el EPO del antivirus, pero que no está integrado, no cuenta con elementos que si te generan alerta o que no tiene proceso te monitoreo periódicos que van levantando el cumplimiento o incumplimiento de los procesos de tecnología, entonces con eso no cuenta nuestro

monigote. Y tiene un proceso de concientización de usuarios insuficiente, hablábamos de tal vez el envío de PPT por correo electrónico, alguna publicación por la intranet de la organización.

- Una consulta ¿El de acá, tiene el respaldo de la organización?
- ¡Buen punto!

¿Puede suceder que este caballero no tenga respaldo de su empresa?

- Si.

¿Y eso sucede en la vida real?

- Sí.
- Claro, sí.

¿Y entonces, para que lo contratan al monigote?

- Porque la SBS dice que tiene que haber una persona.
- Porque estamos hablando de un banco.

Es sólo porque existe en la normativa que debe existir un monigote en la empresa.

- Si.
- Si.

O sea, que hay empresas que ni siquiera te dicen que "Cuentas con esto".

- No.

¿Y entonces, con que cuenta, con sus buenas intenciones?

- Si.
- E Internet y los contactos (risas)

¿Y existe mucho eso en la vida real?

- Si (varias)

¡Ah primera noticia! O sea, te ponen a trabajar con tu propio jefe para que vayan las cosas.

- Así es.
- Y llevar la propuesta a la alta dirección, y depende mucho de la cultura organizacional, porque vas a tener organizaciones que van a estar mucho más alineadas y que no te van a estar diciendo, que punto de la norma…

Lo que nos estaba contando Víctor, que este señor no tiene respaldo de su propia institución.

- Así es.
- O, al menos que tenga la suerte que lo visite la SBS y lo audite.

¡Y ahí da sus quejas!
Pero la SBS no te obliga a tener el IPS… ¿No es cierto?

- Posiblemente lo haga validar.
- Pero si me dice que debo tener los controles a ciertos procesos. Y eso también les obliga también a ellos; y como le digo, si tiene la suerte que la SBS lo visite y entonces puede haber hasta multa, porque la normativa sí o sí la cumplen.
- Igual, antes que presentes tu organización, le dices "Mira, ante la multa, estos controles mitigan el impacto en tu organización que puedes tener", entonces ahí de repente si se aprueban el presupuesto.

Supongo que están peleados por el presupuesto, porque esto supongo, que todos esos sistemas no son baratos.

- Claro.
- Claro.

Y eso es un presupuesto duro, porque no están pidiendo 5000 soles, me estoy imaginando, no tengo la menor idea, pero me imagino.

- Claro.
- Hay estrategias, una de ellas es la que mencionó John, que venga una entidad supervisora y que le diga a la empresa, necesito realmente esto más fuerte. Y otro es lo que menciona ángel, que se presente business case y le diga: "El tema de la multa, el tema de las pérdidas que van a ser en contra y necesitamos invertir tanto" y se hace un rol y ya. Y otra estrategia más, es dar valor a las cosas que uno tiene, si tengo un antivirus que es lo más básico, me fijo que el antivirus esté en todas las máquinas, le llamó la atención y le espero y le digo y veo los ataques que hay y saco un reporte ante la jefatura para un poco vender mi trabajo "He encontrado virus de la máquina de la secretaría de la gerente general" y eso se llama un escándalo y comienza a ganar valor, y el monigote le está dando también un poco de conocimiento y entonces no puede llegar a hacer esas cosas, pero si logra cosas de impacto, vender su trabajo con cosas de impacto, puede ir avanzando y entonces va a armar una visión diferente "Yo no quiero que haya virus en mi máquina, no creo que alguien esté monitoreando lo que yo estoy haciendo", entonces ¿Qué herramientas necesitas? ¡Tal cosa! "Entonces, vamos a comenzar poniéndole esto" y sobre eso tenemos que vender esa herramienta ya con los resultados que se tiene, pueden seguir avanzando; de hecho, hay empresas que han logrado eso, pero si necesita que el pago primero, el básico, esté cubierto, si el monigote logra adquirir mayores conocimientos, saber cómo implementar y explotar a fondo las herramientas, puede lograr beneficios en su trabajo y lograr que den más inversión.

¿Qué hace ese monigote? Víctor, César ¿Cuándo el ataque es interno? ¿Qué hace ese monigote, que es el que todo lo sabe?

- Si ya sucedió, va a tomar acción, va a aislar probablemente ese equipo, lo va a corregir, va a ver qué ha sucedido, podría haber sido un ataque día cero, entonces va a pasar a un análisis forense con las herramientas que tiene iba a decir "Esto ha sucedido por esto".

¿Y qué herramientas tendría que tener este monigote para evitar un ataque interno, con que lo ha solucionado o con que lo está solucionando?

- Puede tener todas las herramientas, pero un ataque de día cero, puede hacer que ninguna herramienta lo detecte, entonces tienes que tener muy fuerte el tema de concientización, temas de ingeniería social, que es lo que tiene también en Ciberseguridad.

Pero perdóname, César, me pareció entender, no sé si estoy en lo correcto, que el ataque día cero ¿Viene de afuera o también puede ser interno?

- No, interno yo entiendo porque alguien mando un correo de afuera o puso un USB indebido, que puede tener todos los sistemas, pero ninguno lo detecta; el riesgo es muy bajo, pero puede suceder.

Y puede suceder que un empleado como por ejemplo en el caso de ustedes, un empleado de bancos ¿Sea quien haga el ataque por algún tema personal de que quiere robar?

- Si.

¿En ese escenario, es lo mismo que un día cero o no?

- No.

Entonces, en ese escenario, de la gente que trabaja en el mismo banco, está tratando de hacer un ataque cibernético.

- Las herramientas, el 100, correlacionar eventos de lo que hace la gente, entonces hay otros sistemas también de parte de comportamiento, que puede detectar si alguna persona entró a algo indebido que no está autorizado.

Yo puedo ver de qué máquina salió ¿Algo así?

- Si.
- Si.
- O el DLP te ayuda para evitar que salga cierta información, pero en los casos que ha pasado, en los sistemas mismos, roban.

Vamos a dejar un ratito en los monigotes, porque nos estamos enterando de cosas internas. Quiero saber, como es el mercado en general, como lo leen, que tiene ¿Cómo ha sido atacado, como lo ven, está más acá o más acá? ¿Cómo sienten?

- Yo me siento en un mix.

¿El resto?

- Sí, también en un mix.
- Depende de cuál sea el estándar.

Pero imagínate el máximo estándar de lo que hay, todo lo que hay; en este momento, todo lo que tú sepas como persona, tú dices: "¿Mi institución está más allá o más acá?"

- Mi institución, está más acá, pero también tienes que tener en cuenta que hay organizaciones que tienen mayor predisposición. Hay atacantes que tienen mayor predisposición para unas y otras organizaciones, los hackers van a buscar más tener una presencia tipo BCP, organizaciones mucho más grandes que en unas organizaciones más pequeñas.
- Aunque ahí, varía, a veces los atacantes van al que tiene menos control, quieren menos esfuerzo. Si bien, todos tenemos datos de clientes, ahorita la joya es robar datos de clientes, datos de tarjeta y basta que un banco tenga dato de tarjeta, uno tiene los controles A y el otro tiene A menos, menos, el hacker va a ir a robarte esa base de datos.

EXPERIENCIA PROPIA. TODOS (15 minutos)

¿Qué experiencias hay? Quiero entender, tu decías que el año pasado tuvieron estos ataques ¿Qué ataques ha habido, los cuales diríamos que han sido los más complicados? ¿En general, que ataques ha habido?

- Los ataques han subido bastante en los últimos años, se han sofisticado bastante.

¿Cuánto porcentaje diríamos?

- Yo diría que los que ataca actualmente, son 100 o 200 por ciento son más, conocen más que los ataques que atacaban más antes, lo digo por experiencia de lo que se ha visto, de los ataques que hemos sufrido y que se ve que ha sufrido en el gremio, que los hackers están aprovechando vulnerabilidades que antes no detectaban, hay el del Ransomware por ejemplo y hay otros muchos más que no se conocen, y que están ahí y que han atacado temas muy puntuales, hay ataques de ingeniería social también.

¿Cómo es de ingeniería social?

- Ingeniería social es cuando alguien se hace pasar o engaña, ya sea al cliente o al usuario dentro del banco para que entregue información.

O sea, yo me llamo otra persona, algo así.

- Llama por ejemplo diciendo que soy un usuario del banco y llamo diciendo que soy el Gerente General o soy de soporte "Y necesito que hagas tal o cual operación o me entregues tal o cual información".
- Siempre trata de entrar en confianza contigo.

Pero eso no es a través del mundo extraño cibernético. No estoy invadiendo, sino por la fuerza tratando de meterme como una persona.

- Pero es fundamental dentro de lo que es Ciberseguridad, la persona que esté ahí, como algo técnico en el mismo ataque, porque de allí, se parte para muchos ataques.
- Es que, si hablamos el phishing, se basa en ingeniería de sociedad, el phishing es cuando te llega un correo y te dice "Dale clic acá o dame tus datos", se basa en convencerte, no le obligan a nadie, no rompen nada, pero tú eres el que cae.
- Te llega el correo de un banco en el cual te dice: "Actualice sus datos", a lo mejor también lo ha recibido.
- Pero las grandes pérdidas acá en Perú han sido internas, no estamos hablando de estos que han sido externos.

Diríamos que aquí, no somos un mercado atractivo para los hackers internacionales, ¿Eso es lo que me estás dando entender?

- Si.

¿O sea, que no nos mira como buenas presas para atacarnos, es más internamente por lo que te estoy entendiendo?

- No, de ambos lados, de todo tipo de ataques se ha recibido.

Pero Víctor, me dice que son más internos.
¿Sienten todos que es más interno o es más la percepción de él?

- Yo creo que es de ambos lados.
- Lo que pasa, que los ataques internos suelen ser más fuertes, o sea, los golpes son más fuertes, el que roba internamente, suele robar más que el que roba de afuera.
- Los robos más grandes han sido internos.
- Los más grandes y públicos, han sido internacionales.

¿Por ejemplo, cuáles me cuentan?

- Lo del BCP con un USB se llevaron 7 millones.

¿Y ese USB es de alguien de adentro?

- Si.

¿Pero con toda la intención o fue por error?

- No.
- Es toda la intención.

Y fue un trabajador de adentro.

- Claro, salió en las noticias y todo.
- ¡Llegó al poder judicial!
- Se llegó a publicar el video, entonces se ve que la cajera poner un USB y lo conecta a la máquina de su compañero.

¿Y puede ir a delito penal, está judicializado?

- Si, hay una norma de delitos informáticos.

- Como el caso de Cromwell, era una persona que hacía también...

El que robaba por poquitos.
- Por poquitos.
- Igual, fue por sistemas y entonces fue penado, pero ahí, no fue ningún virus, fue que él tenía los accesos.

Exacto, ahí no fue ataque cibernético, ahí fue asalto.
- Pero aprovechó una debilidad en el sistema que hace este tipo de cosas. Muy similar acá, aprovechó una debilidad del sistema, que pudo mover dinero.

¿Qué otros ataques han ocurrido, más chicos, más grandes?
- En el Ransomware, que comentan, infectar la máquina y encriptar todo el disco duro y te pide una recompensa.

¿Plata?
- Te pide plata, pero todo virtual, si quieres desencriptar la información de tu disco duro.

¿Y para eso también tengo sistemas que me pueden ayudar?
- Si.
- Preventivamente, claro.
- Ataques a los cajeros automáticos, son bastantes.

¿Pero al cajero automático como ataca, para que me dé la plata?
- Claro.
- Si.

O sea, es como que yo tenga un sistema de clave y ya con eso me da.
- Es algo más complicado, algunos tienen conexión con algún proveedor o algo así, que tienes que conectarte de alguna manera o poner algún sistema para que el cajero pueda darte, son vulnerabilidades.
- Y habría diferencia también entre los 2 monigotes, porque hay un monigote que tiene su ATM con todos los instrumentos de seguridad, monitoreo y todo y es muy difícil que caiga, salvo los ataques de identidad social en cuanto a la tarjeta, porque también hay cambios de identidad social del cambio de la tarjeta, y tiene la clave, y los cajeros que no tienen tanta seguridad si pueden ser susceptibles a que le instalen una minicomputadora por ejemplo, porque le instalen una camarita y un teclado falso, lo pone encima, el usuario va con su tarjeta, le copian la tarjeta, le copian la clave y ya tienen todos los datos de la tarjeta y la pueden clonar, la pueden replicar, o pueden lograr un dispositivo de red intermedio, con el cual se comunican entre el autorizador, el cajero y le dicen al cajero que piense más, lo que realmente tiene que pensar, o logran inyectar un virus, un malware, el año pasado estuvo Lotus, un virus conocido muy fuerte y logra hacer que bote dinero aunque no haya tarjeta o ante determinados eventos.

O sea, los cajeros son súper vulnerables, por lo que voy viendo.
- Paso eso y de ahí todo el mundo empezó a reaccionar y ahora está mucho más controlado, que nadie dice que puede haber otro pico, pero como que la gente está, la gente está más atenta.
- En ese tema, siempre está bajo los defraudadores.
- ¡A la gana, gana!
- En los temas de phishing, primero le afecta bastante a una entidad, pasa un tiempo y pasar los controles y va a otra entidad, sube y sube, toma controles, baja y se va a otra.

¿Se pasan la voz entre las entidades?

- Para eso está el comité.

Claro, porque igual uno, supongo que lo que tapar para que su imagen no se vea maltratada, pero a su vez es importante ayudar al vecino, porque igual le puede pasar, me imagino.

- Son diferentes, de los demás.
- No sólo bancos, las entidades de antivirus que envía notificaciones.

O sea, ¿Se supone que están inscritos en algo de eso o no?

- Si.
- Si.

Ahora, dígame una cosa, yo quiero saber todo lo que tiene el monigote ahí, quiero saber si eso existe en Lima o estamos hablando de utopías.

- Si existe.

¿Diríamos que en Lima están bien resguardados o sienten que estamos muy expuestos, como es en general, como ven el mercado limeño en relación con la Ciberseguridad?

- Lo que pasa que lo que estamos hablando, si ponemos ahí, hay mucha más tecnología, es una inversión bien fuerte. O sea, si tú llevas como una entidad y dices, en un año "Quiero estar de acá, a acá y necesito" y no vas a tener la capacidad de recursos para implementar todo en un corto tiempo, o sea, vas avanzando en priorizar tecnologías y recursos que lo van a implementar, porque muchas de las tecnologías, tengas que tocar sistemas y llegar al final y a nuevas tecnologías que salen, no es que la plata tampoco a la entidad más grande se la den.

O sea, por lo que entiendo, no estamos como mercado, del todo protegidos ¡Ninguno!

- Totalmente, no hay nadie que diga que tengo el top y de las últimas tecnologías, no creo.
- Pero hay un rango de calidad, de los que tienen bastante y hasta los que casi no tienen, hay de todo.
- Pero nadie tiene el ideal. No creo.

PLAN DE SUGERENCIS DE MEJORA (15 minutos)

Y una pregunta, vamos a imaginarnos que ustedes son los gerentes de Ciberseguridad de su empresa ¿Qué harían, que pedirían, qué necesidades detectan, que me dicen?

- Primero tercerizaría todo con un SOC, un servicio, porque para que nosotros simplemente hemos todo, nos va a salir más caro que pagarlo como servicio.

O sea, para tercerizarlo, me dices.

- Si.

¿John, tú qué harías como gerente de Ciberseguridad de tu empresa?

- Lo que pasa que como nosotros somos corporativo, vemos muchas tareas con disco, entonces a veces, como han dicho, nosotros tenemos conexión con México y a veces esos ataques vienen desde allá como que nos impacta muy fuerte acá.

¿Y qué le pedirías al gran jefe?

- Que desconéctame el equipo (risas)

¿Y cómo equipos, como herramientas, como recursos?

- Como equipos, estamos muy bien, como herramientas también, a veces sí hay demasiada responsabilidad sobre el tema de protección de datos personales, que es la ley que ha salido del ministerio de justicia y estamos en esa época y estamos viendo más funciones.

¿Pero nada que te instala?

- No, tengo las herramientas necesarias, en algunos casos por decir, ya me han pedido el tema, porque yo presento una herramienta óptima, fuerte, etcétera, etcétera, pero ellos me dicen, como es, que me va a dar una herramienta, si entre comillas no ha sucedido casi ningún tipo de transferencia

Pero si tú fueras el gerente ¿Qué haces, cual pones?

- El UTM, y el SOC.

Carmen, tú eres la nueva gerente de la empresa de Ciberseguridad ¿Qué pides, que instalas, que pones, que haces?

- Conociendo los procesos y viendo las ramitas que tenemos yo si pongo un SOC.

¿Ángel?

- Igual, creo que la tendencia es, tercerizar con un SOC, porque es más económico, a largo tiempo y largo plazo, nosotros tenemos los recursos especializados seguridad y también la rotación de personal bancario es difícil detenerla, o sea, el rotar de personal de planta, en los bancos es complicado a veces. Entonces nos conviene en ciertos casos tercerizar.

¿Carlos, qué haces?

- En mi caso, lo primero sería fortalecer el equipo de sistemas, de tecnología, en los temas de seguridad de información para que genere sistemas más seguros, que es una problemática propia y si también tenemos un software, pero me gustaría que fuera más maduro.

¿Algo específicamente que le falte al SOC que tienen?

- En primer lugar, el poder recopilar más información de sistemas para poder tener un mejor diagnóstico.

¿César, que me dices?

- Nosotros, también tenemos un SOC que estamos potenciando, pero entre lo más importante es fortalecer más nuestra herramienta de monitoreo, o sea que se pueda conectar todas las fuentes del banco a esta herramienta y ser mejor correlación, poder detectar más finamente y otro. Es las herramientas de protección de base de datos porque ahí está la información, tenemos protegida toda la base de datos, lo principal y que se pueda, que es lo más difícil, pero si estuviera en sus manos, es cifrar algunas bases de datos; y el último concepto que si estamos tratando de hacer es un sistema de toquenización, es decir, que tu base de datos más crítica tiene en 2 o 3 lugares especiales y de ahí aplicas este sistema de toquenización, porque sino las bases de datos se difunden mucho con tanto crítico; entonces, en otras base de datos que necesitas intermedias, van toquenizadas, van enmascaradas con un dato llave, que el único que sabe son matrices, entonces, que evita proteger 500 sistemas donde hay información ha de repente unas cuantas, porque las otras si se las llevan, mientras que no tengan una llave maestra, no van a poder; eso es bien difícil, sé que en el extranjero lo hacen.

PRESENTACIÓN DEL PRODUCTO (15 minutos)
Bien señores, yo quería hacer pasar a una persona, hace un momento Ángel decía: "A veces tenemos consultas y no tenemos expertos sobre esas cosas o no me asesoran bien", nosotros tenemos acá un experto que me gustaría que compartan un poco opiniones con él sobre el tema, espérenme un momentito, lo voy a hacer pasar.
Permiso, me presento y digo quién soy, soy Carlos Álvarez, soy consultor SOC, o consultor de ciberseguridad y llevo en el mundo de la ciberseguridad, en la industria de la ciberseguridad, dedicado exclusivamente a ciberseguridad, 17 años y en el mundo TI, 30.
(Se presenta consultor SOC)

¿No sé si tiene alguna consulta, algún interés, algunas novedades que puedan existir en el mercado, algo que puedan estar sintiendo que necesitan, si existe o no, si tiene ruta de solución? Posiblemente hablamos de los problemas que tenemos todos, que ya no es ni solución, ni queja, ni espera de un proceso o procedimiento, un instructivo, un modelo de gestión como una política o una norma de obligado cumplimiento, sino, simplemente el problema a lo que nos enfrentamos todos, con la ignorancia del usuario, la falta de cultura general y si me permitís incluso, el mal asesoramiento del estándar de proveedores terceros. No voy a generalizar, porque hay gente muy buena, pero hay mucho charlatán ¡O habemos! Ni voy a incluirme, ni voy a excluirme, pero creo honestamente que nosotros en este momento estamos dando soporte al ministerio de defensa de España, vemos la parte de SOC…
Individualmente ¿Cuantos de vosotros creéis que tiene el apoyo del gobierno corporativo, lo suficientemente razonable o alineado a la tendencia de riesgo que manejáis? Tu Carlos, porcentaje de apoyo versus riesgo que manejas.

- ¿Porcentaje de apoyo?

Sí, vamos a suponer que tu nivel de riesgo es 10 ¿Cuánto crees que te apoya el gobierno de Falabella?

- La mitad.

Y la otra mitad te la dejan a tu inventiva, a tu capacidad.
¿Tú César?

- Entre 7 y 8.

¡Está muy bien!

- Ha sido en los últimos años.

Sí, por la sensibilización obligada.
¿Trabajas en una entidad local o internacional?

- Local.

Es banco local. De capital local, no de capital internacional.

- No.

Bien, buen punto, gente local que tenga ese nivel de sensibilización, indica un nivel de madurez dentro del país ¿Víctor?

- 50 y 50.

¿Y 50, que significa, 50 de riesgo y 50 de apoyo?

- 50 de apoyo y a nivel local, a nivel de grupo, yo le pongo 30.

Bueno, pero el grupo te pide rendimiento y resultados y arréglate.
¿John?

- Será, 40, 60.

O sea, hay un 40 por ciento por tu lado.
¿Carmen?

- 50 y 50, 50 que nosotros tenemos con el corporativo.

¿Y tú?

- 50 y 50.

Normalmente el nivel de exigencia es superior al apoyo y el nivel de tendencia de riesgo que tienes que manejar es muy superior al de capacidad.
Mientras tú trabajas 8 horas por defenderte, los delincuentes trabajan 24 horas para atacarte, por lo tanto, la desventaja es abismal, internamente y como recurso, como responsables oficiales de seguridad.
¿Cuál es vuestro plan para escalar al WAP, para pedir ayuda, que medidas? ¿A través del área de seguridad para reclamar este desequilibrio, el nivel de riesgo y la capacidad que tengo?
César, tú que eres el que mejor situado estás.

- En nuestro caso, tenemos un comité formal de seguridad de información que tiene personas que reportan al gerente general de la compañía, entonces ahí hemos sensibilizado para que éste pueda atacar los riesgos de alguna manera, de tolerancia alta, que están los que no se pueden tolerar, o sea, los más altos, a eso, nos han dado un presupuesto o nos han apoyado con algún plan de acción de ataque.

Bien, te han dado dinero.

- Han dado, y recursos.

Y recursos, pero no te han dado soluciones.

- Es que la solución, se ha propuesto.

En teoría, tienes que salir de ti como experto.

- Si. O sea, proponer las soluciones, sabes como experto, pero también se dice que se puede presentar 2 soluciones que pueden tener algún riesgo y a veces, se ha tomado la decisión de seguir A o B.

De hecho ¿Quién confía que la seguridad protege al 100 por ciento?

- Eso se le tiene que quedar claro hacia arriba.

