

**PLAN DE NEGOCIO PARA LA CREACIÓN DE UNA EMPRESA DE SOLUCIÓN
INTEGRAL ANTIFRAUDE PARA LA SEGURIDAD DE LA INFORMACION**

NOMBRES ESTUDIANTES

Jairo Andres Pinillos Rozo

Winston Arley Gaviria Ordoñez

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO

FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS

ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACION

2016

**PLAN DE NEGOCIO PARA LA CREACIÓN DE UNA EMPRESA DE SOLUCIÓN
INTEGRAL ANTIFRAUDE PARA LA SEGURIDAD DE LA INFORMACION**

EVALUACIÓN DEL PLAN DE NEGOCIOS

NOMBRES ESTUDIANTES

Jairo Andres Pinillos Rozo

Winston Arley Gaviria Ordoñez

Asesor

Giovanny Andres Piedrahita Solorzano

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO

FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS

ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACION

2016

AGRADECIMIENTOS

Inicialmente, damos gracias a dios por permitirnos tener tan buena experiencia dentro de la Universidad, gracias al Politecnico Grancolombiano por permitirnos en especialistas en un área que tanto nos apasiona, gracias a cada maestro que hizo parte de este proceso integral de formación que deja como producto este grupo de compañeros, y como recuerdo y prueba viviente de la historia; este proyecto de grado, que perdurara dentro de los conocimientos y desarrollo de las demás generaciones que están por llegar.

Finalmente, agradecemos a quien lee este apartado y más que nuestro proyecto de grado, por permitir a nuestras experiencias, investigaciones y conocimiento, incurrir dentro del repertorio de su información mental.

TABLA DE CONTENIDO

1 RESUMEN	5
2 INTRODUCCION	6
3 JUSTIFICACION	7
4 MARCO CONCEPTUAL	8
4.1 Situación problema	8
5 OBJETIVOS	10
5.1 Objetivo general	10
5.2 Objetivos específicos	10
6 MARCO TEORICO	11
7. DESARROLLO DE PLAN DE NEGOCIO	14
7.1 Resumen Ejecutivo	14
7.2 Descripción de los servicios	14
8 ESTUDIO DE MERCADO	16
8.1 Objetivos específicos	16
8.2 Mercado Potencial	17

8.3 Estrategia de mercado	18
8.3.2 El área de mercado	19
8.3.3 Comportamiento de la demanda	19
8.3.4 Comportamiento de la oferta	20
8.4 Planeación estratégica del proyecto	21
9 ESTUDIO DE LA OPERACIÓN	22
9.1 Flujograma de proceso y procedimiento por incidente	22
9.2 Plan de trabajo	22
9.3 Identificación de actores relevantes	23
9.4 Cadenas causales	25
9.5 Análisis de la retrospectiva del problema	26
9.5.1 Escenario pesimista	26
9.5.2 Escenario Optimista	26
9.5.3 Escenario tendencial	26
9.6 Valoración de la viabilidad, gobernabilidad y pertinencia	27
9.7 Indicadores de desempeño del negocio	28
10 ESTUDIO TECNICO	30

10.1 Objetivo general	30
10.2 Objetivos específicos	30
10.3 Especificaciones de servicio	31
11 ESTUDIO ECONOMICO Y FINANCIERO	40
11. 1 Objetivos específicos	40
11.2 Estados financieros	40
11.3 Estados financieros proyectados	41
11.4 Determinación de los precios de los servicios	43
12 ASPECTOS LEGALES	
12.1 Normas de todo género pertinentes para la generación del proyecto	48
13 BIBLIOGRAFIA	

INDICE DE DIAGRAMAS, TABLAS Y GRAFICOS

Diagrama 1. Flujo de proceso ante incidente de seguridad	22
Tabla 1. Plan de trabajo	23
Diagrama 2. Actores relevantes	24
Diagrama 3. Cadenas causales	25
Tabla 2. Viabilidad, gobernabilidad y pertinencia	28
Tabla 3. Indicadores de desempeño	29
Grafica 1. Costo progresivo del ataque de Phishing	31
Diagrama 4. Mapa conceptual del funcionamiento del Phishing	32
Tabla 4. Tipos de Phishing	32
Tabla 5. Top de marcas de Phishing	33
Tabla 6. Estrategia para detectar, prevenir y mitigar ataques de Phishing	34
Tabla 7. Partes interesadas contactos desactivación de Phishing	37
Tabla 8. Precios por casos	43
Tabla 9. Costos fijos de arranque	44
Tabla 10. Gastos administrativos, operación y ventas	45
Tabla 11. Gastos de personal	46

1. RESUMEN

El objetivo del presente trabajo de grado es realizar un análisis global sobre el PLAN DE NEGOCIO PARA LA CREACIÓN DE UN NEGOCIO DE SOLUCIÓN INTEGRAL ANTIFRAUDE PARA SEGURIDAD DE LA INFORMACIÓN. La descripción de la empresa, las actividades y respectivos análisis realizados en el proyecto, se encuentran en los diferentes capítulos del documento.

La idea como oportunidad de negocio del presente proyecto de grado surgió ante la situación que se presenta actualmente, donde muchas empresas están teniendo pérdidas millonarias por falta de soluciones de seguridad para la conectividad a internet y la carencia de procesos, buenas prácticas y consultorías en temas de seguridad de la información.

Para el desarrollo del trabajo se utilizó un diseño metodológico de tipo descriptivo, mediante el análisis e investigación de fuentes bibliográficas primarias y secundarias confiables.

La investigación mostró que no existe una fuerte demanda de empresas que proporcione soluciones integrales antifraude por internet en temas de seguridad de la información por parte del mercado objetivo, quienes además muestran gran interés ante la perspectiva de creación de una empresa de soluciones de seguridad en temas de transacciones por internet que cumpla con sus requerimientos y estándares de calidad.

Durante el desarrollo del proyecto y análisis de indicadores financieros de rentabilidad y liquidez y la evaluación financiera, se concluyó que el negocio es viable y su actividad es rentable, con un

retorno total de la inversión al tercer año y generando un aporte a la economía del país en el plano social a través de la generación de empleos directos.

2. INTRODUCCIÓN

Durante los últimos años, Internet se ha convertido en un medio masivo de comunicación y de intercambio de información. Millones de personas están usando el Internet cada vez más para los negocios y para su vida social debido a la masificación de sistemas de fácil acceso a él y con precios asequibles para todos los estratos tanto del internet como de equipos para conectarse a él.

Desafortunadamente debido al desconocimiento de los riesgos asociados al uso de internet, este se ha convertido en medio para cometer acciones ilegales y criminales contra personas naturales, empresas públicas y privada. Estas acciones se realizan por lo general con ataques informáticos como los ataques de phishing, pharming, malware, man in the middle, y accesos no autorizados a la información entre otros.

Así como aparecen las amenazas y los ataques, aparecen nuevas técnicas para detectar y prevenir, estas son las técnicas anti-fraude, que podrían ser preventivas o reactivas y son ofrecidas por diferentes fabricantes a través del mundo.

Este trabajo analiza el Plan de Negocio para la creación de una organización cuya función sea proveer una solución antifraude integral en Seguridad de la Información. Se evalúa la factibilidad del proyecto, se interpreta el entorno de actividad empresarial y se analizan resultados. La idea principal de la empresa es garantizar la confianza en el uso de la información de las compañías a través de internet, proporcionando diferentes soluciones para este propósito. Estas soluciones se utilizarán como complemento y medio confiable para identificar posibles amenazas de seguridad

para las empresas. Además, los servicios propuestos permiten rastrear el origen de la amenaza utilizando un conjunto de información de ubicación.