Existen medidas de protección, medidas de sectorización, o acciones de defensa, ¡Pero seguridad y garantía! Yo conozco una consultora de la (VITFOR) que, seguro que a todos nos han visitado alguna vez Deloitte, Deloitte es magnífica en sus presentaciones, siempre que habla de "Garantizamos" ¿Y cómo lo hacen, como pueden garantizar un día cero? Puedes tener ventaja, porque tienes una plataforma de investigación y de análisis de patrón y comportamiento, de casos de uso, de detección de secuencia de ataque, por lo tanto puedes ir adelantándote, como lo digo yo siempre, al que le duele la cabeza o al que sufre de migraña, tú le pones muchas horas de estar trabajando con la computadora y empieza a sentir como una vena y empieza a doler por aquí y cuando empieza a doler por aquí, sé dónde empieza y se dónde termina, toda la cabeza agolpada; en el tema de ataques cibernéticos, estamos exactamente igual, vosotros que lidias día a día con esto…
Y el Ransomware, el último, el Wannacry ¿Quién me sabe decir que particularidades tenía? Aparte de ser Ransomware ¡Era gusano, se preparaba internamente! Como técnica, era bastante novedosa…
Dicho esto, yo me voy a callar y espero que alguien me pregunte algo.
Tú ¿Creo que tenías una pregunta?

- Sí, yo tenía aprobado un pequeño presupuesto para implementar un SOC de Ciberseguridad, nosotros tenemos un SOC, pero estamos viendo el uso aparte, independiente, para que el mismo SOC que monitorea todos los elementos de seguridad.

¡Tienes un SOC! ¿Cuál es la diferencia?

- Lo que pasa que el SOC que yo tengo ahorita, no me da el servicio de Ciberseguridad, entonces estoy buscando eso, pero quería saber en base a tu experiencia ¿Qué necesitaría para poder implementar un SOC enfocado en sí ver seguridad si ahorita no tienen nada de eso?

Madurez en la capacidad de gestión para el servicio de Ciberseguridad, y me explicó, un SOC se compone de tecnología, recursos y procesos, esos son los 3 componentes básicos, se dice muy fácil, pero es que la parte tecnológica es tan amplio y voy a poner un ejemplo muy poco, hay un banco que se ha gastado 7 millones de dólares en implementar (Fyri) y todavía no lo ha puesto en marcha, y no deja de ser una tecnología de alerta de amenaza; si no tienes la inteligencia para gestionar correctamente, es como tener un Ferrari y no saber conducirlo, entonces ¿Desde mi punto de vista, que se necesita? Aparte del apoyo importante, formación, capacitación o en su defecto una empresa que venga a montarte un SOC un modelo no Outsourcing, ¡Insourcing! Te monta el SOC, te trae a gente experta, pero tienes tu gente propia, que vayan interactuando y asimilando el conocimiento. Curiosamente la mayor brecha de capacidad está en el talento del recurso, yo he visto gente que con un Open Source, ha sacado más rendimiento que con un (No se entiende) y se supone que al ser de IBM tiene que ser ¡La hostia…! Pero no, y eso es al final capacidad, destreza, habilidad, técnica táctica, conciencia. Un SOC de sí ver seguridad, establecer un plan de madurez para la capacidad de gestión, porque al final puedes crear un SOC, que te va a salir carísimo como porque no vas a ser capaz de soportarlo.

- ¿Y dentro de la solución que brindan, brindan un paquete completo? O sea, me va a dar su Ferrari con el piloto ¿O solamente el Ferrari?

Nosotros, somos una sastrería ¿Qué quieres? Si necesitas un traje de baño, yo te doy un traje de baño, si necesitas un traje, un traje, si necesitas un esmoquin, un esmoquin, damos soluciones a la medida, no somos la Coca-Cola, que vendemos en lata o en botella, ¡No! No creemos en las soluciones paquetizadas, te puedo dar soluciones paquetizadas de IRC, nivel bronce, nivel plata, nivel oro, en función del tamaño y del número de incidencias que tengas, también depende mucho de qué capacidad tienes tú de dar respuesta tú a los disidentes que tengas dentro. Por ejemplo, una actividad típica, el parcheo de vulnerabilidades, dame 5 clasificaciones, crítico, alta, media, baja, informativa. Bueno, estos 5 niveles y normalmente el nivel medio, bajo e informativo, es el que internamente la organización tiene la capacidad de parchar, las altas y las críticas, al ser completas, ya requieren, como digo yo, este es el cirujano que abre cerebros, 360 días al año y lo hace con los ojos cerrados, en cambio un cirujano que empieza a abrir un cerebro, tengo mucho miedo te meterle el bisturí; dame un problema de Ciberseguridad y me remango y disfruto. La diferencia está en la seguridad que te da el conocimiento, la madurez, la experiencia, nosotros podemos asesoraros, simplemente en el modelo de SOC, en cómo migrar las tecnologías y optimizar el SOC Know, porque meses que uno va a motorización y el otro que es que te dé la respuesta; por otro lado tienes que tener un programa, un plan de Ciberseguridad, tener un SOC con mucha tecnología, con muchas capacidades, con mucho proceso como con mucho procedimiento, con mucha chicha, pero si no tienes un plan estructurado de hacia dónde vas a ir desarrollando tu capacidad, no vas a aprovechar nunca nada; es decir, si el primer año quiero empezar con gestión interna de vulnerabilidades, perimetrada la auditoría y monitorización, alerta temprana, simplemente poder hacer autodescubrimiento de qué está pasando en tu ecosistema para poder generar tu conjunto de reglas de alerta, porque si no vas a tener que hacer el 24 por 7, a 4, 5 o 20 tíos mirando monitores ¡Y a los 40 minutos se pierde la atención! Cualquiera, el ser humano no es capaz de estar viendo

un monitor durante 8 horas al día, con la misma atención, con la misma intensidad de atención, entonces ¿Qué haces? Defines la inteligencia, un SOC de seguridad de inteligencia que lo que hace es definir casos de uso, patrones, reglas, alertas y un modelo de comunicación, ante este tipo de patrón, ante este tipo de alerta "Que pasaría si" y entonces empiezas a generar tu ecosistema de alerta y luego el plan de comunicación, tipificación, nivel de criticidad, una matriz de riesgo, una matriz de riesgo es activo, crítico, potencialidad de amenaza y potencialidad de ocurrencia y posible solución, saber cuáles son los activos que soporta otro negocio, cuáles son los riesgos que le pueden afectar, cuáles la probabilidad que ocurra y que tienes para salir adelante.
¿En Lima, qué probabilidad hay que llueva? Poca. Pues entonces el paraguas es una medida, pero no hace falta tener 6 paraguas, por si uno se me rompa, no. En cambio ¿Qué probabilidades hay de que te asalten?

- Muchas.

Hay probabilidades, es un riesgo, pues entonces ese tipo de cosas son, la matriz de riesgo es la que me da a mí el plan de securización, curiosamente en algunas ocasiones a mí me han dicho ¿Carlos qué pasaría si nos ataca un Wannacry? Depende ¿Qué le ha atacado, al correo tu secretaria? ¡Bótala! ¡Literalmente! Pero si te han incrementado la base de datos de tu facturación de tu cliente, es una preocupación; la diferencia está en crear una cultura interna al usuario de que tiene que ser copias de seguridad, de que tiene que tener la costumbre de no desvelar su contraseña estando de vacaciones, de no dejar la cripta debajo del teclado, "Oye mi contraseña es Pepito de los palotes" y ese tipo de cosas; o el de abrir correos que no tienen ningún sentido que llegue, porque hay Ransomware, malware, spyware… ¿Quién me podría decir la clasificación de elementos nocivos y maliciosos que se están repartiendo por la red? ¡Hay más de 60! Evidentemente no puedes conocer el nivel de vacuna de todos, ¡De hecho no hay vacuna para todos! Hay spyware que muchas organizaciones no son conscientes que lo tiene en su sistema y que están haciendo un sniffing de todos sus datos, a mí me ha llamado cliente en una organización que me dice: "Nosotros estamos securizados", "¿Y te parece normal que desde Rumanía se conecte tu director general que está sentado todos los días ahí, a las 3 de la mañana? ¿O te parece normal, a un banco que la tarjeta de crédito de Víctor haya comprado en Sídney, en Nueva York, en 4 minutos?" Es imposible que físicamente que este señor haya estado en 4 tiendas, en 4 países diferentes de 3 continentes, eso no tiene lógica; el sentido común, que no es el más común de los sentidos, es el que nos tiene que dar un poquito de aterrizaje sobre la realidad. Desesperarte ante un ataque informático o a un Cyber ataque, lo único que te hace es perder la noción de la capacidad de reacción, ejercitarte y ejercitar a tu equipo de respuesta eso es importante, crear Cyber ejercicios de ataque, de respuesta, multidisciplinarios, es decir, en gente de base de datos, de sistemas, de redes, porque un ataque multivector, normalmente todos los ataques lastimosamente entran por la mala calidad de las comunicaciones que nos dan los ISP, es decir en el primer Firewall nosotros tenemos que poner a Telefónica con Entel, a Claro ¡Es que es así! Tú puedes tener muy seguro todo, pero si ellos no filtran, se están exponiendo y tampoco tienes la capacidad de ser banco y ser ISP a la vez, entonces un SOC, cabe a tu criterio, madurez, procesos, conocimiento, pero sobre todo tener claro que activos tienes, porque en función de los activos que tienes definidas los servicios que debes implementar, la cultura que has de trasmitir y el modelo de gestión en la respuesta que tienes que desarrollar para proteger, recuperar y restaurar el correcto funcionamiento de tus activos y de los procesos que soportan tu negocio.
¿Tienen alguna otra consulta? ¿Alguna sugerencia?

- (No hay respuesta)

¡Contigo tenemos que hablar!

- Imagino que sí, ahora vas a pasar por el banco.

No, yo estoy invitado por ASBANC como experto para venir a comentaros cosas, pero creo que la gente de ASBANC está preparando una agenda importante para el futuro.

- A nivel de gremio, o sector financiero, estamos hablando de un gobierno que, de acuerdo con nuestra realidad, ¿Eso no lo tienen ustedes en algún país, como gremio de ASPABC, dando el servicio de SOC integrado con varios?

Si.

- Yo diría que daría más valor que cada empresa tenga su Cyber inteligencia por decirlo de alguna manera, te ayuda.

Y un (no se entiende) externo.

- Externo.

Si ¡No!
Necesitas el soporte de gente externa, experta, sí; necesitas gente que conozca tu ecosistema, tu infraestructura, sí; porque por muy experto que sea el externo, viene y te deja meter a un elefante en una cristalería.

- Claro, pero tú puedes tener el interno.

Si, claro.

- Pero si viene algo más gremial, como un ataque más gremial o gubernamental.

Nosotros tenemos un modelo de gestión de nuestros 5 SOC y con todos los clientes, en este momento tenemos 200 en el mundo y todos los días gestionamos alertas, IOC y los comunicamos con nuestros clientes, "Implementar estos Firewall, lleva esto, hemos descubierto un nuevo vector, un nuevo malware", nosotros en nuestra plataforma de alerta temprana, creo que estamos integrando unas 600 firmas al día y eso, lo que es un servicio más para nuestros clientes y siempre tiene el soporte de IRTM de 24 por 7, para decir "Necesito ayuda", pero nunca para dirigir, tu casa la gobiernas tú y así tiene que ser, o gente experta mía, pero que está dedicada a ti; otra cosa que digas, ha habido un ataque mundial y necesitamos la colaboración de todos, y para que tengas una idea yo tengo mi cuartel general aquí en Santiago de Chile, tenemos oficinas en Santiago, en Quito, Guayaquil y próximamente aquí en Lima, eso es nuestro proyecto de expansión, ¡Ah y para la (no se entiende) estamos con un SOC también! Como la región que es bajo mi circunscripción, ese es mi plan de desarrollo, y el próximo es Lima, queremos montar aquí un centro de operaciones de seguridad, un centro de consultoría, un centro de asesoramiento, un centro de capacitación, un centro de entrenamiento, queremos montar una plataforma de Cyber ejercicios, que eso es lo que nos está dando muchas satisfacciones, porque realmente ¿Cuántos de vosotros habéis contratado un servicio de estimulación de (no entiende) para medir vuestra capacidad de respuesta? ¡Quienes, ninguno! Básicamente, porque también te arriesgas a salir muy feo en la foto.

- Si.

Pero también tiene otra cosa, en un caso real, sabrías cual fue, lo único que le estás dando a la gerencia es, le estás dejando claro que estás preocupado y a lo mejor saber que no estás preparado a ese primer punto, para llegar al board y decirle "Necesito medios parece preparado", porque ¿Quién de nosotros en el banco no ha sufrido un ataque? ¡Hoy! Si sobre este señor llama ahora mismo a su equipo de monitorización, incluso están desbloqueados, bloqueados ¡Cuantos, muchos a diario! Entonces, la pregunta no es, me van a atacar o no me van a atacar, ¡Es cuando me va a tocar a mí!
¡Y el tiempo de respuesta!
El tiempo de respuesta es, cuanto tiempo soy capaz de emplear, el neutralizar el ataque y si estoy comprometido, en restaurar la normalidad, porque curiosamente un ejercicio de negación de servicio, te puede costar 60,000 dólares hacer 3 pruebas, porque una prueba no tienes sentido, porque una prueba es lo que te da la foto de hasta dónde eres vulnerable, la otra es si la medida que estas adoptando son razonables y la tercera es para practicar a defenderte, te puede costar

unos 60,000 dólares en un año, porque no se hace las 3 pruebas el mismo día, las haces una en el Q1, otra en el Q2 y otra en el Q 4 o el Q3, que también al oficial de seguridad le dé tiempo a entender que le ha pasado aquí como va a prepararse para mitigarlo, eso cuesta 60, 000 dólares ¿y un ataque de negación del servicio cuanto os ha costado? ¡Eso porque hoy en día todavía no hemos ratificado lo que cuesta perder la reputación! Hasta ahí, todavía no nos han imputado lo que cuesta el branding protection de la prensa, pero el día que nos metan ese coste en la espalda, es como digo yo "Quiero ser farmacéutico, me dedico a otra cosa", hay días en mi trabajo que soy feliz y hay días que salgo como un pollo al que le han echado agua hirviendo, ¡Desplumado! No siempre se gana, lo importante es saber levantarte y saber prepararse y ser consciente de dónde estamos parados.
Pero básicamente a través del agente del ASBANC, buscar la asesoría de la consultoría SOC, con ellos estamos trabajando muy de cerca en una alianza estratégica como socios estratégicos en temas de Ciberseguridad y ellos son los que te tienen que orientar, más bien, nosotros estaremos encantados de venir, hacer una de las conversaciones, de ver que tenéis y que pretendéis y luego ver si lo que pretendes está alineado, si te va a servir para lo que tienes que proteger, es decir, hay un montón de cosas, el montar un SOC, en mi vida, como consultor SOC, te diré que el año pasado fue para nosotros un año atípico porque montamos 9 SOC, y durante 17 años había montado 9, de los 9 que hemos montado el año pasado, 3 son nuestros, por lo tanto esos están funcionando, pero de los 9 anteriores, al 2015, desde el 2015 para atrás, monte 9 SOC y sólo funcionaban 2 y el resto lo cerraron, y el coste, por no saber qué hacer con ellos ¿Y alguno sabe lo que cuesta un SOC?

- Ni ideal.

Un SOC 1003, ahora tengo 1005 ¡Un 1003!
¡Venga, una cifra al aire! No nos van a castigar por esto, no es un examen.

- ¿Con local propio?

Si, un SOC 1003.

- De 10 a 15 millones.

De 10, a 15 millones, súbete al comité a decirle ¡Me equivoqué! Tienes que ir con la carta de división y decirle ¡Hola chicos, me equivoqué!
Bueno, ahora César voy a darles la nueva perspectiva de SOC, sí, de 15 a 20 millones cuesta un SOC interno, con todo, ahora imaginemos un SOC, con tecnologías CLAU ¿Cuánto costaría? 5 millones de dólares, la diferencia está en los costes de operación, soporte y mantenimiento que tiene que hacer del hierro y del compromiso que tienes que hacer con los fabricantes, entre 5 y 10 millones; un 50 por ciento.
Y un ISOC 1001, millón y medio de dólares, y como digo yo: "Quieres aprender a conducir, hay que gatear, caminar, trotar, correr y volar", si pretendes volar el primer año, te recogen en el suelo, lo más importante en esto es tener la madurez suficiente para saber dónde estás y tener un plan; el objetivo, no se ha de cambiar, se puede cambiar el camino, porque no siempre tomamos decisiones acertadas, pero si el objetivo es uno y tenemos claro cuál es, cambiemos el método, la técnica y la táctica, pero nunca el objetivo.
¡Me ha encantado lo conversadores que soy!

- (Risas)

Señores, nosotros estamos terminando, ¿No sé si tengan alguna, alguna sugerencia o algún comentario antes de irnos?
O si queréis que vayamos a veros, agendarlo con la gente, nosotros estaremos aquí hasta mañana, porque tenemos reuniones internas con la gente de ASBANC, pero por favor acercaros a la gente de ASBANC, que como organización están haciendo un trabajo muy fuerte y muy bueno, trayendo lo mejorcito que hay en el mercado y no lo digo porque sea yo, pero si están preocupándose por vosotros y yo creo que escuchar siempre antes de tomar una decisión, tienes

que escuchar 3, 4 5 y comprarle al que más cariño te parece, al que más le crees, que no significa que aciertes, pero al final hay gente que nos contrata a nosotros, no por lo dulce que somos, sino por lo eficaces que llegamos a ser.

- Y qué fecha tienen ustedes para implementar su SOC acá en Perú.

¿Cuándo lo necesitas? En 4 meses yo pongo un SOC ¿Cuándo lo necesitarías?

- No tengo la fecha exacta, pero tengo claro que este año o el próximo tengo que renovar el servicio.

Antes de octubre el SOC de Perú, está funcionando, el CSIRT ya lo estamos dando, ahora mismo tenemos una fuerza multidisciplinar, ¡Pero es el remoto! No puedo tener gente local si no tengo un centro donde entrenarles, porque sino es tener las gallinas sueltas, y el talento, y lo más complicado de todo esto es retener el talento ¡O no! ¡Cuantos se han salido! ¡Cuántos se os han ido! Tú eres el más joven ¡No sabes lo que te espera todavía, estás a tiempo!

- (Risas)

Muy bien señores.
Este mundo es divertidísimo.

- Varía mucho.

¿Ninguna duda, algo querías decir antes?
Si, dudas, muchísimas, seguro, lo que no tienen es la confianza de preguntarlas, ¡Pero dudas! Yo, entiendo que esto un primer acercamiento está muy bien y en el futuro desarrollaremos otras sesiones de trabajo.
Consulta con la gente de ASBANC y vamos a ver Luis Ángel ¡Vale!

- Si, claro.

Un SOC, nos encantaría echarles una mano con el SOC, o incluso nos encantaría que nos contratarais servicios gestionados ¡Porque vamos a negarlo!
El mercado local tampoco da para tener 6 SOC, no hay clientes para 6 SOC ¡No los hay!
Y vosotros, como entidad financiera estáis obligados a tener un ISOC, es tan sensible la información que manejáis, que no la podéis delegar a un tercero.
Bueno señores, no les quito más tiempo, muchísimas gracias, si tienen una sugerencia final, aprovechen que estamos acá, sino, les agradezco muchísimo, espérenme un momentito, voy a ver si están sus regalos.
En los próximos 60 minutos, se admiten quejas y no vamos a protestar.

- (Risas)
- Okey, gracias.

Anexo III – Guía de pautas – Entrevista Dra. Ángela Vaca

Encuadre: (5 minutos)

- Finalidad de la reunión: Conocer cuál fue el determinante de los bancos que les hicieron contratar el servicio.
- Micrófono / Grabadora (Confidencialidad)
- Breve presentación de cada uno

OBJETIVO:

El objetivo es indagar los siguientes aspectos:

CSIRT Conocer los motivos que le llevaron a adquirir el servicio, servicios que han sido más solicitados por las entidades financieras y temas regulatorios.

PARTE I: ROMPER EL HIELO (3 MINS)

Objetivo: Establecer las reglas de la entrevista y establecer el rapport

- Agradecer por su participación; presentarse y explicar el propósito de la investigación – entender sus experiencias y opiniones.
- Hay que explicar que se grabará (audio), y que habrá confidencialidad.
- ¿Cuál es su nombre?
- ¿Cargo, tiempo que vienen trabajando en la empresa?
- ¿Cuáles son sus principales funciones?
- ¿Qué es lo que más le gusta de su trabajo?
- ¿Y aquello que le resulta complicado?

PARTE II: LOS RIESGOS EN SUS ASOCIADOS

Si hablamos de los riesgos a los que se exponen al no contar el servicio CSIRT

- ¿A cuáles se exponen las entidades financieras? (pérdida financiera, pérdida de la información, pérdida del producto, etc.)
- De estos riesgos ¿Cuál(es) les genera mayor impacto? ¿Por qué?
- ¿Han podido cuantificar las consecuencias de estos riesgos?

PARTE III: APRECIACIONES SOBRE EMPRESAS - CSIRT

Quisiera que me comente sobre su proceso de selección a las empresas que brindan el servicio CSIRT:

- En general ¿Cómo describiría este tipo de servicio que debe ofrecer las empresas? ¿Por qué?
- ¿Cuáles son los retos/obstáculos que deben cumplir las empresas que ofrecen el servicio CSIRT?
- ¿Con que entidades tienen que convenios / certificación para brindar el servicio?
- ¿En qué consiste este convenio / certificación?
- ¿Cómo interviene el banco o que mirada tienen con respecto a estos convenios? ¿Consideran importante? ¿Por qué?

PARTE IV: APRECIACIÓN SOBRE MNEMO

Hablando específicamente de MNEMO:

- En general ¿Qué les parece este servicio de CSIRT que ofrece MNEMO? ¿Por qué?
- ¿Habían oído hablar de un sistema similar anteriormente? ¿Dónde?
- ¿Cómo están agrupado los servicios que ofrece MNEMO? ¿La agrupación de los servicios va con lo que quiere tus asociados? ¿hubo alguna reagrupación? ¿Por qué?
- ¿Qué beneficio les parece que les traería este servicio a sus asociados?
- ¿Qué aspectos de este servicio les resulta especialmente atractivos?, ¿algún otro?, ¿por qué?