3. JUSTIFICACION

La información es un activo con el cual absolutamente todas empresas cuentan y es valioso para las mismas por lo tanto debe ser sostenido por tecnologías de punta que le promociónen las principales características de la información: Integridad, confidencialidad y disponibilidad. Entre mayor tecnología aparece y se implementa, estas características de la información evolucionan también para mejorar la rentabilidad de las compañías y hacer más fácil la vida de muchas personas, sin embargo, así mismo aumentan los riesgos para esta información de ser robada, modificada, inaccesible, entre otros, generando principalmente pérdidas económicas a las empresas donde se materialicen estos riesgos.

El phishing sigue siendo aún el medio más común para el fraude de tarjetas de crédito y robo de identidad, los fraudes de phishing con un costo de miles de millones economía global cada año y sigue aumentando.

La idea del plan de negocio es ofrecer una manera de defenderse. El servicio antiphishing que se quiere ofrecer va a servir para ayudar a prevenir y mitigar los ataques de suplantación de identidad y el fraude en línea a través de la autenticación, el seguimiento y desmontaje rápido. Adaptar una solución a las necesidades de seguridad y los requisitos de presentación de informes. Ofrecer capacidades de detección robustos y los tiempos de desmontaje más rápidos que los documentados de la industria, para minimizar los daños causados por el phishing y el fraude en línea.

A diferencia de otros proveedores de servicios, la solución antiphishing que nosotros proponemos supervisara el canal de correo electrónico de forma proactiva para la actividad

fraudulenta. La autenticación de correo electrónico es un arma importante en la lucha contra los delincuentes y puede reducir su exposición a los ataques de phishing.

4. MARCO CONCEPTUAL

4.1 SITUACION PROBLEMA

En recientes encuestas realizadas por la marca número uno de seguridad en internet APWG (<http://www.antiphishing.org/>) reporto que cerca del 55% de los ataques realizados en internet se trataban de ataques con el fin de sustraer información confidencial de las personas y organizaciones.

“Los ataques a la seguridad de la información están ahora focalizados en negocios de todos los tamaños y ha crecido exponencialmente como la forma de crimen preferido actuales por los atacantes” **(Cifras oficiales fue tomada y adaptada al texto publicado en <http://www.antiphishing.org/>)**

“En un reciente estudio realizado por RSA (<http://www.emc.com/domains/rsa/index.htm>), estimaron que el costo económico global causados por fraudes por internet se incrementó en un 22% entre el 2012 y 2016 a 1.5 billones de dólares. El problema de los robos de la información ahora tan grande que todas las compañías afectadas por este tipo de amenazas han comenzado a realizar millonarias inversiones para bajar los índices de pérdidas”. **(Cifras oficiales fue tomada y adaptada al texto publicado en <http://www.emc.com/domains/rsa/index.htm>)**

A través de diferentes herramientas de seguridad basadas en la nube se busca que las empresas cliente estén protegidas ante la mayor cantidad de ataques posibles cuando los usuarios intenten

por ejemplo conectarse a internet, las herramientas tendrán la capacidad de detectar que el sitio al que se está ingresando es un sitio válido y que no contiene amenazas que puedan infectar los equipos que navegan a internet. Adicional a lo anterior, las herramientas utilizadas están destinadas a detectar y detener ataques avanzados en las redes que utilizan las brechas de seguridad para robar información y sacarla de las redes de los clientes. Las herramientas instaladas tendrán la capacidad de detectar de forma temprana las amenazas, y buscará automatizar la detección de sitios fraudulentos en un 200% por encima de la competencia. Una detección temprana es esencial para mantener estos sitios fraudulentos activos en periodos de tiempo cortos, para evitar otras personas ingresen a estos sitios y pierdan su información. Este servicio estará acompañado de auditorías continuas a los administradores de las herramientas de seguridad, para evaluar los avances en la implementación del proyecto en cuanto a procedimientos, evaluación y acciones tomadas frente a las amenazas detectadas. Nuestro producto contará con un portal de administración en la nube, que incluye servicios como vigilancia de dominios, información de feeds de terceros, navegación segura, monitoreo de los sitios web protegidos, protección de su sitio web de daños, vulnerabilidades y ataques, en conjunto con el monitoreo de menciones de la marca en foros, blogs y redes sociales, haciendo de la oportunidad de negocio el servicio de mitigación de ataques de seguridad el más poderoso del mercado.