PARTE V: ASOBANCARIA

Desde ASOBANCARIA

- ¿Percibe que existe una cultura preventiva por parte de todos los bancos?
- ¿Consideras que los bancos necesitan un servicio de ciberseguridad o CSIRT? ¿Por qué?
- ¿Los bancos cuentan con los recursos necesarios para adquirir el CSIRT? ¿Por qué?
- ¿Hay alguna agrupación por tamaño entre los bancos? (¿Bancos grandes, medianos y pequeños? ¿Consideras que la necesidad en temas de Ciberseguridad entre el tamaño de los bancos es muy diferente? ¿Por qué?
- De los servicios que ofrece MNEMO, ¿se ajustan a las necesidades de sus asociados? ¿por qué?
- ¿Cómo fue la iniciativa de implementar un CSIRT desde ASOBANCARIA?
- ¿Cuántos bancos se encuentran afiliados a este nuevo servicio?
- ¿Qué servicio de CSIRT lo ven más atractivo?
- ¿Cuentan con alguna ley relacionado con el tema de ciberseguridad? ¿Es favorable para sus asociados?
- Finalmente, ¿Si tuvieran que adquirir algunos de los servicios que ofrece MNEMO, seria a corto, mediano o largo plazo?

Anexo IV: Transcripción Entrevista Ángela Vaca

Emisanti: Aló, buenas tardes

Doctora Ángela: buenas tardes

Emisanti: que tal, le saluda Emisanti Quinta de la Asociación de Bancos de Perú

Doctora Ángela: hola Emisanti, como estas

Emisanti: aquí Dra. Ángela, molestándole, tenemos una consulta; estoy realizando un informe para hacer la evaluación de implementar un CSIRT para la Asociación de Bancos, entre ellos esta la empresa Mnemo como parte de los postores, sin embargo, tenemos otros postores mas, pero nos interesa saber en especial acerca de Mnemo por la experiencia que tiene con ustedes allá en Colombia

Doctora Ángela: así es

Emisanti: entonces todo lo que vamos a conversar son temas confidenciales, solo queda entre ustedes y nosotros

Doctora Ángela: así es

Emisanti: perfecto, Ángela un favor, voy a tomar nota de unas preguntas que me ha encargado del área de Estudios de Mercado

Doctora Ángela: si

Emisanti: ¿Cuánto tiempo viene trabajando usted en este proyecto?

Doctora Ángela: Nosotros venimos trabajando en este proyecto desde el año 2014

Emisanti: ok, dígame usted sobre este servicio que se ofrecería a los bancos, cuales los riesgos que corren al no contar con un servicio CSIRT ¿Qué tipo de riesgo se exponen las entidades financieras? ¿Pérdidas financieras? ¿perdidas de información? ¿perdidas de productos? Al no contar con un CSIRT.

Doctora Ángela: pues mira, lo primero … es que nosotros no lo tenemos como que si estuviera pensado bajo la forma de un servicio, nosotros en nuestro gremio bancario lo que hacemos son proyectos gremiales y estos proyectos, primero no se están comercializados como un servicio sino lo hacemos como un modelo auto sostenible entonces empleamos en todas las comunicaciones y todos los lenguajes que manejamos con las entidades, manejamos como un servicio porque eso te lleva a que ellos comparten servicios y te pongan como al mismo nivel que el proveedor y justo los proveedores no pueden prestar las funciones o no pueden ejercer la operativas que tiene el gremio. Primero no es como un servicio como tal sino es un proyecto gremial

Emisanti: ok

Doctora Ángela: y respecto a los riesgos, nosotros hemos notado que los riesgos de ciberseguridad se han incrementado, digamos que cada vez el delito informático y el tema de fraude informático es mas importante y esto es natural de acuerdo a la evolución que han tenido la banca en los temas de transformación digital y esta nueva línea de transformación digital

también a traído nuevos riesgos y nosotros hacemos un seguimiento de como evoluciona las transacciones y más de la mitad de las transacciones se ejecuta por vía de internet y medios electrónicos y cada vez cae mas en desuso el tema de las oficinas y esto genera nuevos riesgo para la operativa bancaria y nosotros lo que le hemos dicho que este CSIRT financiero que es un tema sectorial que no podría tener un proveedor un CSIRT financiero porque es muy difícil …. que le entregue una información a un tercero, es mas fácil que el banco te lo entregue a ti como entidad gremial que no tiene ningún interés de manera particular, sino que es de todos y como materia de información que ellos entregan bajo un marco de colaboración y de confianza que pueden tener mejores herramientas para tomar decisiones y pueden anticiparse de los temas cibernéticos o de riesgos cibernéticos.

Emisanti: perfecto, ya me queda claro. ¿y estos riesgos cibernéticos han sido cuantificados en pérdidas de millones hay algún aproximado de esto?

Doctora Ángela: pues mira es muy difícil aproximar las grandes preguntas que inclusive los grandes bancos se hacen es muy difícil que tu puedas tratar de cuantificar esos riesgos porque no es fácil aprender la superficie del ataque depende de los incidentes y generalmente las entidades no comparten los incidentes y es muy difícil calcular eso y lo que si sabemos es que los incidentes han venido creciendo y cada vez es mas la preocupación de la banca.

Emisanti: perfecto, ahora sobre la selección de Mnemo, hubo varios postores, me dijo ayer Alva me gustaría usted que me describa como fue esta selección ¿Cuál fue lo que se le pidió principalmente que se le pido a la empresa que cumpla como CSIRT, ¿Ustedes evaluaron si este tenía convenios internacionales? ¿Que cosa prepondero en la selección de Nemo?

Doctora Ángela: básicamente criterios técnicos para ser mas especifico, tendría que preguntarle a nuestra vicepresidenta no le puedo compartir mas detalles, pero Básicamente fueron criterios técnicos que tuviera experiencia en desarrollo de CERT, CSIRT sectoriales y en capacidades técnicas

Emisanti: perfecto, y si nos centramos sobre Mnemo, el servicio que va a prestar Mnemo a las entidades bancarias ¿este servicio como es percibido por los asociados?

Doctora Ángela: nosotros buscamos el operador, para ello ser transparente el CSIRT como tal no debe depender del operador sino debe tener un marco institucional propio eso quiere decir que primero se hace como tal el levantamiento corporativo institucional del CSIRT y luego se hace un tema del operador el CSIRT que quede claro que es lo que quiere el operador no es como el al revés sino primero parte de la circulación del gobierno corporativo orientado a objetivos y metas estratégicas, todo, y luego si se hace el tema del operador.

Emisanti: había oído hablar de un sistema similar anteriormente

Doctora Ángela: de un sistema como cual

Emisanti: de CSIRT o algo parecido al CSIRT, o ¿es la primera vez?

Doctora Ángela: nosotros mostramos este proyecto hace cuatro años, y estuvimos trabajando con otro CSIRT y hemos tenido diferentes experiencias internacionales

Emisanti: y este CSIRT que va a ofrecer Mnemo ¿ofrecerá una serie de servicios?, me imagino

Doctora Ángela: Nemo ofrece unos servicios complementarios al CSIRT bancario

Emisanti: es decir el CSIRT bancario ok, ok

Doctora Ángela: siempre … el gremio, a través de los comités y una gestión gremial, ellos son los operadores, pero CSIRT, pero es Asobancaria el dueño de la información.

Emisanti: entonces el CSIRT le pertenece a Asobancaria, pero lo opera Mnemo y hay servicios complementarios que va a ofrecerá Mnemo de manera especifica, de acuerdo con lo que vaya detectando el CSIRT.

Doctora Ángela: si

Emisanti: allá, ok, Perfecto ya entiendo así es como lo han diseñado, una pregunta doctora Ángela ¿Usted sabe cómo han agrupado este servicio los señores de Nemo?

Doctora Ángela: si, ellos han agrupado los servicios como cuatro grandes grupos:
Servicio de Inteligencia de amenazas externas, servicio de gestión de respuesta ante incidentes externos, observatorio de seguridad para el sector financiero y servicios complementarios y otros servicios a demanda.

Emisanti: ¿Qué beneficio les parece trae este servicio a sus asociados?

Doctora Ángela: este proyecto, tal como lo mencionamos como servicio es un proyecto que va a mejorar las capacidades de cada una de las entidades correspondientes …

Emisanti: ok, ¿Qué aspecto de este servicio les resulta especialmente atractivo?

Doctora Ángela: para esto se debe contar con la información de sus gremios es decir contar con la información de sus pares de forma anónima, tener como estas alertas en línea y tener un observatorio de seguridad sectorial

Emisanti: y desde Asobancaria ¿percibe usted que existe una cultura preventiva por parte de todos los bancos?

Doctora Ángela: se está desarrollando, cada vez la banca colombiana ha entendido más el tema de ciberseguridad y sin duda hay que ir avanzando el tema de prevención.

Emisanti: perfecto, ¿Los bancos colombianos en si están buscando en este momento tener un CSIRT?

Doctora Ángela: no solo la banca colombiana sino es una tendencia internacional, y ellos son consientes de la necesidad de compartir información y tener un mecanismo de protección sectorial.

Emisanti: ¿los bancos cuentan con los recursos necesarios para adquirir un CSIRT?

Doctora Ángela: digamos, cada banco podría montar su CSIRT, pero eso es muy costoso, entonces al hacerlo en conjunto les resulta más ventajoso y en nuestra percepción sí podrían acceder al CSIRT

Emisanti: y ustedes al brindar este servicio a todos los asociados lo han clasificado de acuerdo con su participación de mercados es decir bancos grandes, medianos pequeños

Doctora Ángela: no, lo que hemos hecho es como una cuota fija por cada uno de los miembros

Emisanti: ¿considera que la necesidad de tema de ciberseguridad entre el tamaño de los bancos es muy diferente?

Doctora Ángela: si, pero cada banco tiene las capacidades que requiere, los bancos grandes tienen más capacidades porque tienen mas superficiales backs, entonces es un poco tratar de ver que cada banco se ha armado estructuralmente de acuerdo con sus riesgos

Emisanti: ok, ¿De los servicios que ofrece Mnemo se ajusta a la necesidad de sus asociados?

Doctora Ángela: eso lo estamos trabajo en conjunto, no es solo un trabajo que haga el operador inclusive que lideran temas siempre es la asociación, eso nos permite garantizar que cumplamos las expectativas.

Emisanti: perfecto, me comento ayer Alba, que había ya quince bancos inscritos en este servicio para arrancar el primero de abril, eso es correcto.

Doctora Ángela: Si al momento ya contamos con 15 bancos inscritos de un total de 23 bancos en menos de un año.

Emisanti: Muy bien, sobre esto, existe alguna ley que este impulsando este tema de ciberseguridad o es un tema netamente por iniciativa de la asociación.

Doctora Ángela: el marco regulatorio colombiano es uno de los mas fuertes de esta materia y desde del CONPES es nuestra política nacional en temas de ciberseguridad …de la clase de los CSIRT si quieres revisar podrías leer el CONPES treinta y ocho, cincuenta y cuatro 2016 que se estableció la creación de CSIRT sectoriales.

Emisanti: CONPES treinta y ocho cincuenta y cuatro 2016, ok, perfecto, con eso es mas que suficiente. Me habían pedido hacer un reporte acá en ASBANC, Ok Dra. Ángela no le quito más el tiempo, y le agradezco por la entrevista realizada y la estaré molestándole por cualquier consulta adicional

Doctora Ángela: claro que si con mucho gusto

Emisanti: me gustaría sobre todo en el tema de lo que me dijo en las partes técnicas de los criterios de selección, no se si se podría compartir esa información

Doctora Ángela: tenemos que revisarlo al interior que lo revisen los abogados respecto a ese tema.

Anexo V – Guía de pautas – Entrevista Magno Condori

Encuadre: (5 minutos)

- Finalidad de la reunión: Conocer si existe una norma con respecto a "CSIRT"
- Micrófono / Grabadora (Confidencialidad)
- Breve presentación de cada uno

OBJETIVO:

El objetivo es indagar los siguientes aspectos:
Si en los próximos meses la Superintendencia de Banca y Seguros tiene alguna intención de poder sacar una normativa al respecto.

PARTE I: ROMPER EL HIELO (3 MINS)

Objetivo: Establecer las reglas de la entrevista y establecer el rapport

- Agradecer por su participación; presentarse y **explicar el propósito de la investigación** – entender sus experiencias y opiniones.
- ¿Cuál es su nombre?
- ¿Cargo, tiempo que vienen trabajando en la empresa?
- ¿Cuáles son sus principales funciones?
- ¿Qué es lo que más le gusta de su trabajo?
- ¿Y aquello que le resulta complicado?

PARTE II: LA NORMATIVA SOBRE CSIRT

Quisiera que me comente… en temas relacionada a CSIRT:

- En general ¿existe alguna norma o reglamentación respecto a este tema actualmente? ¿Cuál? ¿En qué consiste?
- ¿Se encuentra vigente?

Si mencionan que no existe ninguna norma:

- ¿Qué temas considera que deben ser cubiertos? ¿Por qué?
- ¿Cuáles serían las ventajas? y ¿Cuáles serían las desventajas?
- ¿Qué cambios deben realizar de aplicarse la norma? ¿Son viables?
- ¿Que percibe desde su punto de vista con respecto a los bancos? ¿Le favorece o estarían en contra de contar con un CSIRT?
- Sobre el convenio de Budapest ¿Que conocimiento tiene?
- ¿Alguna sugerencia adicional?

Anexo VI – Transcripción Entrevista Magno Condori

Magno Condori: buenos días

Emisanti: ¿Cómo esta?, le saluda Emisanti Quintana de ASBANC

Magno Condori: que tal Emisanti, mucho gusto

Emisanti: mucho gusto, haciendo mi trabajo de tesis para la Maestría de marketing de Esan y estoy proponiendo hacer un plan de negocio para crear una plataforma de ciberseguridad, basado en un CSIRT estaba hablando con Giovanni Pichiling, me dice que seria bueno saber el tema de cómo lo ve la superintendencia, y este es el motivo de mi llamada, quería hacerle algunas preguntas, básicamente sobre la normativa ¿si es que existe una normativa sobre ciberseguridad? o ¿esta planteándose hacer una?.

Magno Condori: sobre ciberseguridad

Emisanti: si

Magno Condori: ¿Conoces la normativa vigente?

Emisanti: No la conozco

Magno Condori: La normativa vigente esta recogida en la circular G ciento cuarenta, dos mil nueve, esta circular establece el marco normativo de seguridad de información que las empresas deben de cumplir, las empresas incluyen bancos, financieras, cajas, aseguradoras, AFP es el marco normativo vigente, ahora no es la única norma relativa que se puede vincular de ciberseguridad, porque existe otro reglamento, existe un reglamento que tiene un alcance mas amplio, permíteme revisar el numero que no lo tengo en la cabeza, la resolución 272 dos mil diecisiete, esta resolución de SBS establece el reglamento de gobierno corporativo y gestión integral de riesgos, entonces ese reglamento establece que el proceso de gestión de riesgos es responsabilidad del directorio, la gerencia y diversas unidades, ¿y que es lo que dice? Dice que estos entes que he mencionado deben hacerse cargo de identificar el riesgo al que se expone el negocio y su gestión, y luego ese reglamento menciona algunos riesgos digamos los más usuales riesgo de crédito, el riesgo de mercado el riesgo operacional etc., pero también menciona que esa lista no es limitativa es un tic, eso quiere decir que en verdad la regulación puede no necesitar que se especifique el riesgo de ciberseguridad, pero al ser un riesgo al que esta expuesto el negocio bancario por ejemplo las entidades sin necesidad de la existencia de esa regulación hoy en día deberían tomar medidas respecto al riesgo de ciberseguridad

Emisanti: La Superintendencia pretende sacar alguna regulación en especifica en temas de ciberseguridad en los próximos meses, sabiendo que es un riesgo latente.

Magno Condori: Haber, vamos a ponerlo en perspectiva la ultima parte de la pregunta, sabiendo que es un riesgo latente , uno tiene que tomar en cuenta que tiene que gestionar el riesgo es la entidad supervisada, al interior de cada banco, el banco es el responsable de gestionar los riesgos, por eso hacia referencia a esa normativa del reglamento de gobierno corporativo gestión de riesgo, lo que dice nuestra normativa vigente es que el directorio y la gerencia son responsables de gestionar el riesgo, entonces por eso decía, no es necesario una regulación adicional sobre ciberseguridad para que los bancos empiecen a tomar acciones en efecto lo están haciendo ¿entonces cual es la necesidad de una regulación especifica ….? es necesario porque hay que establecer requisitos mínimos, es decir dentro de esa gestión de riesgos, que se supone que debe saber Porque es su obligación, es la obligación de gestionar los riesgos de su negocio,

entonces la regulación lo que va hacer es requisitos mínimos, lo mínimo que hay que hacer, ojo es diferente que la empresa debe hacer comparado con lo que es mínimo que debe hacer. Entonces un banco no debería esperar a la que SBS saque una regulación.

Emisanti: entonces ¿Debería autorregularse el banco?

Magno Condori: Si, no toda la regulación no es prescriptiva, no es como la receta del médico, yo hago solamente lo que me dice el medico, no voy mas allá, no voy más acá, para fines de cumplimiento hay que cumplir la norma hay que cumplir la receta, pero no es lo único que las empresas deben hacer, aclarado eso la respuesta es si, la SBS va a sacar una normativa que va a exigir practicas mínimas en materia de ciberseguridad

Emisanti: también estuve revisando el plan operacional este año, decía crear una plataforma de ciberseguridad, estaba en el lineamiento estratégico de este año de la SBS

Magno Condori: Así es, en materia de ciberseguridad hay varias líneas de acción, están las líneas de acción de un sistema de monitoreo una plataforma para monitorear
Primero necesitamos saber si lo tiene que tener la SBS o lo tiene que tener el sistema financiero el sistema financiero tiene varias autoridades involucradas ahí esta el banco central.

Magno Condori: lo que preguntabas si había una ……., si lo hay, hay varias autoridades en el sistema el Banco Central, la Superintendencia de Mercado de Valores, la SBS y en el sistema financiero están los bancos, los agentes de bolsas esta la cámara de compensación electrónica en realidad el sector no esta solamente regulado por la SBS entonces lo que tiene que suceder que se coordine cual es el esquema más eficiente para un monitoreo, para el monitoreo del sistema para ver si esta siendo sujeto de un ataque y tomar las acciones del caso cuando corresponda, ahora la mayor parte de servicios que pueden ser afectados o están en los bancos y alguna parte esta en la administración pública ejemplo el LBTR que esta a cargo del Banco Central o algún servicio de intercambio de información que puede estar a cargo de la SBS, pero la mayor parte de actividad que puede ser interrumpida afectada esta en el sistema bancario y algunas entidades que son del sector privado, en ellos esta la mayor parte de actividades que podrían ser interrumpidas o suspendidas etc. Entonces este monitoreo puede tener la finalidad de mantenernos informados y a la vez rehabilitar la información compartida entre los que estén interconectados, se que hay iniciativa como las de ASBANC lo que buscan es dar un soporte no sólo a sus asociados sino a otras empresas

Emisanti: así es, cajas financieras

Magno Condori: por el lado de la SBS lo que vemos es todo el ámbito que nosotros regulamos y supervisamos en el que están el universo de las empresas de seguros y otras empresas y no necesariamente tienen una interacción con ASBANC, entonces existen plataformas como las de ASBANC que pueden contribuir a esto que estamos describiendo que se debe tener una plataforma para poder estar al tanto de Cyber ataques incluso para nuestra actividad interna, acá la gerencia y tecnología también tiene planes tener un mecanismo que le permita saber si estamos bajo ataque

Emisanti: perfecto, entonces esto haría que el tema de ciberseguridad se vuelva como un bloque, más o menos lo que estoy entendiendo de varios actores, superintendencia de mercado de valores, el banco central son varios los que están inter relacionados ahí para hacer frente a las Cyber amenazas actuar como bloque no solo como industria, como sector banca, sector valores con CAVALI sino algo mas global estoy entendiendo que la norma debería estar apuntándose por ahí, cual es lo mas eficiente

Magno Condori: aquí hay dos cosas distintas, una es la regulación, la regulación nosotros la sacaremos y será obligación de las empresas que supervisamos que cumplió, el banco central también saca regulación, el SMV también saca regulación y todos tienen alcances diferentes, la tarea para un poco de eficiencias que esos esfuerzos que en la medida de lo posible se coordinen, entones esa en una tarea que existe hacia delante, no hay una decisión tomada sobre la plataforma tiene que ser a nivel sectorial ese tipo de decisiones no se han tomado todavía, es una tarea de ver que es lo mas conveniente por el momento en la súper intendencia lo que tenemos es contar con apoyo internacional para clarificar cual es la necesidad de monitoreo que tiene la SBS para sus propios fines, y luego de eso veremos si es factible integrarnos con los que corresponde a otras autoridades

Emisanti: entonces, ustedes estarían tomando la iniciativa, para poder llevar mas sectorial, alguien tendría que tomar la batuta para avanzar en este tema que es un poco largo el proceso

Magno Condori: si es largo el proceso, pero lo primero que nosotros debemos entender que se necesita por nuestro lado para poder girar al lado y preguntar, si las necesidades son comunes si hay algo de todo el esfuerzo que hay que hacer es integrar, si es que lo hay

Emisanti: de mi lado a quedado todo claro, le agradezco la información recibida.
No se si tiene alguna sugerencia adicional que podría incluir en mi trabajo sobre este tema el punto de vista del supervisor.

Magno Condori: no se cual es la dirección que tenga la tesis

Emisanti : es crear una plataforma de ciberseguridad para la entidad financiera bancos cajas, entonces es compartir información, mas que todo saber si va a ver una regulación que apoye la creación de un sistema para que todos apoyen a compartir, porque ahorita no existe porque cada uno es receloso de su información y en su mundito van a ser eficientes y no es así, ayer que estuve hablando Asobancaria con la doctora Ángela Vaca me dijo que se esta compartiendo el Asobancaria, esta información. En Colombia ahí están mas dispuestos a compartir la entidad de Asobancaria es un poco mas neutra y esta buscando ayudar al sistema

Magno Condori: en ASBANC también hacen eso.

Emisanti: Si también, pero muchos bancos esperan como usted dice que exista la norma para hacer, sino no avanza

Magno Condori: así

Emisanti: es mi opinión

Magno Condori: claro, claro

Emisanti: estoy trabajando en ASBANC 10 años y están esperando estos temas de esa forma.

Magno Condori: dentro los requisitos mínimos probablemente sea el tema de intercambio de información, que se valla establecer y si hecho una de las cosas es que mas pronto sean notificados los participantes del sistema que hay un nuevo tipo de ataque o un tipo de ataque que existe mejor información y una respuesta mas oportuna, esta dentro de los requisitos, para nosotros no es necesario a que se espere una regulación, observamos entidades bancarias que están tomando acción no solo bancaria
Emisanti: si hay, pero son esfuerzos individuales, crear estas plataformas es colaborativas donde se enriquece mas la información, donde también son los sueños de Giovanni, crear estos sistemas de colaboración, buenos estamos en ese reto

Magno Condori: mira, en realidad las microfinancieras, las cajas municipales en realidad todos los privados son libres de integrarse y hacer su esfuerzo de colaboración, la policía de la perspectiva de la superintendencia en el marco de sus funciones necesita ese monitoreo ¿cuál es la finalidad? Es el proceso de entender la necesidad y clarificar la conveniencia eso es lo que debemos hacer en los próximos meses

Emisanti: muchas gracias, Magno, le agradezco muchísimo por su tiempo.

Magno Condori: un gusto.

Anexo VII: Principales Ataques de Ciberseguridad a nivel mundial

Estonia: Ciberataque de Denegación de Servicio Distribuido

Estonia es desde hace ya varios años, uno de los países con mayor acceso a Internet a altas velocidades, que es considerado un derecho humano básico en ese país. Alrededor del 90% de toda la actividad bancaria se realiza por Internet y fue el primer país en votar a través de la gran red. Esto creó el campo propicio para que en el 2007 se enfrentara a un gran ciberataque que amenazó principalmente al gobierno, al sistema financiero y a los medios de comunicación.

Durante dicho año y por decisiones políticas se aprobó un plan para trasladar un importante monumento soviético de la Segunda Guerra Mundial a una locación diferente, lo que provocó que varios ciudadanos rusos locales se sintieran disconformes.

El mismo día que el gobierno de Estonia trasladó el monumento soviético, el país comenzó inmediatamente a ser victima de un gran ciberataque, las páginas gubernamentales comenzaron a colapsar y el acceso a los sistemas financieros por Internet fue bloqueado. Las noticias sobre este incidente no se propagaban porque los sitios de los medios de comunicación estaban también fuera de servicio. Ese día Estonia fue victima de un ciberataque conocido como DDoS (Distributed Denial of Service), es decir que, desde algún lugar remoto, una red de computadoras estaba sobrecargando los servidores críticos de Estonia con una gran cantidad de solicitudes de servicio.

La herramienta utilizada para este ciberataque es conocida como botnet, definida como el conjunto de computadores que realizan tareas automáticas en base a instrucciones de una computadora central, conocido como centro de comando y control.

Estonia pasó así a enfrentarse con un ciberataque de gran magnitud en el mundo digital. El objetivo fue incomunicar a Estonia del resto del mundo y afectar a sus servicios. Fue la primera vez que se usó Internet como arma para colapsar el funcionamiento de un país en el ciberespacio. Este ciberataque pudo haber sido ocasionado por un grupo de hackers actuando de manera independiente o con el apoyo de un gobierno.

Estonia nunca tuvo claro quiénes fueron los responsables de los ciberataques. Este hecho fue considerado como un acto de ciberguerra porque perturbó la soberanía digital de un país. Aún después de lo ocurrido, no se han establecido claramente aún los protocolos para poder actuar, defenderse y contraatacar en una ciberguerra.

Ciberataque con malware Stuxnet

En el año 2010, el gobierno de Irán confirmó su intención de seguir adelante con el programa nuclear de enriquecimiento de uranio que había iniciado. Anteriormente, los Estados Unidos y algunos países de la OTAN (Organización del Tratado del Atlántico Norte) habían expresado su disconformidad, considerando que dicho país estaba desarrollando una carrera armamentista en el campo nuclear.

El programa nuclear instalaba centrifugadoras de enriquecimiento de uranio que se encontraban por debajo de la superficie. Debido a esto, la probabilidad de un impacto con un ataque aéreo tenia menor posibilidad de ser exitosa. Por ese motivo se planeó y logró propagar un virus informático letal mediante una memoria USB. Alguien a quien no se pudo identificar

conectó un dispositivo de este tipo en un computador de una planta de enriquecimiento de uranio y ayudó a propagar el virus, conocido como Stuxnet. El objetivo de este virus era afectar el programa nuclear de Irán.

Stuxnet se infiltró en las computadoras aprovechando vulnerabilidades de día zero, es decir vulnerabilidades que no son conocidas o reportadas hasta su descubrimiento y en consiguiente, no tienen actualizaciones de seguridad para su control y prevención. Stuxnet había sido desarrollado para buscar PLC's específicos relacionados a las centrifugadoras de enriquecimiento de uranio de marca SIEMENS y que casualmente, coincidían con los instalados en las plantas del programa nuclear de Irán.

El objetivo de Stuxnet era alterar la velocidad de giro de las centrifugadoras de enriquecimiento de uranio y así ir averiándolas de una en una. De ese modo se las dañaba de manera paulatina y no masivamente, para no levantar sospecha en los administradores de la infraestructura.

Después de algunos meses de detectar varias averías en las centrifugadoras y con ayuda de expertos nucleares e informáticos, los iraníes se dieron cuenta que estaban siendo victimas de un ciberataque. Pero ya era tarde ya que Stuxnet destruyó el programa nuclear de Irán, al infectar los sistemas de enriquecimiento de uranio y dejar físicamente destruidas las centrifugadoras.

Stuxnet fue de algún modo, un arma cibernética perfecta, inteligente y generadora de una gran destrucción. El virus saltaba de una computadora a otra e iba verificando su tipo y el entorno en que trabajaba. El virus fue resultado del uso armamentístico de la programación y se considera que fue originado por una nación con muchos recursos económicos, computacionales y profesionales, ya que su desarrollo está fuera del alcance de un hacker promedio o aún, de un grupo organizado.

Estados Unidos e Israel negaron tener relación con Stuxnet. Ningún país se hizo responsable del ataque cibernético y dado lo complejo del virus, es muy probable que nunca se sepa quién estuvo detrás del ataque.

Ucrania: Ciberataque con malware BlackEnergy

En diciembre del 2015 Ucrania sufrió un gran apagón de su sistema eléctrico. Un ciberataque coordinado afectó a las infraestructuras críticas, específicamente a las redes de suministro de energía eléctrica. Este ciberataque no fue un incidente aislado, sino que impactó en más de una empresa del sector de distribución de energía. Se calcula que afectó alrededor de 600.000 hogares, que no tuvieron electricidad durante algunas horas.

Ucrania y Rusia mantenían en ese momento un conflicto político y el gobierno de Ucrania acusó a Rusia de generar el ciberataque. Esta acusación fue apoyada por profesionales dedicados a la ciberseguridad de los Estados Unidos que analizaron el incidente. Se realizaron entrevistas al personal de tecnologías de la información de las 6 empresas eléctricas afectadas. De acuerdo con el historial de ciberataques, este sería el primer ciberataque contra una infraestructura crítica del sector eléctrico.

Los Ciberdelincuentes utilizaron una familia de malware llamado BlackEnergy. El malware se propagó por un ataque de ingeniería social y usó la técnica llamada spear phishing, es decir, correos personalizados con objetivos específicos que tenían adjuntos de Microsoft Office, con código maliciosos.

Como antecedente, este malware ya había sido detectado por el gobierno de los Estados Unidos, cuando intentó infiltrarse en el sistema eléctrico norteamericano, sin registrar un impacto. El objetivo era desconectar las estaciones y subestaciones eléctricas mediante el acceso remoto a las instalaciones.

BlackEnergy fue usado como técnica de acceso inicial para adquirir información de los usuarios, que permitiera realizar conexiones de manera remota. El malware fue detectado en otros sectores con infraestructuras críticas, pero no afectó la operación de los servicios.

Adicionalmente a BlackEnergy, también se utilizó el programa de borrado Killdisk, que borró archivos importantes del sistema para impedir que se pudieran recuperar los sistemas de suministro de energía. Dicho sistema de energía quedó inutilizado.

El ciberataque fue sincronizado y coordinado por un grupo de hackers, que antes de lanzarlo hicieron una exploración y reconocimiento de la red de las infraestructuras críticas de las empresas proveedoras de energía. Según el personal, los ciberataques a cada empresa ocurrieron con 30 minutos de diferencia e impactaron múltiples estaciones centrales y regionales.

De manera similar a los casos citados anteriormente de Estonia e Irán, nunca se supo quiénes fueron los responsables de este ataque y nadie se atribuyó su autoría. Sin embargo, existen muchas sospechas de que lo pudo haber causado el propio gobierno ruso. Estos ejemplos muestran las dificultades de la atribución, cuando se trata de ataques cibernéticos.

Otros ciberataques a nivel mundial

Algunos países también alertaron a sus centros de respuestas de incidentes, conocidos como CERTs o CSIRTs por sus siglas en inglés, sobre ciberataques que comprometieron sus infraestructuras críticas. De acuerdo con noticias periodísticas, en la mayoría de los casos tampoco se pudo detectar los orígenes. Esto demuestra que las distancias se han reducido y que, por diversos motivos, los grupos criminales organizados están realizando ciberataques. Adicionalmente y como ya se mencionó, las vulnerabilidades presentes en las infraestructuras críticas permiten una fácil ejecución de un ciberataque.

A continuación, se mencionan otros casos de ciberataques a nivel mundial:

- - Turquía en 2008: Ciberatacantes se infiltraron en sistemas industriales e hicieron explotar tuberías de petróleo.
- - Georgia en 2008: Ciberdelincuentes accedieron a redes de datos y cambiaron imágenes de diferentes sitios web del gobierno.
- - Israel en 2009: Se registraron ciberataques a sitios gubernamentales mediante el Internet.
- - Canadá en 2011: Se registraron ciberataques contra algunas agencias del gobierno que ocasionaron se desconectaran temporalmente de Internet.
- - Estados Unidos 2011: Se registró un ciberataque a un proveedor del Departamento de Defensa, que permitió el robo de 24.000 documentos de ese departamento.

  Adicionalmente a los mencionados precedentemente, se registraron ciberataques sobre instituciones privadas, especialmente de comercio en línea, que comprometieron información confidencial de los clientes.

  A nivel de Latinoamérica no existen reportes fidedignos sobre ciberataques a las infraestructuras críticas. Sin embargo, no por ello se puede confirmar que no hayan

existido. Pudieron registrarse casos aislados que no tuvieron repercusión nacional o que no fueron reportados por falta de conocimiento o para no causar temor en la ciudadanía. En este contexto, se genera una oportunidad entre las naciones u organizaciones de la región para crear instancias de colaboración, coordinación y cooperación sobre la ciberseguridad.

En cambio, diferentes países Latinoamericanos han sufrido ciberataques que han comprometido la privacidad y confidencialidad de la información. Estos ciberataques incluso afectaron a algunos países de Europa. A través de filtraciones de información realizados por expertos y trascendidos periodísticos, se pudo confirmar que Estados Unidos a través de sus agencias de servicio secreto estuvo espiando los correos y llamadas telefónicas de los presidentes o autoridades gubernamentales de Latinoamérica y Europa.

Políticamente los países afectados quedaron expuestos en temas de ciberseguridad. Por este motivo muchos de ellos decidieron desarrollar sus estrategias de ciberseguridad para proteger la información confidencial y las infraestructuras críticas. Un rol importante de estas estrategias es desarrollar protocolos para contraatacar un ciberataque y contar con la cooperación entre países y organizaciones que trabajan en ciberseguridad.

Anexo VIII: Tipologías de Ciberseguridad

Prácticas de Gestión de Seguridad

El dominio de las prácticas de gestión de seguridad es la base fundamental para el trabajo de los profesionales de seguridad y facilita la identificación de conceptos clave de cyber seguridad, controles y definiciones. Se podría interpretar la seguridad informática como "La protección otorgada a un sistema de información automatizado con el fin de alcanzar los objetivos aplicables de la preservación de la integridad, disponibilidad y confidencialidad de los recursos del sistema".

Un paso clave en la gestión de la seguridad es el análisis de riesgos; es decir, la identificación de amenazas y vulnerabilidades en contra de los controles y medidas de seguridad. Un correcto análisis de riesgos permitirá estimar objetivamente la pérdida potencial. También ayudará a determinar las medidas de seguridad más adecuadas y rentables para poner en práctica.

El dominio de las prácticas de gestión de seguridad incluye la clasificación de la información y de activos. El proceso de clasificación o categorización de información y activos proporciona una base para la definición de los controles y ayuda a diferenciar los tipos de medidas de seguridad y los controles necesarios para proteger a cada tipo de clasificación y proporciona una visión clara sobre los roles (propietario o usuario), divulgación o distribución, y la identificación de otros criterios como el valor, la vida útil, y una relación de elementos asociados.

Los dos últimos componentes de la gestión de la seguridad son la documentación y el conocimiento es por ello por lo que se suele mantener las políticas, procedimientos, directrices y normas que dirigen sus esfuerzos de documentación. A su vez, los empleados deberían de ser conscientes de las políticas y prácticas de seguridad, debiendo reconocer la importancia de los esfuerzos de seguridad y entender su función en mantener la información segura.

Control de Acceso

A fin de mantener la confidencialidad, integridad y disponibilidad de la información es importante que se defina una correcta estrategia de acceso a la información. Los controles de acceso impedirían que los usuarios no autorizados almacenen, utilicen o alteren información sensible o confidencial.

Debido a que ciertos controles de seguridad inhiben la productividad, la seguridad es normalmente un compromiso hacia el que los profesionales de seguridad, los usuarios de sistemas, las operaciones del sistema y personal administrativo trabajan para lograr un equilibrio satisfactorio entre la seguridad y la productividad.

Los controles de acceso se pueden clasificar en cuatro aspectos: prevención, detección, correctivo, de compensación. Los controles preventivos pretenden evitar que se produzcan eventos maliciosos, los controles de detección servirían para identificar que un evento malicioso ha vulnerado los sistemas de seguridad, mientras que los controles correctivos se utilizan tras el impacto de un evento malicioso para restaurar el sistema. Los controles de compensación se pueden considerar cuando no puede cumplir con un requisito explícitamente establecido, pero se ha mitigado suficientemente el riesgo asociado con el requisito a través de la implementación de otros controles.

Telecomunicaciones y Seguridad de la red

Las telecomunicaciones y seguridad de la red es uno de los dominios más técnicos ya que aborda las diversas estructuras de una red, los métodos de comunicación, formatos para el transporte de datos, y las medidas adoptadas para asegurar la red y la transmisión donde los factores elementales de este dominio son:

Confidencialidad
Protocolos de seguridad de red
Servicios de autenticación de red
Servicios de cifrado de datos

Integridad
Servicios de Firewalls
Gestión de la seguridad de las comunicaciones
Servicios de detección y prevención de intrusiones

Disponibilidad
Tolerancia a fallos para la disponibilidad de activos
Rendimiento del funcionamiento del proceso
Procesos de seguridad fiables y mecanismos de seguridad de red interoperables

Aplicación y Desarrollo de Sistemas de Seguridad

Más de la mitad de los cyber ataques actuales se centran en las vulnerabilidades de software de aplicación en lugar de en los sistemas de red. Se debe poner especial atención en estructurar los controles adecuados para las aplicaciones web que permiten el acceso externo a través de Internet debiendo adoptar buenas prácticas en el desarrollo donde el código de software deberá ser escrito siguiendo una pauta de codificación segura y donde todos los componentes de seguridad deberán dirigirse armónicamente durante el ciclo de desarrollo de las aplicaciones.

Criptografía

El dominio de la criptografía se ocupa de las medidas de seguridad que se utilizan para garantizar que la información transmitida es legible sólo por los usuarios apropiados. En términos sencillos, se conoce comúnmente como el cifrado de la información. El cifrado es la transformación de texto plano en un texto cifrado ilegible y es la tecnología básica utilizada para proteger la confidencialidad e integridad de dato.

Podemos clasificar la criptografía en dos modelos estándares: simétricos y asimétricos. La criptografía simétrica utiliza la misma clave privada o secreta para cifrar y descifrar un mensaje. Criptografía asimétrica utiliza dos claves diferentes: una clave privada y una clave pública.

Mientras que la encriptación es una especificación de implementación direccionable bajo el dominio de seguridad algunos elementos de cualquier organización requieren métodos de cifrado que hacen que la información está protegida, ilegible y cumplan con las directrices establecidas por diferentes normativas específicas de cada industria.

Arquitectura y Modelos de Seguridad

Los profesionales que se hagan responsables de este tema deberán comprender la totalidad del entorno de los Sistemas de Información propios y de sus potenciales clientes para poder desarrollar e implementar una arquitectura de seguridad apropiada y aplicar salvaguardias adecuadas.

Frecuentemente se utilizan modelos predefinidos de seguridad de la información para organizar y formalizar las políticas de seguridad de una organización, proporcionando un concepto específico y un marco referencial. Citamos tres tipos de modelos predefinidos de seguridad:

- Control de acceso: Este modelo, muy común en la mayoría de las organizaciones permite definir perfiles, identificar al usuario y entender el tipo de información a la que se les permite el acceso.

- Integridad: Este modelo no sólo protege la confidencialidad, también permite proteger la integridad de la información. Es un modelo que impide que la información sea modificada por usuarios no autorizados y evita que los usuarios autorizados realicen cambios no autorizados.

- El flujo de información: En este modelo, la información es clasificada y fluye de una manera específica en base a las políticas y reglas de seguridad.

Operaciones de Seguridad

El dominio de las operaciones de seguridad se refiere a la aplicación de controles y protecciones correctas en el hardware, software y otros recursos del sistema, al mantenimiento de una auditoria y seguimiento adecuados; y la evaluación de las amenazas y las vulnerabilidades del sistema.

Hay una serie de controles que se deben tener en cuenta para asegurar sus operaciones. Este dominio se ocupa de temas como la aplicación de:

- Controles preventivos para reducir la amenaza de errores involuntarios o impedir el acceso al sistema y la posibilidad de modificar la información por parte de usuarios no autorizados.

- Controles de detección ayudan a identificar el momento en que se ha producido un error.

- Separación de funciones mediante la asignación de tareas a los distintos recursos, por prevención, un recurso no debe tener el control total de las medidas de seguridad.

- Gestión de las copias de seguridad y las medidas para restaurar los sistemas con practicas alternativas.

- Definir las medidas para el seguimiento y aprobación de los cambios o la reconfiguración de cualquier sistema crítico.

- Realizar verificaciones de antecedentes de los empleados y no exponer posiciones que por función tenga acceso a información sensible o la aplicación de controles o medidas más recias de seguridad.

- Aplicar las políticas apropiadas de retención según lo dictado por la normativa vigente en cada organización en cuanto reglas legales y reglas de negocio.

- Mantener la documentación apropiada; la política organizativa, los procedimientos de seguridad, la seguridad, la contingencia y planes de recuperación de desastres.

- Definir, implementar, mantener y mejorar las medidas de protección para hardware, software y recursos de información.

Además de los controles, las operaciones de seguridad de sonido incluyen el monitoreo y la auditoría correspondiente. Hay tres tipos de técnicas que se utilizan para supervisar la seguridad: detección de intrusiones, pruebas de penetración, y el análisis violación. La auditoría es el examen de los registros de auditoría de forma regular, lo que puede ayudar a alertar a una organización de prácticas inadecuadas.

Seguridad Física

El dominio de seguridad física aborda el entorno que rodea al sistema de información y medidas de prevención adecuadas para proteger físicamente el sistema.

Las amenazas físicas y ambientales o vulnerabilidades pueden haber sido identificados mediante una evaluación de vulnerabilidad de peligros. Esto incluye situaciones específicas de emergencia, interrupciones de servicio, desastres naturales y el sabotaje.

El medio ambiente donde se ejecuta la operación de los sistemas también debe ser controlado (energía, ruido, voltaje, humedad, estática, detección y extinción de incendios, calefacción, ventilación y aire acondicionado, etcétera.

Más allá del medio ambiente, la seguridad física también incluye controles y mecanismos de acceso, como cerraduras de seguridad, guardas jurados, monitores de vigilancia, detectores de intrusión y alarmas. También incluye un control adecuado de los equipos informáticos mediante el mantenimiento de un sistema y proceso de inventario, la retención y el almacenamiento, y el proceso de destrucción.

Continuidad del Negocio y Recuperación de Desastres

Tanto los planes de continuidad del negocio, como el plan de recuperación de desastres deben estar en su ubicación perfectamente definida, lo que permitirá preservar el funcionamiento del negocio a consecuencia de un desastre natural o interrupción no controlada del servicio. Este dominio se refiere a dos tipologías de planificación: la planificación de continuidad del negocio y planificación de recuperación de desastres.

La planificación de la continuidad del negocio es el proceso de elaboración de los planes que garanticen que las funciones críticas del negocio tengan la capacidad de soportar una diversidad de situaciones de emergencia. En cambio, la planificación de recuperación de desastres consiste en desarrollar los preparativos para solventar un potencial desastre, y también se ocupa de los procedimientos que deberán seguir los recursos durante y después de una pérdida.

Hay cuatro fases principales en el proceso de planificación de la continuidad del negocio: alcance y el inicio del plan, la evaluación del impacto en el negocio, desarrollo de planes de continuidad de negocio, y la aprobación del plan y la ejecución.

La planificación de recuperación de desastres ayuda en la toma de decisiones críticas y orientar la acción en caso de un desastre.

Para seguridad de la información, el plan general se centra en los centros de datos o salas de ordenadores que alojan los servidores y equipos de red que conforman la infraestructura de tecnología de la información. El plan aborda cómo estos sistemas deberán ser recuperados sistemáticamente en el caso de un desastre para el centro de datos o sala de ordenadores.

Ley, Investigación y Ética

El dominio final establece las expectativas que los profesionales de seguridad deben entender, así́ como leyes internacionales sobre la seguridad de la información, tipologías de cyber delitos que se pueden cometer y las complicaciones específicas que la investigación de un cyber delito representa para el equipo de analistas de una organización.

La correcta interpretación y aplicación de este dominio también incluye procedimientos de notificación de las violaciones detectadas, así́ como la divulgación de las contramedidas aplicadas.

Anexo IX: Evaluación Externa

Fecha de elaboración	24 abril 2018
Elaborado por:	Jesús Calle
Fecha de revisión:	
Revisado por:	Grupo de Análisis ASBANC-CSIRT, **ASBANC**
Fecha de revisión:	2 mayo 2018
Revisado por:	Jesús Calle
Fecha de adición:	9 mayo 2018
Revisado por:	Jesús Calle

EVALUACIÓN FINAL

Habiendo revisado los diferentes aspectos que presentaron los oferentes para asociado de ASBANC-CSIRT, se incluye ahora un comparativo final entre ambas propuestas y se indica una recomendación a **ASBANC** sobre quien pudiese ser el correcto asociado. Esta tabla final presenta

Ítem	**AIUKEN-GMS**	**MNEMO**	**¿Cuál conviene más?**
Metodología	Cumple	Cumple	Ambas ofertas incluyen metodología válida para trabajar.
Servicios adicionales	Ofrece 40 de los cuales 10 tienen ya costo	Presenta 9 no presenta costo	AIUKEN-GMS tiene una oferta más completa
Certificaciones de Calidad	LEET ISO 27001	ISO 9001 ISO 27001 CMMI Nivel 3	AIUKEN-GMS presenta certificaciones enfocadas en servicios de seguridad.
Asociaciones	8 CSIRTs	FIRST	MNEMO está asociado a FIRST 421 diferentes CSIRT
Experiencia	6 instituciones financieras 2 telcos, 2 energía, 1 servicios públicos, 1 ITSP, 2 retail	4 instituciones financieras 2 gubernamentales	AIUKEN-GMS presenta más compañías
SOC en Lima	Ventas U$500.000	5-8 instituciones	AIUKEN-GMS es consistente
Plan de trabajo presentado	2 meses, 3 recursos por parte de ASBANC	No presentado. 2 meses, 3 recursos por parte de ASBANC	AIUKEN-GMS incluyó el plan de trabajo en la presentación.
Presentación	Cumple	Errores ortográficos y tipográficos	AIUKEN-GMS hace una presentación impecable
Costo Cliente final SOC/anual	U$42.000 – U$45.000	U$97.344.53	AIUKEN-GMS tiene una oferta más atractiva al cliente
Costo cliente final información/anual	U$6.000	U$78.561.29	AIUKEN-GMS tiene una oferta más atractiva al cliente

En la mayoría de los aspectos evaluados AIUKEN-GMS presenta una oferta más competitiva, consistente y completa para **ASBANC** y con mejores precios. Es por esto por lo que se recomienda la asociación con AIUKEN-GMS.