Con base a lo anterior se identifica claramente una OPORTUNIDAD de negocio promisoría que se estudiará, demostrando su viabilidad a lo largo del desarrollo de este trabajo. La oportunidad de negocio proporcionara protección integral proactiva contra ataques de seguridad, brindando detección temprana y servicios integrales, todo manejado desde un portal innovador basado en la

nube. Usando vigilancia de dominios, información de feeds de terceros y navegación segura para encontrar evidencia de nuevos ataques. La oportunidad de negocio también monitoreara tácticamente el sitio web protegido de un cliente, desactivando rápidamente los ataques en un tiempo mucho menor que el promedio de la industria, incluso antes de que puedan ser lanzados. Las características extendidas de la empresa incluirán proteger su sitio web de daños, vulnerabilidades y ataques, en conjunto con el monitoreo de menciones de la marca en foros, blogs y redes sociales, haciendo de la oportunidad de negocio el servicio de mitigación de ataques de seguridad el más poderoso del mercado.

Este servicio en tiempo real evalúa la solicitud de la URLs y las almacena instantáneamente, analiza su contenido de la página, la reputación de la información del dominio y entre otros factores. Determinará la información determinante de cada URL para así determinar la legitimidad de los sitios. Continuamente incrementará la exactitud de las determinaciones que tiene como retroalimentación que agrega la evaluación de personal humano dentro del modelo de automático.

Los ataques por internet reflejan lo fácil que es crear un ‘clon’ de un sitio legítimo, ofuscar la URL y re direccionar el tráfico a sitios web falsificados. Estos engañan a los usuarios para robar información sensible, dar clic en un link que activa un exploit, o simplemente usa vulnerabilidades en el navegador o aplicación para instalar un malware. Al final resulta como una brecha en la seguridad que robara al negocio información sensible como credenciales financieras para robar dinero online. La oportunidad de negocio proveerá una nueva y proactiva

forma para que esta muy real y significativa forma de amenaza que tiende a crecer significativamente en los años próximos no genere un impacto negativo en las compañías.

5. OBJETIVOS

5.1 OBJETIVO GENERAL

Convertimos en el principal proveedor de seguridad que se centre en la detección integral y prevención del fraude electrónico para todos los dispositivos, sistemas operativos, los canales en la nube a través de una solución que asegure la autenticación de múltiples factores y detección de anomalías, que ofrece una ventana única para múltiples servicios de prevención del fraude.

5.2 OBJETIVOS ESPECÍFICOS

- Innovar en el ámbito tecnológico de Colombia
- Desarrollar servicio Antifraude fácil y seguro
- Concientizar a los usuarios que ellos deben ayudar a proteger su identidad.
- Realizar estudio de mercado concienzudo con el fin de establecer la demanda, la oferta, los precios y así de esta manera tener claro los parámetros que puedan generar valor en la prestación del servicio anti-fraude.
- Tener cifras exactas del mercado potencial para la utilización de los servicios antifraude.
- Verificar los aspectos técnicos realización con servicio y la implementación de los mismos y que está alineado con ser servicio que se quiere ofrecer.
- Implementar políticas, procedimientos y referentes para gestión de los servicios para que sean coherentes para la creación de la empresa.
- Establecer el valor exacto necesario para la inversión, los ingresos previos en los primeros años, costos de arranque, así como los egresos.

- Analizar financieramente el plan de negocio determinar la rentabilidad y ver si es rentable ejecutarlo.
- Establecer un plan Responsabilidad Social empresarial que este alineado con el compromiso corporativo que actualmente está en auge en las industrias.

6. MARCO TEORICO

PHISHING

Un ataque de suplantación de identidad que se produce cuando un usuario recibe un correo electrónico fraudulento o " falso " que representa una fuente de confianza (por ejemplo, banco, tienda o tarjeta de crédito de la compañía). Esta dirección de correo les lleva a un sitio Web fraudulento que recoge datos personales, la información de cuenta, contraseñas y números PIN.