MNEMO no presenta consistencia en los servicios adicionales, no los explica, tiene precios más altos para los clientes. Bajo estas condiciones no sería conveniente una asociación con ellos.

Anexo X: Contrato Marco Comercial

CONTRATO MARCO COMERCIAL DE SERVICIOS DE CIBERSEGURIDAD

Conste por el presente documento, el **CONTRATO DE SERVICIOS DE CIBERSEGURIDAD** que celebran de una parte **ASOCIACIÓN DE BANCOS DEL PERU**, con RUC No. 20139491077, con domicilio en Calle 41 No. 975, Urb. Córpac, distrito de San Isidro, provincia y departamento de Lima, debidamente representada por su Gerente General, señor Miguel Vargas Ascenzo, identificado con DNI No. 09445023, conjuntamente con su Gerente de Control Institucional, señora Patricia María de Lourdes Barreda Meyer, identificada con DNI N° 08186323, según poderes y facultades que corren inscritos en la Partida No. 03024350 del Libro de Asociaciones del Registro de Personas Jurídicas de la Oficina Registral de Lima y a quien en adelante se le denominará "**LA ASOCIACIÓN**"; y de la otra parte, **AIUKEN SOLUTIONS SpA**, con RUT No. 76410862-0, con domicilio legal en Calle Matías Cousiño 150 of. 322, Santiago de Chile - Chile, debidamente representada por su Director General el señor Sergio Fernando Novoa Galán, identificado con RUT chileno N° 3639467-6, con poderes inscritos en la Partida Electrónica N° _____ del Registro de Personas Jurídicas de la Oficina Registral de _____, a quien en adelante se le denominará la "**AIUKEN**", con la intervención de **GRUPO MICROSISTEMAS PERÚ S.A.**, identificado con RUC N° 20563034484, con domicilio en Av. Paseo de la República N° 3195, of. 602, distrito de San Isidro, provincia y departamento de Lima, debidamente representada por su Gerente General el señor Esteban Lubensky Jaramillo, identificado con Pasaporte ecuatoriano N° 1708071178, según poderes que obran inscritos en la partida electrónica N° _____ del Registro de Personas Jurídicas de Lima, a quien en adelante se denominará "**GMS**" en los términos y condiciones siguientes:

PRIMERA.- ANTECEDENTES

LA ASOCIACIÓN, es una persona jurídica sin fines de lucro cuya finalidad es la representación gremial de los legítimos intereses comunes de las entidades privadas del sistema financiero que la integran.

GRUPO MICROSISTEMAS PERÚ S.A., es una empresa multinacional que ofrece soluciones de seguridad de la información que tiene su matriz en Quito, Ecuador, y una posición de liderazgo en el mercado andino.

AIUKEN SOLUTIONS SPA, es una empresa multinacional especializada en servicios de Security Operations Center (SOC, o centro de operaciones de seguridad, en adelante SERVICIOS SOC), cuya matriz está en Madrid, España.

GMS tiene una relación contractual con la empresa AIUKEN Solutions, por medio de dicha relación contractual, GMS ofrece SERVICIOS SOC conjuntamente con AIUKEN a clientes en la región.

En abril del 2018, LA ASOCIACIÓN organizó un concurso para seleccionar un proveedor de SERVICIOS SOC que sea su aliado para ofrecer dichos servicios a sus entidades vinculadas mediante la suscripción del contrato específico correspondiente (en adelante los CLIENTES o CLIENTE, cuando la referencia sea en singular). Tras recibir la oferta de AIUKEN-GMS con fecha 17 de abril del 2018, más aclaraciones a la misma en las semanas subsecuentes, LA ASOCIACIÓN declaró como ganador del concurso a AIUKEN-GMS, notificando su decisión por medio de una carta con fecha 10 de mayo del 2018.

SEGUNDA.- OBJETO DEL CONTRATO

El objeto del presente contrato es formalizar la relación comercial entre LA ASOCIACIÓN, GMS y AIUKEN, por medio de la cual LA ASOCIACIÓN podrá ofrecer a sus CLIENTES, a través de la suscripción de Contratos Específicos, los servicios de Security Operations Center entregados conjuntamente por AIUKEN y GMS, tal como se señala en los acuerdos de nivel de servicio contenidos en el **Anexo C** (Servicios SOC).

GMS y AIUKEN son los responsables técnicos de la prestación de los SERVICIOS SOC. LA ASOCIACIÓN cumple el rol de facilitador administrativo de los SERVICIOS SOC, en su condición de persona jurídica sin fines de lucro de carácter gremial, integrada por entidades privadas del sistema financiero que operan en el territorio de la República del Perú.

*Todo reporte o flujo de información que LA ASOCIACIÓN requiera hacer a AIUKEN y GMS, se entenderá como realizada si ésta es emitida a GMS. Es decir, la constancia de entrega o de envío de las comunicaciones / información realizada a GMS tendrá efectos inmediatos también para AIUKEN, sin admitirse prueba en contrario.

TERCERA.- ANEXOS

Los siguientes Anexos forman parte integral del presente contrato:

- Anexo A: Oferta y aclaraciones entregadas durante el concurso de LA ASOCIACIÓN.
- Anexo B: Equipo de trabajo.
- Anexo C: Plan de trabajo.
- Anexo D: Acuerdo de nivel de servicios de servicios básicos.
- Anexo E: Catálogo de servicios (básicos / específicos).
- Anexo F: Documentos habilitantes.

CUARTA.- FORMA DE PAGO Y PROCESO DE FACTURACIÓN

LA ASOCIACIÓN pagará toda factura de GMS, más los impuestos de ley, en un plazo de diez (10) días hábiles contados a partir de la fecha de su recepción. En caso de aplicar retenciones de ley, las mismas se deberán realizar en las condiciones más favorables para GMS que permita la reglamentación fiscal y los comprobantes respectivos deberán ser entregados a GMS en el plazo más corto que permita la misma reglamentación. AIUKEN y GMS se reservan el derecho de suspender cualquier servicio cuyos pagos no estén al día, aún si dicho retraso se deba a una inconformidad reportada por LA ASOCIACIÓN en la cual las partes mantengan un desacuerdo.

4.1. Facturación por SERVICIOS SOC

GMS facturará a LA ASOCIACIÓN por todos los SERVICIOS SOC vigentes colocados en sus CLIENTES según los CONTRATOS ESPECÍFICOS una vez que LA ASOCIACIÓN haya entregado y AIUKEN y GMS hayan aceptado los documentos habilitantes según lo establecido en el Anexo G. La facturación de los SERVICIOS SOC se realizará en los periodos que correspondan a los aceptados por el CLIENTE en su respectivo CONTRATO ESPECÍFICO, sin perjuicio de lo establecido en los documentos habilitantes según el Anexo G. GMS, a su exclusivo criterio, podrá facturar valores proporcionales a periodos más cortos para unificar ciclos de facturación, siempre y cuando esto no genere cambio alguno en los valores totales a ser pagados por LA ASOCIACIÓN.

4.2. Facturación por productos

En caso de que un SERVICIO SOC colocado por LA ASOCIACIÓN requiera de un producto adicional a los considerados dentro del alcance del respectivo SERVICIO SOC, sea que este producto consista en equipos o licencias de un FABRICANTE, LA ASOCIACIÓN deberá generar los documentos habilitantes respectivos según lo establecido en el Anexo G. Con la recepción y aceptación de tales documentos habilitantes por parte de AIUKEN y GMS, GMS procederá a facturar por los productos contra su entrega.

4.3. Facturación por servicios puntuales

Durante el giro regular de negocio para promover el objeto del presente contrato, las partes podrán encontrar instancias en las cuales se requiere de consultoría o soporte especializado, sea de forma planificada o bajo una situación de emergencia, que deberá ser entregado a CLIENTES o directamente a LA ASOCIACIÓN. Para tales instancias se deberán generar los documentos habilitantes según lo establecido en el Anexo G, los cuales establecerán para cada caso específico el proceso de facturación respectivo.

4.4. Facturación directa a CLIENTES

Las partes podrán, por mutuo y previo acuerdo, determinar casos en los cuales sea de mayor beneficio para ellas la emisión directa de facturas por parte de GMS al CLIENTE. De ser necesario en estos casos específicos, GMS asumiría las responsabilidades normalmente asignadas a LA ASOCIACIÓN según la cláusula 5.1.5. En cualquier caso, que las partes determinen que GMS facture directamente al CLIENTE, se respetarán las condiciones comerciales establecidas para el servicio o producto del caso, de tal forma que LA ASOCIACIÓN facturaría a su vez a GMS por el margen que le corresponda en cada transacción aplicable. LA ASOCIACIÓN emitiría estas facturas dentro de los diez (10) días hábiles posteriores al cobro por parte de GMS al CLIENTE, y GMS pagaría a LA ASOCIACIÓN dichas facturas en un plazo de diez (10) días hábiles posteriores a su recepción. En estos casos, se deberán mantener los documentos habilitantes establecidos en el Anexo G con las modificaciones respectivas para reflejar correctamente el origen y destino de los documentos relevantes.

QUINTA.- OBLIGACIONES DE LAS PARTES

Serán obligaciones específicas de las partes, además de las generales establecidas por el presente contrato, las siguientes:

5.1. Por parte de LA ASOCIACIÓN:

5.1.1. Designar a los funcionarios idóneos de su organización a los roles que le correspondan dentro del equipo de trabajo establecido en el Anexo B.

5.1.2. Asegurar la puntual y efectiva ejecución de las responsabilidades que le correspondan en concordancia con el plan de trabajo detallado en el Anexo C.

5.1.3. Realizar y sostener su mejor esfuerzo comercial para la colocación de los SERVICIOS SOC entre sus CLIENTES y reportar a GMS sobre cada oportunidad detectada con una frecuencia al menos quincenal.

5.1.4. Realizar y sostener su mejor esfuerzo de atención para mantener el máximo nivel de satisfacción entre sus CLIENTES, en concordancia con la estructura de funciones establecida en el equipo y plan de trabajo.

5.1.5. Suscribir los respectivos Contratos Específicos con cada CLIENTE. Esta obligación es de responsabilidad exclusiva de LA ASOCIACIÓN, por lo que AIUKEN y GMS no son parte de estos contratos.

5.1.6. No revelar, ceder o transferir a terceros ninguna información referente a los negocios, clientes, instalaciones, cuentas, ofertas, precios, finanzas de AIUKEN ni GMS, ni sus procedimientos, métodos, transacciones, “know-how”, o cualquier otro

aspecto relacionado con la actividad de dicha entidad que pueda conocer o haya conocido con motivo de la prestación de servicios prevista en el presente contrato.

5.1.7. Actuar con la mayor diligencia para evitar la publicación o revelación de cualquier información confidencial referente a esas materias.

5.1.8. Asegurar el pago puntual a GMS por todos los servicios activados bajo el amparo del presente contrato, según las condiciones comerciales establecidas en el mismo.

5.1.9. Se compromete a no suscribir contratos ni Alianzas Estratégicas Comerciales similares a los SERVICIOS SOC con terceros mientras esté vigente el presente documento. Tampoco podrá promover ni ofrecer servicios similares a los SERVICIOS SOC mientras esté vigente el presente documento.

5.1.10. ASBANC incorporará en los contratos específicos que suscriba con las EMPRESAS USUARIAS, cláusulas que establezcan las siguientes obligaciones para las EMPRESAS USUARIAS:

5.1.10.1. Brindar toda la información y facilidades necesarias a GMS - AIUKEN para que pueda cumplir con la prestación de EL SERVICIO.

5.1.10.2. Utilizar EL SERVICIO solo para su uso exclusivo y cubrir sus propias necesidades y de ser el caso, de su empresa, bienes o servicios, quedando estrictamente prohibida la transferencia/ cesión/ comercialización del presente Contrato, total o parcialmente a terceros, bajo cualquier título.

5.1.10.3. Las EMPRESAS USUARIAS no podrán comercializar EL SERVICIO con terceros.

5.1.10.4. No usar los medios contratados con fines contrarios a la ley, orden público, seguridad nacional, moral o buenas costumbres. En ese sentido, la EMPRESA USUARIA será la única responsable del uso que dé a EL SERVICIO contratado, responsabilizándose, además, por el contenido de la información que almacene, respalde o llegase a publicar en merito a EL SERVICIO contratado, liberando de esta forma a GMS - AIUKEN de cualquier responsabilidad que pudiera imputársele como consecuencia del uso, provecho o disfrute de ASBANC sobre EL SERVICIO.

5.1.10.5. No ceder las obligaciones y derechos emanados del presente contrato, salvo que medie autorización expresa y por escrito de GMS - AIUKEN.

5.1.10.6. Comunicar por escrito todo cambio de domicilio.

5.1.10.7. No utilizar bajo cualquier forma, de manera directa o indirecta, para los fines del presente Contrato y para cualquier otra finalidad, las marcas, logotipos, lemas comerciales y demás signos distintivos de GMS - AIUKEN sin su previa autorización por escrito.

5.1.10.8. Cumplir los protocolos de Seguridad y Acceso que comunique GMS - AIUKEN en su oportunidad.

5.2. Por parte de GMS:

5.2.1. Designar a los funcionarios idóneos de su organización a los roles que le correspondan dentro del equipo de trabajo establecido en el Anexo B.

5.2.2. Asegurar la puntual y efectiva ejecución de las responsabilidades que le correspondan en concordancia con el plan de trabajo detallado en el Anexo C.

5.2.3. Juntamente con AIUKEN, facilitar a LA ASOCIACIÓN la información técnica, comercial y funcional de los servicios para que pueda generar su propio material de marketing o elementos promocionales para procurar una mayor eficacia en la difusión comercial de sus productos y servicios.

5.2.4. Coordinar con AIUKEN la entrega puntual y efectiva de los servicios contratados por los CLIENTES de LA ASOCIACIÓN, en virtud de los Contratos Específicos, en concordancia con los estándares y condiciones establecidos en los documentos habilitantes según el Anexo G.

5.2.5. Facturar localmente a LA ASOCIACIÓN por todos los SERVICIOS SOC colocados a los CLIENTES en concordancia con los documentos habilitantes debidamente autorizados por LA ASOCIACIÓN para el efecto. De existir cualquier otro servicio o transacción debidamente autorizada por las partes, también será responsabilidad de GMS facturar el mismo a LA ASOCIACIÓN de forma local. Tal facturación deberá sujetarse a la normativa legal y fiscal del Perú.

5.2.6. Asegurar el pago puntual a AIUKEN de los cargos que correspondan a los servicios contratados y pagados por LA ASOCIACIÓN para sus CLIENTES, como también de cualquier cargo adicional que corresponda a otro servicio o transacción debidamente autorizada por las partes. Tales pagos deberán sujetarse a las normativas legales, fiscales y de comercio exterior del Perú.

5.3. Por parte de AIUKEN:

5.3.1. Designar a los funcionarios idóneos de su organización a los roles que le correspondan dentro del equipo de trabajo establecido en el Anexo B.

5.3.2. Asegurar la puntual y efectiva ejecución de las responsabilidades que le correspondan en concordancia con el plan de trabajo detallado en el Anexo C.

5.3.3. Atender con la máxima diligencia y profesionalidad posible todos los pedidos de servicios, soluciones o productos que LA ASOCIACIÓN gestione en nombre de sus CLIENTES.

5.3.4. Dar apoyo y soporte a LA ASOCIACIÓN en los aspectos técnicos y comerciales que le resulten necesarios para cumplir con su función.

5.3.5. Gestionar diligentemente la provisión, operación y cumplimiento de los acuerdos de nivel de servicio que recen en los contratos formalizados con los CLIENTES de LA ASOCIACIÓN

5.3.6. Facturar a GMS por los servicios o demás transacciones debidamente aprobadas por las partes, en concordancia con el contrato de distribución suscrito entre AIUKEN y GMS.

Asimismo, GMS y AIUKEN, conjuntamente tienen como obligaciones las siguientes:

- Prestar los SERVICIOS SOC a LOS CLIENTES de acuerdo con lo establecido en el presente contrato, en el Anexo 1 y en los contratos específicos que suscriba juntamente con LA ASOCIACIÓN y LOS CLIENTES, debiendo cumplir los parámetros de calidad, así como mantener operativo los SERVICIOS SOC, con exclusión de las interrupciones o suspensiones ocasionadas como consecuencia de caso fortuito o fuerza mayor, así como las derivadas del incumplimiento de LA ASOCIACIÓN y / o de las EMPRESAS USUARIAS.
- Atención conjunta exclusiva a las EMPRESAS USUARIAS del sector banca y finanzas, competencia de ASBANC.
- Cumplir con todas y cada una de las obligaciones establecidas en el presente Contrato, en sus Anexos, y en los contratos específicos que suscriba juntamente con ASBANC y las EMPRESAS USUARIAS.
- Recibir, tramitar y resolver todos y cada uno de los reclamos que pudiera presentar ASBANC y las EMPRESAS USUARIAS conforme a la legislación vigente.
- Otorgar acceso a ASBANC y a las EMPRESAS USUARIAS a los servicios de atención y números de emergencia.
- Realizar su mejor esfuerzo para mantener los niveles de calidad y disponibilidad de LA ASOCIACIÓN y de las EMPRESAS USUARIAS.

SEXTA.- INDEMNIZACIONES

Las partes serán mutuamente responsables entre si por las indemnizaciones que correspondan por daño emergente, lucro cesante, daño material o moral, directo o indirecto, presente o futuro que resulte directamente por el incumplimiento de sus respectivas responsabilidades asumidas por el presente contrato, por un valor máximo equivalente al pagado por ASBANC a GMS en los seis meses calendario previos a la fecha en la cual una parte reclame una indemnización.

SÉPTIMA.- AUTORIZACIÓN DE USO DE MARCAS

AIUKEN y GMS autorizan expresamente a ASBANC para utilizar el nombre y la marca que les corresponden respectivamente, sólo en relación al cumplimiento del presente contrato y de los contratos específicos que LA ASOCIACIÓN suscriba con LOS CLIENTES. Por otro lado, para un uso adicional, ASBANC someterá a la aprobación de AIUKEN y GMS respectivamente cualquier utilización de sus nombres y marcas, ya sea en el establecimiento comercial, en los papeles, documentos, materiales de promoción, publicidad, etc., previamente a su utilización.

OCTAVA.- EXCLUSIVIDAD

Las partes se conceden mutuamente la exclusividad en su relación comercial según el objeto del presente contrato, consistiendo explícitamente en lo siguiente:

8.1. LA ASOCIACIÓN ofrecerá a sus clientes (sean estos del sector financiero o no) únicamente los SERVICIOS SOC amparados por el presente contrato, a ser ejecutados exclusivamente por AIUKEN y GMS. LA ASOCIACIÓN no ofrecerá a sus clientes ningún otro servicio ni producto orientado a la CIBER SEGURIDAD. En caso de que se identifique la posibilidad de ofrecer SERVICIOS SOC adicionales a los catalogados en el presente contrato, las partes trabajarán conjuntamente para desarrollar los mismos e integrarlos al presente contrato.
8.2. AIUKEN y GMS no realizarán ofertas directas a entidades que tengan un giro de negocio sujeto a la regulación de la Superintendencia de Banca, Seguros, y AFP, tales como bancos, financieras, cajas de crédito y cooperativas, independientemente de que sean estas Afiliadas a ASBANC. Cualquier gestión comercial a estas entidades se realizará exclusivamente dentro del marco del presente contrato.
8.3. Para claridad, las partes reconocen explícitamente que la compraventa de productos de CIBER SEGURIDAD provistas por distintos FABRICANTES no constituye un SERVICIO SOC, independientemente de que ciertas soluciones de dichos FABRICANTES también puedan ofrecerse como un SERVICIO SOC. Al ser parte del giro normal de negocios de AIUKEN y GMS, ofertas que realicen de forma individual o conjunta de compraventa de productos a CLIENTES de LA ASOCIACIÓN no constituirían un incumplimiento de la exclusividad acordada.
8.4. Las partes reconocen que el giro de negocios de comercialización de SERVICIOS SOC es variable y, como tal, puede haber circunstancias en las que excepciones en el manejo de la exclusividad pueden ser de mutuo beneficio. Sin embargo, las partes aceptan que cualquier excepción que se pueda otorgar al compromiso de exclusividad deberá ser previo a una autorización escrita y debidamente firmada por las partes, la cual aplicará únicamente al caso especificado.

NOVENA.- SUSPENSIÓN DE SERVICIOS

GMS y AIUKEN se reservan el derecho de suspender la prestación del servicio que corresponda, en caso que:

a) Por uso indebido de los SERVICIOS SOC, como por ejemplo, los siguientes actos: (I) Utilizar los SERVICIOS SOC contratado para uso de terceros, quedando estrictamente prohibida la transferencia / cesión / comercialización del presente Contrato, total o parcialmente, a dichos terceros, bajo cualquier título; (II) Utilizar personal propio y/o de terceros, software o cualquier metodología o proceso con fines maliciosos para afectar, degradar, dañar los aplicativos o Infraestructura Tecnológica que forman parte de los SERVICIOS SOC (III) Usar medios contratados con fines contrarios a la ley, orden público, seguridad nacional, moral o buenas costumbres; (IV) Ceder las obligaciones y derechos emanados del presente Contrato, salvo que medie autorización expresa y por escrito de **GMS y AIUKEN**; (V) Utilizar bajo cualquier forma, de manera directa o indirecta para los fines del presente Contrato y par cualquier otra finalidad, las marcar registradas, logotipos, lemas comerciales y demás distintivos de GMS y / o AIUKEN sin previa autorización por escrito; (VI) Utilizar los SERVICIOS SOC más allá de las razones sociales (RUC) contratada por LA ASOCIACIÓN y LOS CLIENTES. Queda establecido que, si esta causal perdura por más de cinco (5) días calendario, **GMS y AIUKEN** dará por resuelto el presente Contrato y le será de aplicación la penalidad establecida en el 2° párrafo de la cláusula tercera.
b) Por la declaración de insolvencia y/o quiebra de LA ASOCIACIÓN de acuerdo con la legislación de la materia.
c) Por mandato judicial.