Man-in - the-middle (MITM)

Un tipo sofisticado de suplantación de identidad, man-in - the-middle se producen ataques cuando un atacante logra interceptar las comunicaciones entre dos partes, como un cliente y una entidad financiera, sin su conocimiento.

Al hacer esto, el atacante se convierte en " el hombre en el medio. " Ambas partes no son conscientes de la presencia del atacante. Por lo tanto, actúa como un proxy, el atacante puede a la vez capturar y manipular el contenido de los mensajes que están re-transmitiendo entre las dos partes.

MALWARE

“El malware (del inglés “malicious software”), también llamado badware, código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo

infiltrarse y comprometer una computadora o sistema de información sin el consentimiento de su propietario. El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto.¹ El término virus informático suele aplicarse de forma incorrecta para referirse a todos los tipos de malware, incluidos los virus verdaderos”. (Tomado textual de <https://es.wikipedia.org/wiki/Malware>)

“El software se considera malware en función de los efectos que provoque en un computador. El término malware incluye virus, gusanos, troyanos, la mayor parte de los rootkits, scareware, spyware, adware intrusivo, crimeware y otros softwares maliciosos e indeseable”. (Tomado textual de <https://prezi.com/vm8o2doqllaw/copy-of-spyware-malware/>)

- “Adware (contracción de ADvertisement -anuncio -y softWARE) es un programa malicioso, que se instala en la computadora sin que el usuario lo note, cuya función es descargar y/o mostrar anuncios publicitarios en la pantalla de la víctima” (Tomado textual de <http://intercambiosos.org/showthread.php?t=15470>)

- “Botnets Un malware del tipo bot es aquel que está diseñado para armar botnets. Constituyen una de las principales amenazas en la actualidad. Este tipo, apareció de forma masiva a partir del año 2004, aumentando año a año sus tasas de aparición”. (Tomado textual de <http://www.taringa.net/posts/info/5078414/Amenazas-informaticas.html>)

- ‘‘Gusanos En términos informáticos, los gusanos son en realidad un sub-conjunto de malware. Su principal diferencia con los virus radica en que no necesitan de un archivo anfitrión para seguir vivos. Los gusanos pueden reproducirse utilizando diferentes medios de comunicación como las redes locales o el correo electrónico. El archivo malicioso puede, por ejemplo, copiarse de una carpeta a otra o enviarse a toda la lista de contactos del correo electrónico’’. **(Tomado textual de <http://intercambiosos.org/showthread.php?t=15470>)**
- ‘‘Hoax (en español: bulo) es un correo electrónico distribuido en formato de cadena, cuyo objetivo es hacer creer a los lectores, que algo falso es real. A diferencia de otras amenazas, como el phishing o el scam; los hoax no poseen fines lucrativos, por lo menos como fin principal. Los contenidos de este tipo de correos son extremadamente variables. Entre otros, podemos encontrar alertas falsas sobre virus y otras amenazas, historias solidarias sobre gente con extrañas enfermedades, leyendas urbanas o secretos para hacerse millonario’’. **(Tomado textual de <http://intercambiosos.org/showthread.php?t=15470>)**
- ‘‘Payload es una función adicional que posee cierta amenaza en particular. La traducción exacta del inglés, es más precisa respecto a su definición: "carga útil". Refiere a acciones adicionales, incluidas en virus, gusanos o troyanos; como por ejemplo robo de datos, eliminación de archivos, sobre-escritura del disco, reemplazo del BIOS’’. **(Tomado textual de <http://docplayer.es/8952480-Unidad-2-delitos-informaticos-y-seguridad-de-la-informacion.html>)**