LA ASOCIACIÓN deberá incorporar las causales de suspensión del servicio señaladas en la presente cláusula dentro de los contratos específicos, a fin de que GMS y AIUKEN tenga facultades para suspender parcialmente el servicio, únicamente en relación con LOS CLIENTES que incurra en la causal de suspensión, sin afectar al resto de LOS CLIENTES o a LA ASOCIACIÓN.
La suspensión se mantendrá hasta que cesen las causas mencionadas sin perjuicio de la facultad de GMS y AIUKEN para resolver el presente contrato. La suspensión de LA ASOCIACIÓN, siempre que las causas de suspensión sean imputables a LA ASOCIACIÓN o a LOS CLIENTES, en ningún caso exime al mismo del cumplimiento de todas y cada una de las obligaciones emanadas del presente contrato y sus Anexos, en especial aquellas obligaciones que se encuentren pendientes de pago o de cumplimiento por parte de LA ASOCIACIÓN, así como la devolución de los equipos y/o facilidades de propiedad de GMS y AIUKEN, entre otras.

DÉCIMA.- CUMPLIMIENTO DE NORMAS DE LA SBS Y OTRAS NORMAS

GMS y AIUKEN se comprometen al cumplimiento de las disposiciones emitidas por la Superintendencia de Banca, Seguros y AFP relacionadas con la subcontratación de servicios y con la gestión del riesgo operacional.

LA ASOCIACIÓN como empresa que respalda la prestación de **los SERVICIOS SOC** declara contar con un plan de contingencia para la continuidad de la prestación de los servicios materia del presente contrato, en caso ocurrieran eventos de fuerza mayor o caso fortuito que lo imposibilitaran a cumplir con sus obligaciones.

LA ASOCIACIÓN mantiene el referido plan bajo permanente revisión y actualización, por lo que su entrega a la GMS y AIUKEN queda sujeta a que sea solicitada formalmente y por escrito.

Todo tratamiento de datos personales que realicen las partes en el marco de la ejecución de los términos del presente contrato y de los servicios descritos en los respectivos acuerdos de nivel

de servicio, en tanto se trate de datos cuya titularidad sea ejercida por una o más personas naturales, deberá sujetarse al marco normativo establecido por la Ley de Protección de Datos Personales, su Reglamento y normas modificatorias y complementarias. La parte que transfiera a la otra datos personales no anonimizados dentro del ámbito de aplicación de las referidas normas, asume plena responsabilidad sobre la obtención de los consentimientos respectivos de parte de sus legítimos titulares para la realización de este tratamiento, siendo su deber cumplir y acreditar el cumplimiento de las obligaciones legalmente establecidas para el titular o encargado del banco de datos personales, así como informar clara e inequívocamente a la otra parte acerca de los límites de los consentimientos obtenidos.

UNDÉCIMA.- CONFIDENCIALIDAD

LA ASOCIACIÓN, AIUKEN y GMS acuerdan que toda la información en general de su contraparte revelada en cada caso en relación con este Contrato, tienen el carácter de información confidencial, incluyendo pero no limitado a:

- Definiciones de servicios de ciberseguridad, incluyendo sus alcances, configuraciones y especificaciones técnicas.
- Metodologías y estratégicas comerciales, incluyendo material de capacitación para el personal de las Partes y planes de desarrollo del mercado.
- Precios, cotizaciones y términos comerciales, incluyendo los parámetros con los cuales se define una oferta.
- Todos los contratos que eventualmente se puedan firmar entre las partes, incluyendo sus borradores y material previo requerido para su elaboración, como también los anexos y demás documentos que puedan formar parte integrante de los mismos contratos.
- Toda información financiera de las Partes, tales como estados financieros, que puedan intercambiar entre sí.

En el supuesto de que, previamente a la celebración de este Contrato, cualquiera de las Partes hubiera tenido acceso a información de la otra Parte, aquélla será considerada, a todos los efectos previstos en la presente cláusula, como Información Confidencial, salvo aquélla que expresamente sea calificada por la Parte emisora como información de libre uso y/o divulgación. Las Partes establecen que toda la información intercambiada en el proceso de selección de un socio para servicios SOC, llevado adelante por ASBANC a partir de abril del 2018, incluyendo el RFP, las consultas, las ofertas, las respuestas, y las aclaraciones, se enmarca en la definición de información confidencial del presente acuerdo.

En tal sentido, las partes quedan prohibidas de divulgar y transferir a terceros la información confidencial señalada en el párrafo anterior, así como de incorporarla en redes nacionales o internacionales de transmisión de datos, sin la autorización previa y expresa de su contraparte, bajo responsabilidad civil sobre los daños causados por la infracción de este deber de prohibición.

Las partes asumen el compromiso de guardar reserva respecto de toda información, operaciones comerciales, técnicas y en general de toda información de su contraparte, que conozca en la ejecución de las obligaciones y compromisos asumidos en virtud del presente Contrato.

En consecuencia, las partes se encuentran impedidas de divulgar a terceros de manera total o parcial cualquier información de su contraparte a la que acceda, que reciba directa o indirectamente o que se genere como consecuencia de la ejecución del presente Contrato, o

emplearla para fines distintos a los del presente Contrato, obligándose a mantener absoluta reserva y confidencialidad sobre su contenido. Entonces queda establecido que la presente estipulación tiene carácter esencial en la celebración del presente Contrato y que el compromiso de las partes subsistirá indefinidamente, inclusive una vez que se agote el plazo de vigencia del presente Contrato, o cuando por cualquier razón el presente Contrato concluya, resulte nulo o ineficaz.

Para los fines del presente Contrato, no será considerada información "confidencial" o "privada" la que:

a. Sea o llegue a ser de dominio público por causa distinta al incumplimiento de la obligación de guardar reserva;
b. Sea conocida lícitamente por una de las partes antes que la otra la hubiera transmitido; o,
c. Tenga autorización de divulgación escrita y legítima, a cargo de la parte propietaria o responsable de la información.

En consecuencia, la obligación de las partes de mantener reserva y confidencialidad no será aplicable a la información referida en el párrafo anterior.

Si alguna de las partes resulta legalmente compelida por autoridad competente a revelar cualquier información confidencial recibida, deberá dar aviso a su contraparte a fin de que ésta adopte las medidas legales que considere pertinentes. Si la impugnación planteada resulta infundada, o renuncia al privilegio de confidencialidad sobre la información confidencial, o el mandato o requerimiento legal de entrega de la información confidencial es firme y exigible, entonces la parte legalmente compelida proporcionará solo aquella información confidencial que le sea requerida formalmente.

DUODÉCIMA.- PLAZO DEL CONTRATO

El presente contrato iniciará el **XXX** y tendrá un plazo inicial de un año calendario. Este plazo será extendido automáticamente para amparar todo SERVICIO SOC que sea colocado por LA ASOCIACIÓN mediante los Contratos Específicos y debidamente aceptado con su respectiva orden de trabajo según el Anexo G. El plazo también será extendido de forma automática por períodos anuales sucesivos en caso de que ninguna de las partes exprese por escrito su deseo contrario con al menos 90 días calendario de anticipación.

DECIMOTERCERA.- RESOLUCIÓN DE CONTRATO

Las partes podrán dar por terminado el presente Contrato anticipadamente, sin responsabilidad, autorización alguna o necesidad de resolución judicial ni arbitral previa, mediante carta a la otra parte con una anticipación no menor a ciento ochenta (180) días calendario a la fecha efectiva de resolución.

El mecanismo de resolución será el siguiente: La parte que desee resolver el contrato deberá dar aviso por escrito a la otra con una anticipación no menor a ciento ochenta (180) días calendarios a la fecha en que desee que opere la resolución contractual. Dicha resolución no dará lugar a ningún pago compensatorio o de otra naturaleza ni a responsabilidad alguna por parte de ella, más que el pago de cualquier factura que pudiera tener pendiente de pago por los servicios brindados hasta la fecha establecida para la resolución del contrato.

A la terminación del contrato, GMS y AIUKEN descontinuarán todo SERVICIO SOC que haya estado en operación. Cualquier valor pendiente de pago por parte de ASBANC a GMS deberá ser transferido en su totalidad en un plazo máximo de 10 días laborales. Adicionalmente, ASBANC cesará de inmediato todo uso del nombre, marca, denominación o de cualquier signo distintivo de AIUKEN o GMS, y deberá entregar a AIUKEN y GMS todo elemento de configuración, documentación y / o material promocional que haya recibido de éstas partes para efectos del presente contrato, en un plazo no superior a 30 días calendario desde la finalización.

DECIMOCUARTA.- CARÁCTER CIVIL

Este contrato es de carácter civil y no supone constitución de una sociedad, asociación, joint-venture, vínculo laboral, agencia, sucursal o representación, o cualquier otro tipo similar de vinculación entre las tres partes. Todas las partes en calidad de entidad se mantienen jurídicamente independientes y toda acción, derecho u obligación de cada una de las partes que no estén contempladas en este contrato serán de la única y exclusiva competencia de la parte correspondiente, sin que ello afecte en forma alguna a la otra parte.

DECIMOQUINTA.- SOLUCIÓN DE CONFLICTOS

Las partes recurrirán al trato directo para solucionar cualquier conflicto y/o controversia en torno al presente contrato, trato directo que no excederá de quince (15) días hábiles desde comunicado el conflicto y/o controversia a la otra parte.

En el supuesto negado de no arribar a una solución armoniosa, o transcurrido el plazo del párrafo anterior, recurrirán obligatoriamente al proceso de Arbitraje.

La fijación de los puntos controvertidos, el nombramiento del árbitro o de los árbitros componentes del Tribunal, así como el procedimiento para el desarrollo del arbitraje, el pago de los honorarios de los árbitros y los demás aspectos relevantes del mismo, se sujetarán a lo establecido por el Reglamento del Centro de Arbitraje de la Cámara de Comercio de Lima. El arbitraje será de derecho por lo que el o los árbitros serán abogados y el idioma será el castellano. El procedimiento arbitral no deberá prolongarse por más de veinte (20) días calendario.

Si antes de la expedición del laudo, las partes concilian sus pretensiones, el Tribunal dictará una orden de conclusión del procedimiento.

En caso de conciliación parcial, el proceso de arbitraje continuará respecto de los demás puntos controvertidos.

El Laudo arbitral emitido es definitivo e inapelable, tiene el valor de cosa juzgada y se ejecuta como una sentencia.

DECIMOSEXTA.- COORDINADORES DE LAS PARTES

Para efectos de la coordinación de los aspectos operativos derivados de la ejecución del presente contrato específico, las partes acuerdan establecer los siguientes datos de contacto:

Datos de **AIUKEN**:

1. Nombre del representante: _____.
2. Cargo del representante: _____.
3. Correo electrónico del representante: _____
4. Dirección domiciliaria del representante:_____
5. Número telefónico del representante: _____

Datos de **GMS**:

1. Nombre del representante: _____
2. Cargo del representante: _____
3. Correo electrónico del representante: _____
4. Dirección domiciliaria del representante: _____
5. Número telefónico del representante: _____

Datos de **LA ASOCIACIÓN**:

1. Nombre del representante: _____
2. Cargo del representante: _____
3. Correo electrónico del representante: _____
4. Dirección domiciliaria del representante: _____
5. Número telefónico del representante: _____

La actualización de los datos de contacto que preceden se formalizará por escrito a través de una carta dirigida por el representante legal de la parte que corresponda. Los cambios de los datos de contacto se harán efectivos a partir del tercer día hábil contado desde el primer día hábil siguiente a la fecha de recepción de la carta que los comunique.

DECIMOSÉPTIMA.- CESIÓN DE POSICIÓN CONTRACTUAL Y SUBCONTRATACIÓN

Las partes acuerdan expresamente que GMS y AIUKEN no podrá transferir y/o ceder el presente contrato, así como los derechos y/u obligaciones que se deriven de él, salvo autorización previa y por escrito de LOS CLIENTES.

Por su parte, LA ASOCIACIÓN no podrá transferir y/o ceder el presente contrato, así como los derechos y/u obligaciones que se deriven de él, salvo autorización previa y por escrito de GMS y AIUKEN.

Cualquier subcontratación estará sujeta a la aprobación explícita y por escrito de las contrapartes, en cuyo caso la parte subcontratante será la única responsable ante sus contrapartes por los actos u omisiones de sus subcontratistas y de las personas directa o indirectamente empleadas por ellos.

DECIMOCTAVA.- CLÁUSULA ANTISOBORNO

LA ASOCIACIÓN, GMS y AIUKEN reconocen, garantizan y se comprometen a que, en relación con:

(i) las transacciones contempladas por el presente Contrato, (ii) cualquier cuestión relacionada directa o indirectamente al presente Contrato, incluyendo, sin limitación la negociación de este Contrato y el cumplimiento de GMS y AIUKEN de las obligaciones bajo el presente Contrato, o (iii) cualesquiera otras transacciones que impliquen, o sean realizadas en nombre de LA ASOCIACIÓN.

(a) no ha violado o incumplido y se compromete a no violar o incumplir cualquier ley de anticorrupción y leyes antisoborno y demás regulaciones que resulten aplicables,

(b) no ha realizado y se compromete a no realizar las siguientes prácticas: realización de pagos o transferencias de valor, ofertas, promesas o concesiones de cualquier beneficio financiero u otra ventaja, ya sea directa o indirectamente, la cual tenga como propósito o efecto de corrupción pública o comercial, de aceptación o de conformidad en el soborno, la extorsión, o cualquier otro medio ilegal o indebido para obtener o retener un negocio, una ventaja comercial o un inadecuado desempeño de cualquier función o actividad.

GMS y AIUKEN deberán ceñirse al cumplimiento de dicha legislación sin contravenirla, y no podrá utilizar el nombre de LA ASOCIACIÓN para realizar gestiones que vayan contra ella.

DÉCIMONOVENA.- DIVISIBILIDAD Y RENUNCIA

El presente contrato representa la totalidad del acuerdo entre las partes en relación con su objeto y como tal las partes expresan que el cumplimiento debe respetarse en su totalidad. En caso de que cualquier obligación sea determinada como inaplicable, sea por mutuo acuerdo de las partes o por laudo arbitral, las demás obligaciones establecidas contractualmente se mantendrán en todo su rigor. Adicionalmente, si una de las partes permitiera, una o varias veces, que la otra incumpla sus obligaciones o las cumpla imperfectamente o en forma distinta a la pactada, sin ejercer oportunamente los derechos contractuales o legales que le correspondan, no se reputará ni equivaldrá como modificación del presente contrato, ni renuncia de los derechos de dicha parte en el futuro.

VIGÉSIMA.- CASO FORTUITO Y FUERZA MAYOR

Las partes estarán eximidas de toda responsabilidad en caso del incumplimiento de sus obligaciones materia del presente contrato cuando tal incumplimiento sea consecuencia directa de situaciones producidas por caso fortuito o fuerza mayor, es decir causas no imputables a las partes, consistentes en eventos extraordinarios imprevisibles o irresistibles. Si tales casos fortuitos o de fuerza mayor fuesen de tal dimensión que impidan de forma determinante que alguna de las partes cumpla de forma material sus obligaciones pactadas, el presente contrato quedara resuelto sin responsabilidad alguna para las partes.

VIGÉSIMA PRIMERA.- PROPIEDAD INTELECTUAL

Las partes acuerdan que todos los derechos de propiedad intelectual e industrial sobre descubrimientos, invenciones, ideas, conceptos, diseños, mejoras de cualquier tipo, patentes, modelos industriales o de utilidad, presentaciones comerciales, etiquetas, planes de marketing, estrategias, datos técnicos, know-how, bocetos y dibujos de ingeniería y, en general, sobre las actividades que se encuentren contenidas o relacionadas o sean consecuencia o resultado únicamente sobre los servicios objeto del presente contrato, corresponden exclusivamente a AIUKEN y GMS. Al mismo tiempo, AIUKEN y GMS otorgan a LA ASOCIACIÓN el derecho de uso de dicha propiedad intelectual exclusivamente para promover el objeto del presente contrato mientras el mismo se mantenga vigente.

VIGÉSIMA SEGUNDA

Las partes podrán realizar modificaciones al presente contrato, sea a sus cláusulas principales o anexos, por medio de adendas escritas, acordadas y debidamente firmadas entre ellas.

VIGÉSIMO TERCERA.- LEGISLACIÓN APLICABLE Y CONVENIO ARBITRAL

La legislación aplicable para la ejecución de las obligaciones materia del presente Contrato Marco es la vigente en el territorio de la República del Perú.

Ante cualquier controversia o diferencia derivada de este contrato, las partes se someten a la resolución de un Tribunal de Arbitraje de la Cámara de Comercio Americana del Perú. Las partes renuncian a la jurisdicción ordinaria, se obligan a acatar el laudo que expida el Tribunal Arbitral y se comprometen a no interponer ningún tipo de recurso en contra del laudo arbitral. Para la ejecución de las medidas cautelares el Tribunal Arbitral está facultado para solicitar de los funcionarios públicos, judiciales, policiales y administrativos su cumplimiento, sin que sea necesario recurrir a juez ordinario alguno. El Tribunal Arbitral estará integrado por tres árbitros y el procedimiento arbitral será confidencial y en derecho. El lugar de arbitraje será dentro de las instalaciones de la Cámara de Comercio Americana del Perú.

VIGÉSIMO CUARTA.- DECLARACIONES DE LA ASOCIACIÓN

LA ASOCIACIÓN , GMS y AIUKEN declaran que no tienen conocimiento de juicio, procedimiento arbitral o administrativo alguno en el cual sean parte y cuyo resultado genere o pueda generar en el futuro un perjuicio respecto del negocio o sus operaciones, sus situaciones financieras o sus capacidades para cumplir con sus obligaciones derivadas del presente contrato y que asumen frente a los CLIENTES.

Asimismo, declaran que cumplirán con informar a los CLIENTES de cualquier hecho existente o sobreviniente que restrinja, deteriore o limite de cualquier forma la correcta prestación de los servicios materia del presente contrato.

En señal de conformidad, se firma el presente Contrato en dos ejemplares de igual tenor y validez

Nombre: Miguel Vargas Ascenzo	**Nombre:**
Cargo: Gerente General de ASBANC	**Cargo:**

Lugar y fecha de firma:	**Lugar y fecha de firma:**
Nombre: Patricia Barreda Meyer **Cargo: Gerente de Coordinación Institucional** **Lugar y fecha de firma:**	**Nombre:** **Cargo:** **Lugar y fecha de firma:**

Anexo XI: DICCIONARIO DE COMPETENCIAS

Innovación

Es la capacidad de idear soluciones nuevas y diferentes para resolver problemas o situaciones requeridas por le propio puesto, la organización, los clientes o el segmento de la economía donde actúe.

A. Presenta una solución novedosa y original, a la medida de los requerimientos del cliente, que ni la propia empresa ni otros habían presentado antes.
B. Presenta soluciones a problemas o situaciones de los clientes que la empresa no había ofrecido nunca.
C. Aplica/recomienda soluciones para resolver problemas o situaciones utilizando su experiencia en otras similares.
D. Aplica/recomienda respuesta estándar que el mercado u otros utilizarían para resolver problemas/situaciones similares a los presentados en su área.

Nivel de compromiso – Disciplina personal – Productividad

Apoyar e instrumentar decisiones por completo con el logro de objetivos comunes. Ser justo y compasivo aun en la toma de decisiones en situaciones difíciles. Prevenir y superar obstáculos que interfieren con el logro de los objetivos del negocio. Controlar la puesta en marcha de las acciones acordadas. Cumplir con sus compromisos. Poseer la habilidad de establecer para sí mismo objetivos de desempeño más altos que el promedio y de alcanzarlos con éxito.

A. Apoya e instrumenta todas las directivas que recibe en pos del beneficio de la organización y de los objetivos comunes. Establece para sí mismo objetivos de alto desempeño, superiores al promedio y los alcanza con éxito. Los integrantes de la comunidad en la que se desenvuelve lo perciben como un ejemplo a seguir por su disciplina personal y alta productividad.
B. Apoya e instrumenta las directivas recibidas transmitiendo a los otros, por medio del ejemplo, la conducta a seguir. Se fija objetivos altos y los cumple casi siempre.
C. Instrumenta adecuadamente las directivas recibidas, fija objetivos de alto rendimiento para el grupo que en raras ocasiones él mismo alcanza.
D. Raramente demuestra algún apoyo a las directivas recibidas. Piensa primero en sus propias posibilidades y beneficios antes que en los del grupo y los de la organización a la que pertenece.

Integridad

Es la capacidad de actuar en consonancia con lo que se dice o se considera importante. Incluye comunicar las intenciones, ideas y sentimientos abierta y directamente y estar dispuesto a actuar con honestidad incluso en negociaciones difíciles con agentes externos. Las acciones son congruentes con lo que se dice. Queda fuera de este concepto cualquier manifestación de “doble discurso”, como “haz lo que digo, pero no lo que hago”, actitud frecuente en muchos managers.

A. Trabaja según sus valores, aunque ello implique un importante coste o riesgo. Se asegura de señalar tanto las ventajas como los inconvenientes de un trato. Despide o no contrata a una persona de dudosa reputación, aunque tenga alta productividad. Da permiso a una persona que lo está pasando mal a causa del gran estrés para que se recupere. Propone o decide, según su nivel de incumbencia, abandonar un producto, servicio o línea que aun siendo productivo él considera poco ético. Se considera que es un referente en materia de integridad.
B. Admite públicamente que ha cometido un error y actúa en consecuencia. Dice las cosas como son, aunque pueda molestar a un viejo amigo. No está dispuesto a cumplir órdenes que impliquen acciones que él considera que no son éticas. Acepta este tipo de planteo de sus subordinados e investiga las causas.
C. Desafía a otros a actuar con valores y creencias. Está orgulloso de ser honrado. Es honesto en las relaciones con los clientes. Da a todos un trato equitativo.
D. Es abierto y honesto en situaciones de trabajo. Reconoce errores cometidos o sentimientos negativos propios y puede comentárselos a otros. Expresa lo que piensa, aunque no sea necesario o sea más sencillo callarse.

Orientación al cliente

Implica el deseo de ayudar o servir a los clientes, de comprender y satisfacer sus necesidades. Implica esforzarse por conocer y resolver los problemas del cliente, tanto del cliente final al que van dirigidos los esfuerzos de la empresa como los clientes de sus clientes y todos aquellos que cooperen en la relación empresa – cliente, como los proveedores y el personal de la organización.

A. Establece una relación con perspectivas de largo plazo con el/los clientes/s para resolver sus necesidades, debiendo sacrificar en algunas ocasiones beneficios inmediatos en función de los futuros. Busca obtener beneficios a largo plazo para el cliente, pensando incluso en los clientes de los clientes. Es un referente dentro de la organización en materia de ayudar y satisfacer las necesidades de los clientes.
B. Promueve, y en ocasiones lo hace personalmente, la búsqueda de información sobre las necesidades latentes, pero no explícitas, del cliente. Indaga proactivamente más allá de las necesidades que el/los clientes/s manifiestan en un principio y adecua los productos y servicios disponibles a esas necesidades.
C. mantiene una actitud de total disponibilidad con el cliente, brindando más de lo que éste espera. El cliente siempre puede encontrarlo. Dedica tiempo a estar con el cliente ya sea en su propia oficina o en la del cliente.
D. Promueve, y en ocasiones lo hace personalmente, el contacto permanente con el cliente para mantener una comunicación abierta con él sobre las expectativas mutuas y para conocer el nivel de satisfacción.