- “Ransomware es una de las amenazas informáticas más similares a un ataque sin medios tecnológicos: el secuestro. En su aplicación informatizada, el ransomware es un código malicioso que cifra la información del ordenador e ingresa en él una serie de instrucciones para que el usuario pueda recuperar sus archivos. La víctima, para obtener la contraseña que libera la información, debe pagar al atacante una suma de dinero, según las instrucciones que éste disponga”. (Tomado textual de <http://www.taringa.net/posts/info/6634659/Tenes-virus-informate-Malwares.html>)

- Rogue es un software que, simulando ser una aplicación anti-malware (o de seguridad), realiza justamente los efectos contrarios a estas: instalar malware. Por lo general, son ataques que muestran en la pantalla del usuario advertencias llamativas respecto a la existencia de infecciones en el equipo del usuario. (Tomado textual de <http://intercambiosos.org/showthread.php?t=15470>)

- “Rootkit es una o más herramientas diseñadas para mantener en forma encubierta el control de una computadora. Estas pueden ser programas, archivos, procesos, puertos y cualquier componente lógico que permita al atacante mantener el acceso y el control del sistema. El rootkit no es un software maligno en sí mismo, sino que permite ocultar las acciones malignas que se desarrollen en el ordenador, tanto a través de un atacante como así también ocultando otros códigos maliciosos que estén trabajando en el sistema, como gusanos o troyanos”. (Tomado textual de <http://intercambiosos.org/showthread.php?t=15470>)

- “Spyware o (programas espías) son aplicaciones que recopilan información del usuario, sin el consentimiento de este. El uso más común de estos aplicativos es la obtención de información respecto a los accesos del usuario a Internet y el posterior envío de la información recabada a entes externos”. (Tomado textual de

<http://intercambiosos.org/showthread.php?t=15470>)

- “Trojanos El nombre de esta amenaza proviene de la leyenda del caballo de Troya, ya que el objetivo es el de engañar al usuario. Son archivos que simulan ser normales e indefensos, como pueden ser juegos o programas, de forma tal de "tentar" al usuario a ejecutar el archivo. De esta forma, logran instalarse en los sistemas. Una vez ejecutados, parecen realizar tareas inofensivas, pero paralelamente realizan otras tareas ocultas en el ordenador. Al igual que los gusanos, no siempre son malignos o dañinos. Sin embargo, a diferencia de los gusanos y los virus, estos no pueden replicarse por sí mismos”. (Tomado textual de

<http://intercambiosos.org/showthread.php?t=15470>)

- “Virus Un virus es un programa informático creado para producir algún daño en el ordenador y que posee, además, dos características particulares: pretende actuar de forma transparente al usuario y tiene la capacidad de reproducirse a sí mismo. Todas las cualidades mencionadas pueden compararse con los virus biológicos, que producen enfermedades (y un daño) en las personas, actúan por sí solos y se reproducen (contagian). Como cualquier virus, los virus informáticos necesitan de un anfitrión o huésped donde alojarse, y este puede ser muy variable: un archivo ejecutable, el sector de arranque o incluso la memoria del ordenador”.

(Tomado textual de **<http://intercambiosos.org/showthread.php?t=15470>)**

PHARMING

Pharming es la explotación de una vulnerabilidad en el software de los servidores DNS (Domain Name System) o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio (domain name) a otra máquina distinta''. **(Tomado textual de <http://jacob04b.blogspot.com.co/2013/12/17-cuestiones-sobre-seguridad.html>)**

De esta forma, un usuario que introduzca un determinado nombre de dominio que haya sido redirigido, accederá en su explorador de internet a la página web que el atacante haya especificado para ese nombre de dominio.

7. DESARROLLO DEL PLAN DE NEGOCIO

7.1 RESUMEN EJECUTIVO

El plan de negocio tiene como finalidad creación de una empresa que tenga como rubro de negocio implementación de dos servicios específicos los cuales son un servicio antiphishing y otro de análisis de malware, que busca ser ofrecido a todas aquellas empresas que usas portales por internet para realizar transacciones y que quieren asegurar a sus usuarios para así de esta manera hacerlo de forma segura.

Está enfocado para que este alineado con la ISO 27001 o cualquier otro modelo de gestión de seguridad de la información (SGSI), en empresas pequeñas, medianas o grandes que tengan infraestructuras servicios de pagos y transacciones por internet y en los que se pueda ver expuesta la seguridad de estos datos de alguna manera.

El grosor del servicio va a estar basado en dos grandes servicios de última tecnología.

Prestar servicio de detección y desactivación de sitios de Phishing, Pharming, Man in the middle MITM, entre otros, mediante la detección temprana y que este alineado con las mejores prácticas establecidas por la ISO / IEC 27001 – 27002.

Análisis de muestras de malware que le estén siendo enviadas a los usuarios de las entidades contratantes para así de esta manera encontrar el comportamiento específico de la muestra y generar el respectivo informe de las conclusiones generadas en el diagnóstico.

Estas buenas practicas estarán alineadas con las especificaciones y requerimientos generados en la circular 042, y por lo tanto también contara con un servicio de acompañamiento para certificar servicio antifraude cibernético ante la Superintendencia Financiera de Colombia.

7.2 DESCRIPCION DE LOS SERVICIOS

Protección del nombre de la empresa contratante a través de la inteligencia en el reconocimiento de amenazas de fraude para la detección proactiva de ataques y desactivación de los mismos.

Protección Anti-phishing, pharming y protección contra programas maliciosos que pueden ser propagados a través de internet. Proteger a sus clientes y reducir las pérdidas números tarjeta de crédito fraude o credenciales bancarias después de realizar transacciones por internet.

Aumentar la detección de amenazas y desactivación ataques para reducir el número de tiempo que un ataque puede estar online y controlar las pérdidas por fraude al cambiar los incentivos para el atacante.

Proteger a la población de usuarios finales para que para ellos sea completamente transparente.

Proteger la marca de la empresa contratante con estricta observancia y liderar en la industria con tiempos de desactivación de 3,6 horas.

Integrar de forma transparente la detección de malware en las páginas web críticas para proteger

los clientes contra ataques de Man in the Middle y ataques de inyección web. Utilizar la inteligencia fraude para detectar y analizar al malware en tiempo real.

Integrar la navegación con una solución inteligente de análisis de malware, pero es aún más valioso como una fuente de datos ayudando a acabar con los ataques en su origen. Este enfoque integrado de prevención del fraude es único en la industria.

8. ESTUDIO DE MERCADO

8.1 OBJETIVOS ESPECIFICOS

- Generar ventas de los servicios en el primer año de \$300.000.000.
- Alcanzar un volumen del 3500 caso desactivado de phishing, pharming, malware en el primer año, intentando alcanzar 27 proyectos.
- Posicionar inicialmente a nivel nacional la marca para que así al final del primer año haber tenido un alcance del 10%.
- Crear relaciones de empatía con los clientes para lograr la fidelización de los mismos.
- Idealizar el sentido de pertenencia de la imagen corporativa para Implementar y mantener la Organización.
- Implementar un plan de mejoramiento continuo para tener altos estándares de expectativas de los clientes en cuanto a servicio entregado y acompañamiento post-venta.
- Crear un plan de incentivos para fidelizar los clientes, enfocado en el mejoramiento de manera continua los niveles de satisfacción del servicio.

El plan de negocio está dirigido a un cliente corporativo, entre los que se encuentran bancos o cualquier entidad que realiza transacciones online y que busque asegurar que sus clientes no sean estafados.

Puede ser alineado de acuerdo a las necesidades de la empresa. El aseguramiento de la calidad.

Está dirigido a corporaciones o empresas de todos tamaños. Los clientes potenciales incluyen

aquellos negocios o en vías de desarrollo para apoyar el aseguramiento de los sistemas de información y apoyar las necesidades específicas del negocio que basan su información a través de transacciones por internet.

Los servicios de seguridad de la información del plan de negocios serán de interés para las empresas que reconocen los riesgos de seguridad en las transacciones online asociado a los activos de información y la necesidad de desarrollar políticas con respecto a la seguridad de sus datos y sistemas.