Empowerment

Establece claros objetivos de desempeño y las correspondientes responsabilidades personales. Proporciona dirección y define responsabilidades. Aprovecha claramente la diversidad (heterogeneidad) de los miembros del equipo para lograr un valor añadido superior para el negocio. Combina adecuadamente situaciones, personas y tiempos. Tiene adecuada integración al equipo de trabajo. Comparte las consecuencias de los resultados con todos los involucrados. Emprende acciones eficaces para mejorar el talento y las capacidades de los demás.

A. define claramente objetivos de desempeño asignando las responsabilidades personales correspondientes. Aprovecha la diversidad de su equipo para lograr un valor añadido superior en el negocio. Cumple la función de consejero confiable compartiendo las consecuencias de los resultados con todos los involucrados. Emprende permanentes acciones para mejorar el talento y las capacidades de los demás.
B. Fija objetivos de desempeño asignando responsabilidades y aprovechando adecuadamente los valores individuales de su equipo, de modo de mejorar el rendimiento del negocio.
C. Fija objetivos y asigna responsabilidades al equipo.
D. Escasa capacidad para transmitir objetivos y asignar responsabilidades en función de la rentabilidad del negocio

Orientación a los resultados

Es la tendencia al logro de resultados, fijando metas desafiantes por encima de los estándares, mejorando y manteniendo altos niveles de rendimiento, en el marco de las estrategias de la organización.

A. Siempre va un paso más adelante en el camino de los objetivos fijados, preocupado por los resultados globales de la empresa. Contribuye con otras áreas en el alineamiento de sus objetivos por los definidos por la empresa en el ámbito local o internacional (según corresponda). Se preocupa por el resultado de otras áreas. Aporta soluciones incluso frente a problemas complejos y en escenarios cambiantes, aporta soluciones de alto valor agregado para la organización.
B. Establece sus objetivos considerando los posibles beneficios/rentabilidad del negocio. Compromete a su equipo en el logro de ellos y lo insta a asumir riesgos de negocios calculados. Emprende acciones de mejora, centrándose en la optimización de recursos y considerando todas las variables.
C. Fija objetivos para su área en concordancia con los objetivos estratégicos de la organización. Trabaja para mejorar su desempeño introduciendo los cambios necesarios en la órbita de su accionar.
D. Trabaja para alcanzar los estándares definidos por los niveles superiores, en los tiempos previstos y con los recursos que se le asignan. Sólo en ocasiones logra actuar de manera eficiente frente a los obstáculos o imprevistos.

Comunicación.

Es la capacidad de escuchar, hacer preguntas, expresar conceptos e ideas en forma efectiva, exponer aspectos positivos. La habilidad de saber cuándo y a quién preguntar para llevar adelante un propósito. Es la capacidad de escuchar al otro y comprenderlo. Comprender la dinámica de grupos y el diseño efectivo de reuniones. Incluye la capacidad de comunicar por escrito con concisión y claridad

A. Es reconocido por su habilidad para identificar los momentos y la forma adecuados para exponer diferentes situaciones en las políticas de la organización y llamado por otros para colaborar en estas situaciones. Utiliza herramientas y metodologías para diseñar y preparar la mejor estrategia de cada comunicación.
B. Es reconocido en su área de incumbencia por ser un interlocutor confiable y por su habilidad para comprender diferentes situaciones y manejar reuniones.
C. Se comunica sin ruidos evidentes con otras personas tanto en forma oral como escrita.
D. En ocasiones sus respuestas orales o escritas no son bien interpretadas

Aprendizaje continúo

Es la habilidad para buscar y compartir información útil para la resolución de situaciones de negocios utilizando todo el potencial de la empresa (o corporación según corresponda). Incluye la capacidad de capitalizar la experiencia de otros y la propia propagando el Know How adquirido en foros locales o internacionales

A. Es reconocido como un experto en su especialidad en el medio donde actúa y como experto en la comunidad internacional. Comparte sus conocimientos y experiencia actuando como agente de cambio y propagador de nuevas ideas y tecnologías.
B. Participa en la comunidad local actuando como referente. Ofrece su experiencia y conocimientos para resolver problemas de otras áreas. Escribe papers, artículos, informes o realiza trabajos de investigación que comparte con colegas en el ámbito local.
C. Realiza un gran esfuerzo por adquirir nuevas habilidades y conocimientos. Busca y analiza proactivamente información pertinente para planificar un curso de acción.
D. mantiene su formación técnica, aunque tiene una actitud reactiva: busca información sólo cuando la necesita, lee manuales/libros para aumentar sus conocimientos básicos

Anexo XII: Caracteristicas Técnicas del Servicio de Outsourcing

Tipo de Sistema: MPLS		
	CUMPLE	**OBSERVACIONES**
ENLACE		
1.- Conexión con Instituciones	**SI**	El servicio de Outsourcing contempla la interconexión de los nodos remotos y de los nodo central y alterno con Instituciones (ASBANC, Bancos, Centros de Información u otros que se solicite) mediante una RPV (Red Privada Virtual) basada en tecnología MPLS, mediante el tipo de malla completa (full mesh) para las sedes de Lima, lo que es equivalente a una línea dedicada para el caso de (02) sedes.
2.- Data, Voz y Video por un solo medio	**SI**	La tecnología MPLS permite manejar Voz, Datos y Video a través de un mismo medio. La Red IP RPV de AMERICA MOVIL PERU S.A.C. mediante la que se brinda el servicio, está diseñada sobre una plataforma MPLS de alta capacidad, la cual le permite manejar trafico multiservicio (voz, vídeo y datos) El servicio RPV contempla tres clases de servicio (COS). Las COS podrán ser configuradas de acuerdo al requerimiento de calidad de servicio de cada tráfico que viaje a través de la RPV (voz/vídeo, datos críticos y datos normales).
3.- Voz sobre IP (VoIP)	**SI**	La tecnología MPLS a utilizar en Bancared le permite manejar todos los servicios de valor agregado sobre IP (Voz, Video, etc.). Si bien esta es una característica de la tecnología, su aprovechamiento estará en función del ancho de banda y los COS asignados. Para VoIP se utiliza el estándar de compresión G.729 (CS-ACELP) y la COS 3, lo cual permite priorizar este tráfico sensible al retardo en el tiempo.
4.- Enlace Principal, redundancia de la red y enlace de Back-Up	SI	El enlace principal contratado para el nodo central está constituido por 02 enlaces independientes de 7 Mbps de capacidad provenientes de 02 nodos diferentes. El enlace principal utilizado en el nodo alterno está constituido por un enlace de 7 Mbps, y para los nodos remotos, capacidades variables desde 256Kbps hasta 4 Mbps. Los enlaces instalados para Bancared, serán de uso exclusivo, no utilizándose parte de los mismos para cubrir otros servicios. AMERICA MOVIL PERU S.A.C. utiliza para Bancared la plataforma de red con que cuenta, que está cimentada sobre cuatro (04) Switches MPLS Cisco GSR 12000 de alta capacidad en el núcleo y más de quince (15) Switches MPLS Catalyst 4500 en la capa de distribución, estando todos estos equipos conectados con enlaces de fibra óptica redundantes, que aseguran la escalabilidad y confiabilidad de la red en su conjunto. La tecnología de nuestra plataforma, permite reenrutar los caminos virtuales existentes en la RPV de forma automática en

		caso de fallas. La topología de la RPV ofertada es de malla completa (full mesh). Adicionalmente, AMERICA MOVIL PERU S.A.C. se compromete a proveer, directamente o mediante terceros, enlaces conmutados de respaldo con conexiones MPLS, los cuales se activarán de manera automática en caso el enlace principal quede inoperativo por cualquier motivo. Estos enlaces de respaldo se conmutaran automáticamente cuando el enlace principal se reestablezca. El enlace de respaldo MPLS deberá quedar totalmente instalado, probado y operando automáticamente en el nodo remoto una vez implementada dicha tecnología.
EQUIPAMIENTO **Equipos Nodo Central**		
5.- Crecimiento y Flexibilidad	**SI**	AMERICA MOVIL PERU S.A.C. tiene ubicado en los equipos del Nodo Central de Bancared en sus instalaciones, las que reunirán las condiciones que permitan cumplir con las especificaciones técnicas de ambiente e infraestructura de tales equipos. El equipamiento del Nodo Central será de uso exclusivo para la red de Bancared. El Nodo Central ha sido configurado con una combinación de equipos que permite cubrir los requerimientos de servicios de red para la nueva topología RPV de Bancared en malla completa (full mesh). Se incluyen los equipos siguientes: dos (02) ruteadores Cisco 2921, dos (02) ruteadores Cisco 2901 HSEC, seis (06) switches Catalyst 2960, dos (02) Cisco ASA 5510, un (01) ruteador Cisco 2901 (2FXS). Estos equipos estarán configurados para brindar máxima seguridad a los servidores de Bancared.
6.- Tolerancia a Fallas	**SI**	La configuración de equipos que está instalado en el nodo Central constituye un sistema en alta disponibilidad. La interconexión de estos equipos se presenta en el documento de Propuesta Técnica. Además, dicho sistema utiliza el protocolo HSRP (Hot Stand-By Routing Protocol) que brinda una redundancia de 1:1.
7.- Protocolos TCP/IP , SNA	**SI**	La RPV permite transportar todos los protocolos incluidos en la familia TCP/IP estándar, y también el protocolo SNA mediante su encapsulamiento sobre IP utilizando la funcionalidad DLSW (DataLink Switching) disponible en los ruteadores Cisco.
8.- VPN	**SI**	El Nodo Central proporciona funcionalidades de 'tunneling' mediante el protocolo IPSec, de gran rendimiento y seguridad requeridos para construir Redes Privadas Virtuales (VPNs) para voz, datos y video.

9.- VLAN	**SI**	El Nodo Central ofrece funcionalidades de bridging y configuración de VLANs en los switches ofertados. El ruteo entre VLANs puede ser realizado con los ruteadores incluidos en el nodo. Los Firewall instalados también podrán configurar VLANs para los servicios de los nodos central y alterno.
10.- MPLS	**SI**	Todos los nodos de Bancared conectados a la RPV de AMERICA MOVIL PERU S.A.C. estarán configurados para clasificación y marcado de paquetes según la arquitectura MPLS estándar. El MPLS permite manejar todas las características de Calidad de Servicio (QoS) en la Red.
11.- Ancho de Banda Dinámico, ON DEMAND	**SI**	Se ofrece el servicio BoD (Ancho de banda por demanda) que es una funcionalidad de autoservicio a través de un Portal que permite reconfigurar las puertas RPV de Bancared.
12.- QoS	**SI**	La tecnología MPLS a utilizar permite manejar diversas funcionalidades de Calidad de Servicio (QoS) mediante la implementación de hasta 3 Clases de Servicio (COS). Entre las funcionalidades disponibles en los equipos CPE, podemos mencionar: CAR (Commited Access Rate), RED (Random Early Detection), WRED (Weighted RED), WFQ (Weighted Fair Queuing).
13.- CoS	**SI**	El servicio RPV permite dividir el tráfico en tres (03) Clases de Servicio (COS).
14.- Interface Ethernet	**SI**	El Nodo Central cuenta con interfaces 10/100 y con posibilidad de crecimiento.
15.- Back-Up automático (data y voz)	**SI**	La tecnología a utilizar permite contar con un respaldo automático para el tráfico de voz y datos a través del protocolo HSRP (Hot Stand-By Routing Protocol) con un tiempo de recuperación no perceptible por el usuario.
16.- Niveles de Seguridad	**SI**	La tecnología a utilizar permite manejo de distintos niveles de seguridad (Firewall) a través de filtros de paquetes, filtro de direcciones, autenticación de usuarios con acceso al router, manejo de perfiles de autorización y registro (log) de los intentos de acceso (fallidos o no).
17.- Nivel de Compresión de Voz y Datos	**SI**	La tecnología a utilizar permite compresión de datos (no recomendable para no perder el valor agregado de los COS) y de voz (G.729).
18.- Priorizar dinámicamente los aplicativos	**SI**	La tecnología MPLS a utilizar permite priorizar aplicaciones como la Voz sobre IP, mediante su asignación a la COS 3. Para priorizar el tráfico de datos crítico se debe realizar su asignación a la COS 2. El tráfico clasificado en COS 1 debe asignarse para los datos normales.

Equipos Nodo Alterno		
19.- Características del nodo alterno	**SI**	AMERICA MOVIL PERU S.A.C. ha ubicado los equipos del Nodo Alterno de Bancared en sus instalaciones de Villa El Salvador, las que reunirán las condiciones que permitan cumplir con las especificaciones técnicas de ambiente e infraestructura de tales equipos. El equipamiento del Nodo Alterno será de uso exclusivo para la red de Bancared. El Nodo Alterno ha sido configurado con una combinación de equipos que permite cubrir los requerimientos de contingencia en los servicios de red para la nueva topología RPV de Bancared en malla completa (full mesh). Se incluyen los equipos siguientes: un (01) ruteador Cisco 2921, un (01) ruteador Cisco 2901 HSEC, tres (03) switches Catalyst 2960, un (01) Cisco PIX 525. Estos equipos estarán configurados para brindar máxima seguridad a los servidores de Bancared.
20.- Funcionalidad	**SI**	El Nodo Alterno proporcionará las mismas facilidades técnicas y operativas con que cuenta el Nodo Central, considerando un escenario temporal de contingencia, a fin de mantener la disponibilidad de los servicios en Bancared. Este nodo no estará configurado en alta disponibilidad. El Nodo Alterno mantendrá todas las especificaciones técnicas indicadas en este anexo para el Nodo Central exceptuando las referidas a equipamiento y espacio físico. Deberá considerarse que todo cambio realizado en la Red, es decir, Nodo Central y nodo remotos deberá contemplar los efectos y cambios que deban realizarse en el Nodo Alterno para mantener la funcionalidad global del sistema. En la nueva topología de malla completa, la conexión IP entre el Nodo Central y el Nodo Alterno es permanente a través de la RPV.
Equipos Lado Remoto		
21.- Capacidad de Puerto Principal (Kbps)	**SI**	El puerto RPV principal configurado en cada sede será de: • 1 Mbps Los equipos Cisco ISR4321 tienen una capacidad de soportar hasta 10 Mbps. Estos equipos poseen interfaces FastEthernet. Para mayores capacidades será necesario un cambio de equipo. La infraestructura RPV Metro/Ethernet de AMERICA MOVIL PERU S.A.C., en Lima, puede ofrecer velocidades de hasta 1Gbps en los accesos.
22.- Back-Up automático (data)	**SI**	Considerando la nueva topología de malla completa en la RPV, el respaldo del tráfico de datos hacia el Nodo Central y/o el Nodo Alterno se encuentra disponible permanentemente mediante el enrutamiento directo del tráfico IP. El Back-Up automático considera su recuperación hacia el Nodo Alterno, en caso no se encuentre operativo el Nodo Central.

23.- Nivel de Compresión de Voz y Datos	**SI**	Permite comprimir un canal de voz regular de 64 Kbps a 8 Kbps (solo payload) a través del estándar G.729. Permite compresión de paquetes y de cabecera IP.
24.- Interfases LAN Ethernet o Token Ring	**SI**	El equipo cuenta con al menos una interfase LAN Ethernet o 10/100 Fast Ethernet. En caso se requiera una interfase Token Ring para la red LAN, se utilizará un equipo Cisco 2610, sujeto a disponibilidad de stock.
25.- Implementación de Equipos con Encriptación y DLSW	**SI**	Las funcionalidades de encriptación (DES y 3DES) y DLSW han sido consideradas en los equipos.
UBICACIÓN NODO CENTRAL Y ALTERNO		
26.- Ubicación y Seguridad	**SI**	Con la finalidad de cumplir con los estándares de calidad ofertados por AMERICA MOVIL PERU S.A.C., se ha implementado el Nodo Central y Alterno en las instalaciones de AMERICA MOVIL PERU S.A.C., quedando a cargo de AMERICA MOVIL PERU S.A.C. la instalación y mantenimiento del equipamiento incluido. El nodo central será implementado de acuerdo a los estándares de calidad de todas las instalaciones del backbone de AMERICA MOVIL PERU S.A.C. dentro de su red IP.
27.- Alojar Servidores de ASBANC	**SI**	Siguiendo el mismo esquema de calidad de servicio y basándonos en las características técnicas del Nodo central y alterno, los servidores de EL CLIENTE serán alojados en las instalaciones del nodo central y alterno para poder hacer un uso eficiente de los recursos de la red.
SERVICIO		
28.- 7x24 todo el año	**SI**	El servicio que ofrece AMERICA MOVIL PERU S.A.C. es de 24 horas los 7 días de la semana y los 365 días del año con una disponibilidad operativa del 99.98% anual. La disponibilidad operativa de la red, será medida en forma mensual en cada enlace remoto y en el nodo central, no en su conjunto.
29.- Reporte consumo de ancho de banda	**SI**	Se dará a EL CLIENTE acceso a la información en línea relativa al comportamiento del tráfico cursado de su enlace principal por fibra, a través .de una interfaz gráfica vía WEB.
30.- Tiempo de Respuesta a Fallas	**SI**	AMERICA MOVIL PERU S.A.C. se compromete a un máximo de cinco (05) minutos de tiempo de respuesta vía telefónica, para cualquier llamada en que se le solicite atender una falla o degradación del servicio. Dentro de ese tiempo se considera el necesario para canalizar y coordinar adecuadamente con su personal la atención del problema, antes de la intervención correctiva propiamente dicha.

		El tiempo total de respuesta ante fallas por parte de AMERICA MOVIL PERU S.A.C. será de dos (02) horas como máximo desde el registro de la avería. Debe considerarse dentro de esas dos (02) horas, las coordinaciones para el acceso al router, presencia de personal calificado a intervenir en la falla y la obtención del equipo en stock a ser reemplazado (si fuera necesario), así como la ejecución de los trabajos necesarios hasta concluir la solución a la falla. Se contempla cuatro niveles de atención: • Fallo total de los equipos de comunicación remotos. • Configuración ó enrutamiento del enlace principal o backup. • Caída del enlace principal • Caída del enlace principal y de respaldo.
31.- Tiempo de reposición de servicio	**SI**	El tiempo de reposición del servicio a sus condiciones normales será máximo de dos (02) horas, a excepción de los casos en que la falla sea de ruptura física del enlace de fibra óptica, en los que podrá tomar hasta ocho (08) horas.
32.- Mantenimiento y administración de los routers	**SI**	El mantenimiento de los ruteadores consistirá en la instalación, configuración de software, upgrade de software y reemplazo de dichos equipos en caso de fallas o por actualización tecnológica. La administración de los ruteadores consistirá en el monitoreo y manejo de estos equipos de modo remoto, de tal forma que se podrán visualizar alarmas y realizar actualizaciones de software desde el Centro de Gestión de AMERICA MOVIL S.A.C.
SEGURIDAD		
33.- Firewall en Nodo Central, Nodo Central - Alterno y Lado Remoto	**SI**	Se cuenta con el conjunto de características de software firewall de Cisco IOS certificado por ICSA que ofrece soporte para funciones de seguridad avanzadas, tales como: Context Based Access Control (CBAC), filtro de aplicaciones Java, denegación de protección de servicio y pistas de auditoria. El nodo central estará implementado con dos (02) Cisco ASA5510, en el nodo central alterno estará implementado un (01) Firewall PIX 525 y en las sedes remotas con IOS de Cisco. Estos equipos permitirán el manejo de niveles de encriptación por software (IPSEC) dentro de las cuales se considera DES y 3 DES, pudiendo ambas funcionar simultáneamente en la red, tanto a nivel del nodo central como sedes remotas; facilidad que sólo podrá ser explotada en los equipos ruteadores que contemplan las condiciones necesarias de procesamiento y IOS. Los equipos que no tuvieran estas facilidades conllevarían a ajustes en la mensualidad.
PLAZOS		
34.- Implementación del Nodo Remoto	**SI**	Se cuenta con xx días útiles a partir de la suscripción del contrato o recepción de la orden de servicio, y de contar con las facilidades técnicas necesarias para su implementación.

Anexo XIII: Análisis Financiero

Inversiones

Focus	$1,080	dolares
Consultor	$2,000	dolares
Lanzamiento	$8,000	dolares
Presentacion a GG	$3,000	dolares

Gastos Operativos

Comisiones del vendedor	5%	Ventas
Marketing	$7,716	Anuales
Sueldo del vendedor	$5,556	Anuales
Beneficios sociales del vendedor	$3,333	Anuales
Sueldo de personal operativo	$15,926	Anuales
Beneficios sociales del personal operat	$9,556	Anuales
Gastos Administrativos	2%	Ventas

Ingresos

Precio SOC	$8,000	mensual
Precio CSIRT	$1,000	mensual

Costo de Ventas

	Año 1											
	Jul	Ago	Set	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun
SOC	-	3,000	3,000	3,000	3,000	3,000	6,000	6,000	6,000	6,000	6,000	6,000
CSIRT	-	300	300	300	300	300	600	600	600	600	600	600
eBanking Protection	-	-	-	-	-	-	-	-	-	9,000	9,000	9,000
Ingeniería Social	-	-	-	-	-	-	4,000	4,000	4,000	4,000	4,000	4,000
Instalacion SOC	-	9,000	-	-	-	-	9,000	-	-	-	-	-
Instalacion SIEM	-	9,000	-	-	-	-	9,000	-	-	-	-	-
SIEM	-	1,000	1,000	1,000	1,000	1,000	2,000	2,000	2,000	2,000	2,000	2,000
Instalación eBanking	-	-	-	-	-	-	-	-	-	12,000	-	-
Instalación Ingeniería Social	-	-	-	-	-	-	5,000	-	-	-	-	-
Coste de Ventas	-	22,300	4,300	4,300	4,300	4,300	35,600	12,600	12,600	33,600	21,600	21,600

	Año 2											
	Jul	Ago	Set	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun
SOC	9,000	9,000	9,000	9,000	9,000	9,000	12,000	12,000	12,000	12,000	12,000	12,000
CSIRT	900	900	900	900	900	900	1,200	1,200	1,200	1,200	1,200	1,200
eBanking Protection	9,000	9,000	9,000	9,000	9,000	18,000	18,000	18,000	18,000	18,000	18,000	18,000
Ingeniería Social	4,000	4,000	8,000	8,000	8,000	8,000	8,000	8,000	8,000	8,000	12,000	12,000
Instalacion SOC	9,000	-	-	-	-	-	9,000	-	-	-	-	-
Instalacion SIEM	9,000	-	-	-	-	-	9,000	-	-	-	-	-
SIEM	3,000	3,000	3,000	3,000	3,000	3,000	4,000	4,000	4,000	4,000	4,000	4,000
Instalación eBanking	-	-	-	-	-	12,000	-	-	-	-	-	-
Instalación Ingeniería Social	-	-	5,000	-	-	-	-	-	-	-	5,000	-
Coste de Ventas	43,900	25,900	34,900	29,900	29,900	50,900	61,200	43,200	43,200	43,200	52,200	47,200

	Año 3											
	Jul	Ago	Set	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun
SOC	12,000	12,000	12,000	12,000	15,000	15,000	15,000	15,000	15,000	15,000	15,000	15,000
CSIRT	1,200	1,200	1,200	1,200	1,500	1,500	1,500	1,500	1,500	1,500	1,500	1,500
eBanking Protection	18,000	18,000	18,000	18,000	18,000	18,000	18,000	18,000	18,000	27,000	27,000	27,000
Ingeniería Social	12,000	12,000	12,000	12,000	12,000	12,000	12,000	12,000	12,000	12,000	12,000	12,000
Instalacion SOC	-	-	-	-	9,000	-	-	-	-	-	-	-
Instalacion SIEM	-	-	-	-	9,000	-	-	-	-	-	-	-
SIEM	4,000	4,000	4,000	4,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000
Instalación eBanking	-	-	-	-	-	-	-	-	-	12,000	-	-
Instalación Ingeniería Social	-	-	-	-	-	-	-	-	-	-	-	-
Coste de Ventas	47,200	47,200	47,200	47,200	69,500	51,500	51,500	51,500	51,500	72,500	60,500	60,500

	Año 4											
	Jul	Ago	Set	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun
SOC	15,000	15,000	15,000	15,000	15,000	15,000	15,000	15,000	15,000	15,000	15,000	15,000
CSIRT	1,500	1,500	1,500	1,500	1,500	1,500	1,500	1,500	1,500	1,500	1,500	1,500
eBanking Protection	27,000	27,000	27,000	27,000	27,000	27,000	27,000	27,000	27,000	27,000	27,000	27,000
Ingeniería Social	12,000	12,000	12,000	12,000	12,000	12,000	12,000	12,000	12,000	12,000	12,000	12,000
Instalacion SOC	-	-	-	-	-	-	-	-	-	-	-	-
Instalacion SIEM	-	-	-	-	-	-	-	-	-	-	-	-
SIEM	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000
Instalación eBanking	-	-	-	-	-	-	-	-	-	-	-	-
Instalación Ingeniería Social	-	-	-	-	-	-	-	-	-	-	-	-
Coste de Ventas	60,500	60,500	60,500	60,500	60,500	60,500	60,500	60,500	60,500	60,500	60,500	60,500

	Año 5											
	Jul	Ago	Set	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun
SOC	15,000	15,000	15,000	15,000	15,000	15,000	15,000	15,000	15,000	15,000	15,000	15,000
CSIRT	1,500	1,500	1,500	1,500	1,500	1,500	1,500	1,500	1,500	1,500	1,500	1,500
eBanking Protection	27,000	27,000	27,000	27,000	27,000	27,000	27,000	27,000	27,000	27,000	27,000	27,000
Ingeniería Social	12,000	12,000	12,000	12,000	12,000	12,000	12,000	12,000	12,000	12,000	12,000	12,000
Instalacion SOC	-	-	-	-	-	-	-	-	-	-	-	-
Instalacion SIEM	-	-	-	-	-	-	-	-	-	-	-	-
SIEM	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000
Instalación eBanking	-	-	-	-	-	-	-	-	-	-	-	-
Instalación Ingeniería Social	-	-	-	-	-	-	-	-	-	-	-	-
Coste de Ventas	60,500	60,500	60,500	60,500	60,500	60,500	60,500	60,500	60,500	60,500	60,500	60,500

Costos Operativos

	Año 1											
	Jul	Ago	Set	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun
Gastos de Personal	2,864	3,339	2,864	2,864	2,864	2,864	3,339	2,864	2,864	2,864	2,864	2,864
- Sueldo de vendedor	463	463	463	463	463	463	463	463	463	463	463	463
- Comisión del Vendedor	278	278	278	278	278	278	278	278	278	278	278	278
- Beneficios sociales del vendedor	1,327	1,327	1,327	1,327	1,327	1,327	1,327	1,327	1,327	1,327	1,327	1,327
- Sueldo de personal operativo	796	796	796	796	796	796	796	796	796	796	796	796
- Beneficios sociales del personal operativo	1,286	1,286	1,286	1,286	1,286	1,286	1,286	1,286	1,286	1,286	1,286	1,286
Marketing	0	190	190	190	190	190	505	505	505	730	730	730
Gastos Administrativos	0	0	190	190	190	190	190	505	505	505	730	730
Total	2,864	3,529	3,244	3,244	3,244	3,244	4,034	3,874	3,874	4,099	4,324	4,324

	Año 2											
	Jul	Ago	Set	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun
Gastos de Personal	3,339	2,864	2,864	2,864	2,864	2,864	3,339	2,864	2,864	2,864	2,864	2,864
- Sueldo de vendedor	463	463	463	463	463	463	463	463	463	463	463	463
- Comisión del Vendedor	475	0	0	0	0	0	475	0	0	0	0	0
- Beneficios sociales del vendedor	278	278	278	278	278	278	278	278	278	278	278	278
- Sueldo de personal operativo	1,327	1,327	1,327	1,327	1,327	1,327	1,327	1,327	1,327	1,327	1,327	1,327
- Beneficios sociales del personal operativo	796	796	796	796	796	796	796	796	796	796	796	796
Marketing	1,286	1,286	1,286	1,286	1,286	1,286	1,286	1,286	1,286	1,286	1,286	1,286
Gastos Administrativos	860	860	985	985	985	1,210	1,380	1,380	1,380	1,380	1,505	1,505
Total	5,485	5,010	5,135	5,135	5,135	5,360	6,005	5,530	5,530	5,530	5,655	5,655

	Año 3											
	Jul	Ago	Set	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun
Gastos de Personal	2,864	2,864	2,864	2,864	3,339	2,864	2,864	2,864	2,864	2,864	2,864	2,864
- Sueldo de vendedor	463	463	463	463	463	463	463	463	463	463	463	463
- Comisión del Vendedor	0	0	0	0	475	0	0	0	0	0	0	0
- Beneficios sociales del vendedor	278	278	278	278	278	278	278	278	278	278	278	278
- Sueldo de personal operativo	1,327	1,327	1,327	1,327	1,327	1,327	1,327	1,327	1,327	1,327	1,327	1,327
- Beneficios sociales del personal operativo	796	796	796	796	796	796	796	796	796	796	796	796
Marketing	1,286	1,286	1,286	1,286	1,286	1,286	1,286	1,286	1,286	1,286	1,286	1,286
Gastos Administrativos	1,505	1,505	1,505	1,505	1,675	1,675	1,675	1,675	1,675	1,900	1,900	1,900
Total	5,655	5,655	5,655	5,655	6,300	5,825	5,825	5,825	5,825	6,050	6,050	6,050

	Año 4											
	Jul	Ago	Set	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun
Gastos de Personal	2,864	2,864	2,864	2,864	2,864	2,864	2,864	2,864	2,864	2,864	2,864	2,864
- Sueldo de vendedor	463	463	463	463	463	463	463	463	463	463	463	463
- Comisión del Vendedor	0	0	0	0	0	0	0	0	0	0	0	0
- Beneficios sociales del vendedor	278	278	278	278	278	278	278	278	278	278	278	278
- Sueldo de personal operativo	1,327	1,327	1,327	1,327	1,327	1,327	1,327	1,327	1,327	1,327	1,327	1,327
- Beneficios sociales del personal operativo	796	796	796	796	796	796	796	796	796	796	796	796
Marketing	1,286	1,286	1,286	1,286	1,286	1,286	1,286	1,286	1,286	1,286	1,286	1,286
Gastos Administrativos	1,900	1,900	1,900	1,900	1,900	1,900	1,900	1,900	1,900	1,900	1,900	1,900
Total	6,050	6,050	6,050	6,050	6,050	6,050	6,050	6,050	6,050	6,050	6,050	6,050

	Año 5											
	Jul	Ago	Set	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun
Gastos de Personal	2,864	2,864	2,864	2,864	2,864	2,864	2,864	2,864	2,864	2,864	2,864	2,864
- Sueldo de vendedor	463	463	463	463	463	463	463	463	463	463	463	463
- Comisión del Vendedor	0	0	0	0	0	0	0	0	0	0	0	0
- Beneficios sociales del vendedor	278	278	278	278	278	278	278	278	278	278	278	278
- Sueldo de personal operativo	1,327	1,327	1,327	1,327	1,327	1,327	1,327	1,327	1,327	1,327	1,327	1,327
- Beneficios sociales del personal operativo	796	796	796	796	796	796	796	796	796	796	796	796
Marketing	1,286	1,286	1,286	1,286	1,286	1,286	1,286	1,286	1,286	1,286	1,286	1,286
Gastos Administrativos	1,900	1,900	1,900	1,900	1,900	1,900	1,900	1,900	1,900	1,900	1,900	1,900
Total	6,050	6,050	6,050	6,050	6,050	6,050	6,050	6,050	6,050	6,050	6,050	6,050

Flujo de Caja Económico

	Año 1											
FLUJO DE CAJA ECONOMICO	Jul	Ago	Set	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun
Flujo Operativo												
- Ingreso Operativo	-	9,500	9,500	9,500	9,500	9,500	25,250	25,250	25,250	36,500	36,500	36,500
- Egreso Operativo	4,150	27,115	8,898	8,898	8,898	8,898	40,730	19,654	19,654	38,480	29,486	29,486
FC Operativo	-4,150	-17,615	602	602	602	602	-15,480	5,596	5,596	-1,980	7,014	7,014

	Año 2											
FLUJO DE CAJA ECONOMICO	Jul	Ago	Set	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun
Flujo Operativo												
- Ingreso Operativo	43,000	43,000	49,250	49,250	49,250	60,500	69,000	69,000	69,000	69,000	75,250	75,250
- Egreso Operativo	49,385	34,537	42,800	39,300	39,300	57,532	67,744	54,811	54,811	54,811	63,074	59,574
FC Operativo	-6,385	8,463	6,450	9,950	9,950	2,968	1,256	14,189	14,189	14,189	12,176	15,676

	Año 3											
FLUJO DE CAJA ECONOMICO	Jul	Ago	Set	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun
Flujo Operativo												
- Ingreso Operativo	75,250	75,250	75,250	75,250	83,750	83,750	83,750	83,750	83,750	95,000	95,000	95,000
- Egreso Operativo	59,574	59,574	59,574	59,574	78,185	65,253	65,253	65,253	65,253	83,485	75,085	75,085
FC Operativo	15,676	15,676	15,676	15,676	5,565	18,497	18,497	18,497	18,497	11,515	19,915	19,915

	Año 4											
FLUJO DE CAJA ECONOMICO	Jul	Ago	Set	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun
Flujo Operativo												
- Ingreso Operativo	95,000	95,000	95,000	95,000	95,000	95,000	95,000	95,000	95,000	95,000	95,000	95,000
- Egreso Operativo	75,085	75,085	75,085	75,085	75,085	75,085	75,085	75,085	75,085	75,085	75,085	75,085
FC Operativo	19,915	19,915	19,915	19,915	19,915	19,915	19,915	19,915	19,915	19,915	19,915	19,915

	Año 5											
FLUJO DE CAJA ECONOMICO	Jul	Ago	Set	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun
Flujo Operativo												
- Ingreso Operativo	95,000	95,000	95,000	95,000	95,000	95,000	95,000	95,000	95,000	95,000	95,000	95,000
- Egreso Operativo	75,085	75,085	75,085	75,085	75,085	75,085	75,085	75,085	75,085	75,085	75,085	75,085
FC Operativo	19,915	19,915	19,915	19,915	19,915	19,915	19,915	19,915	19,915	19,915	19,915	19,915

Estado de Resultados

	Año 1											
	Jul	Ago	Set	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun
Ventas	0	9,500	9,500	9,500	9,500	9,500	25,250	25,250	25,250	36,500	36,500	36,500
Costo de Ventas	0	22,300	4,300	4,300	4,300	4,300	35,600	12,600	12,600	33,600	21,600	21,600
Utilidad Bruta	0	-12,800	5,200	5,200	5,200	5,200	-10,350	12,650	12,650	2,900	14,900	14,900
Gastos de Operación	4,150	4,815	4,340	4,340	4,340	4,340	5,130	4,655	4,655	4,880	4,880	4,880
Utilidad Operativa	-4,150	-17,615	860	860	860	860	-15,480	7,995	7,995	-1,980	10,020	10,020
Impuesto a la renta (30%)	0	0	258	258	258	258	0	2,398	2,398	0	3,006	3,006
Utilidad Neta	-4,150	-17,615	602	602	602	602	-15,480	5,596	5,596	-1,980	7,014	7,014

	Año 2											
	Jul	Ago	Set	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun
Ventas	43,000	43,000	49,250	49,250	49,250	60,500	69,000	69,000	69,000	69,000	75,250	75,250
Costo de Ventas	43,900	25,900	34,900	29,900	29,900	50,900	61,200	43,200	43,200	43,200	52,200	47,200
Utilidad Bruta	-900	17,100	14,350	19,350	19,350	9,600	7,800	25,800	25,800	25,800	23,050	28,050
Gastos de Operación	5,485	5,010	5,135	5,135	5,135	5,360	6,005	5,530	5,530	5,530	5,655	5,655
Utilidad Operativa	-6,385	12,090	9,215	14,215	14,215	4,240	1,795	20,270	20,270	20,270	17,395	22,395
Impuesto a la renta (30%)	0	3,627	2,764	4,264	4,264	1,272	538	6,081	6,081	6,081	5,218	6,718
Utilidad Neta	-6,385	8,463	6,450	9,950	9,950	2,968	1,256	14,189	14,189	14,189	12,176	15,676

	Año 3											
	Jul	Ago	Set	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun
Ventas	75,250	75,250	75,250	75,250	83,750	83,750	83,750	83,750	83,750	95,000	95,000	95,000
Costo de Ventas	47,200	47,200	47,200	47,200	69,500	51,500	51,500	51,500	51,500	72,500	60,500	60,500
Utilidad Bruta	28,050	28,050	28,050	28,050	14,250	32,250	32,250	32,250	32,250	22,500	34,500	34,500
Gastos de Operación	5,655	5,655	5,655	5,655	6,300	5,825	5,825	5,825	5,825	6,050	6,050	6,050
Utilidad Operativa	22,395	22,395	22,395	22,395	7,950	26,425	26,425	26,425	26,425	16,450	28,450	28,450
Impuesto a la renta (30%)	6,718	6,718	6,718	6,718	2,385	7,927	7,927	7,927	7,927	4,935	8,535	8,535
Utilidad Neta	15,676	15,676	15,676	15,676	5,565	18,497	18,497	18,497	18,497	11,515	19,915	19,915

	Año 4											
	Jul	Ago	Set	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun
Ventas	95,000	95,000	95,000	95,000	95,000	95,000	95,000	95,000	95,000	95,000	95,000	95,000
Costo de Ventas	60,500	60,500	60,500	60,500	60,500	60,500	60,500	60,500	60,500	60,500	60,500	60,500
Utilidad Bruta	34,500	34,500	34,500	34,500	34,500	34,500	34,500	34,500	34,500	34,500	34,500	34,500
Gastos de Operación	4,150	4,150	4,150	4,150	4,150	4,150	4,150	4,150	4,150	4,150	4,150	4,150
Utilidad Operativa	28,450	28,450	28,450	28,450	28,450	28,450	28,450	28,450	28,450	28,450	28,450	28,450
Impuesto a la renta (30%)	8,535	8,535	8,535	8,535	8,535	8,535	8,535	8,535	8,535	8,535	8,535	8,535
Utilidad Neta	19,915	19,915	19,915	19,915	19,915	19,915	19,915	19,915	19,915	19,915	19,915	19,915

	Año 5											
	Jul	Ago	Set	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun
Ventas	95,000	95,000	95,000	95,000	95,000	95,000	95,000	95,000	95,000	95,000	95,000	95,000
Costo de Ventas	60,500	60,500	60,500	60,500	60,500	60,500	60,500	60,500	60,500	60,500	60,500	60,500
Utilidad Bruta	34,500	34,500	34,500	34,500	34,500	34,500	34,500	34,500	34,500	34,500	34,500	34,500
Gastos de Operación	6,050	6,050	6,050	6,050	6,050	6,050	6,050	6,050	6,050	6,050	6,050	6,050
Utilidad Operativa	28,450	28,450	28,450	28,450	28,450	28,450	28,450	28,450	28,450	28,450	28,450	28,450
Impuesto a la renta (30%)	8,535	8,535	8,535	8,535	8,535	8,535	8,535	8,535	8,535	8,535	8,535	8,535
Utilidad Neta	19,915	19,915	19,915	19,915	19,915	19,915	19,915	19,915	19,915	19,915	19,915	19,915

Cálculo de VAN

VANE	354,911

Metodología de cálculo de los Indicadores de rentabilidad:

- Margen Bruto: Utilidad Neta (año) / Venta (año)
- Margen Operativo: Utilidad Operativa (año) / Venta (año)
- Margen Neto: Utilidad Neta (año) / Venta (año)

BIBLIOGRAFIA

Accenture. (2018). Reinventing the Internet to Secure the Digital Economy.Recuperado de https://www.accenture.com/us-en/insights/cybersecurity/reinventing-the-internet-digital-economy

Anampa, Karen Lidia, Door, Christian (2018), Plan de Ventas, *Plan de Negocios para determinar la viabilidad del desarrollo de un asistente virtual de ventas (Chatbot): Caso Gamarra* (pp. 114), Lima, Perú, Universidad ESAN

Capgemini. (18 de diciembre de 2017). Las 10 principales tendencias para banca minorista: 2018. Recuperado de https://www.capgemini.com/mx-es/resources/las-10-principales-tendencias-para-banca-minorista-2018/

CIO Perú (Marzo, 2018). Fortinet presenta estudio sobre inversiones en ciberseguridad en el Perú. Recuperado de https://cioperu.pe/articulo/25366/fortinet-presenta-estudio-sobre-inversiones-en-ciberseguridad-en/

Deloitte Center for financial Services. (2018). Banking Outlook. Accelerating the transformation. Recuperado de https://www2.deloitte.com/us/en/pages/financial-services/articles/banking-industry-outlook.html

Diario El Comercio. (22 de setiembre de 2018). BCR reduce sus estimados económicos ante vientos externos menos favorables. Recuperado de https://elcomercio.pe/economia/peru/bcr-reduce-estimados-vientos-externos-favorables-noticia-560469

EY. (2018).Ciberseguridad: preparados para afrontar futuros ataques [PDF file].Recuperado de https://www.ey.com/es/es/home/ey-global-information-security-survey-2018

FMI. (enero, 2019). Actualización de Perspectivas de la Economía Mundial. Recuperado de https://www.imf.org/es/Publications/WEO/Issues/2019/01/11/weo-update-january-2019

Gavilán Rivillas, Lucía. (2017). Blogthinkbig.com. Recuperado de https://blogthinkbig.com/tendencias-en-ciberseguridad-2017

Gestión. (6 de diciembre de 2018). Mercado de ciberseguridad en Perú crecerá hasta US$ 220 millones en 2021Recuperado de https://gestion.pe/economia/mercado-ciberseguridad-peru-crecera-us-220-millones-2021-nndc-252046

Jiménez, Juan, Mezarina, Ricardo (2018), Plan de marketing, Plan de marketing estratégico y de lanzamiento para la implementación de una empresa de venta de chocolates elaborados a base de cacao orgánico (pp. 93 - 94), Lima, Perú, Universidad ESAN

Kotler, Philip, (2012), Canales de Marketing: Transferencia de valor para el cliente, Marketing (pp. 338 - 345), Nacaulpan de Juarez, México, Pearson Educación

Laudon, K, (2013), Sistemas de Seguridad y de Pagos en el comercio electrónico, *e-Commerce: Negocios, Tecnología, Sociedad* (pp. 269 - 285), Nacaulpan de Juarez, México, Pearson Educación

Lovelock, Christopher, Wirtz, Jochen(2002), Desarrollo de los productos de servicios: Elementos básicos y complementarios, *Marketing de servicios Personal, tecnología y estrategia (pp. 82 - 94)*, Distrito Federal, México, Pearson Educación

Ministerio de Comunicaciones. (2008). Diseño de un CSIRT de Colombia para la estrategia gobierno en línea [PDF file]. Recuperado de http://www.vive.gobiernoenlinea.gov.co/apc-aa-files/5854534aee4eee4102f0bd5ca294791f/3._Diseno_de_un_CSIRT_Colombiano.pdf

Nasdaq. (Junio 2018). Cybersecurity: Industry Report & Investment Case. Recuperado de https://business.nasdaq.com/marketinsite/2018/GIS/Cybersecurity-Industry-Report-Investment-Case.html

Nicole, P. (2017). Matriz Ansoff. 2019, de Economipedia Sitio web: https://economipedia.com

Osterwalder, Alexander, (2010), El lienzo de modelo de negocios, una herramienta para describir, analizar y diseñar modelos de negocios, *Business Model Generation* (pp. 14 - 41), Barcelona, España, Grupo Planeta

Reputation Institute (Marzo 2015). How do consumer view the Banking Industry Worldwide [PDF file]. Recuperado de https://www.reputationinstitute.com/sites/default/files/pdfs/How-Do-Consumers-View-The-Banking-Industry-Worldwide.pdf

Sinek, Sinek. (15 de setiembre de 2018). Wikipedia. Recuperado de https://es.wikipedia.org/wiki/Simon_Sinek

Sinek, Sinek. [The New York Times conferences]. (2018, Octubre 10). The Infinitive game. Recuperado de https://www.youtube.com/watch?v=tye525dkfi8

Stlouisfed.org (enero 2019). Federal Reserve Bank of Sr. Louis. Recuperado de https://fred.stlouisfed.org

Thierry Karsenti, vicepresidente de nueva tecnología en Europa de Check Point. (2018). La inversión en ciberseguridad se incrementa un 10%. cada año. Madrid, España :. Check Point Press Releases. Recuperado de https://www.checkpoint.com/es/press/2018/thierry-karsenti-vicepresidente-de-nueva-tecnologia-en-europa-de-check-point-la-inversion-en-ciberseguridad-se-incrementa-un-10-cada-ano/

GLOSARIO

APWG: Anti-Phishing Working Group

ASBANC: Asociación de Bancos del Perú

CCE: Cámara de Compensación Electrónica

CEFI: Centro de Estudios Financieros

CERT: Computer Emergengy Response Team

CIO: Chief Information Officers

CSIRT: Computer Security Incident Response Team

DDoS: Ataque de negación de servicio distribuido

FIRST: Forum of Incident Response and Security Teams

FMI: Fondo Monetario Internacional

IP: Internet Protocol

ISACA: Information Systems Audit and Control Association

ISO: International Organization for Standarization

KAM: Key Account Management

KPI: Key Performance Indicator

MPLS: Multiprotocol Label Switch

MSS: Managed Security Services

RepTrak: Índice de reputación

SIEM: Security Information and Event Management

SOC: Security Operation Center