Los servicios están enfocados al siguiente target de usuarios:

- Empresas que experimentan perdidas inesperadas en sus sistemas de información.
- Empresas que no estén satisfechos con el nivel de calidad integrado en su portal transaccional,
- Empresas que encuentran un nivel de costo inaceptable en pérdidas por fraudes por internet.
- Empresas que necesitan personal capacitado para mejorar sus procesos de seguridad online.

8.1 ANALISIS DE LA COMPETENCIA

Los bancos o empresas de transacciones en línea por lo general tienen departamentos de control de transacciones existentes. Su fiabilidad, a veces ven afectada como resultado de la formación inadecuada del personal, no válida o adecuada documentación procesos y procedimientos y políticas internas. Muchas veces el impulso para la garantía de la calidad de estos departamentos es "pasar" la responsabilidad de

estas transacciones online directamente al usuario. Esto usualmente resulta en transacciones fraudulentas y pérdida de información y dinero para la empresa y el cliente.

La insatisfacción del cliente debido a esta falta de atención a la calidad puede generar en pérdida de usuarios y baja en los ingresos.

El plan de negocio busca soluciones de seguridad para las transacciones online incluida la formación del personal en técnicas de aseguramiento aprobadas, desarrollo de nuevas amenazas y las limitaciones específicas del negocio.

La seguridad informática y de recuperación de desastres se están convirtiendo rápidamente como importantes partes de la imagen los sistemas de información. Como tales, varias grandes empresas especializadas en estas disciplinas están en el negocio. Tres de estas firmas están enfocadas en las soluciones de servicios de fraude online, threat SMART, Odyssey Technologies Limited e CSC Digital Brand Services. Todos tienen oficinas en las áreas metropolitana de Los Estados Unidos, pero no hay una sola empresa en Colombia que este enfocada en este tipo de soluciones antifraude lo que abre una gran brecha en el mercado colombiano.

En general, estas empresa proporcionan un conjunto de herramientas estandarizadas, equipos y servicios para abordar

su la desactivación de este tipo de ataques. Sus precios por hora y la calidad son altos.

El plan de negocio reconoce la importancia de la prevención de fraudes online para los más para la pequeña red de empresas de Colombia, así como las empresas más grandes en. Como tal, el plan de negocio busca competir con las empresas establecidas por ser capaz de cumplir con el

las necesidades de la empresa cliente de una manera más económica. Su principio será una menor tarifa por hora que las empresas más grandes, mientras que proporciona un nivel comparable de servicios de calidad.

8.2 MERCADO POTENCIAL

El plan de negocio identifica la zona geográfica del territorio colombiano como mercado principal. Esta área incluye todos los departamentos, incluyendo el Amazonas y la Guajira. Esto se designa como zona de servicio principal para el plan de negocio, aunque no hay razones para limitar sus servicios a esta zona.

Los clientes potenciales pueden ser identificados como los que:

- Desean la automatización de las funciones de negocio el aseguramiento de sus transacciones.
- Modificar las soluciones adquiridas para sistema de transacciones
- Modificar las soluciones existentes para satisfacer las necesidades cambiantes.
- Empresas cuyos procesos de negocio depende de sistemas online de transacciones.
- Empresas que tienen un considerable patrimonio invertido en sus sistemas de información e información privilegiada.

8.3 ESTRATEGIAS DE MERCADO

La estrategia del Plan de negocios ha sido diseñada especialmente para proporcionar diversos niveles de protección y mecanismos de seguridad para ayudar a los bancos, instituciones

financieras y otras entidades supervisadas por la Superintendencia Financiera de Colombia a cumplir con los requerimientos de seguridad y calidad estipulados por la Circular Externa 042 y demás normas a nivel nacional e internacional.

La oportunidad de negocio buscara cubrir todos los canales transaccionales electrónicos que permitirán combatir proactivamente amenazas como ataques de phishing, pharming, malware, Man-in-middle y Man-in-the-Browser. También ofrecerá soluciones que proveen autenticación por múltiples factores, detección de transacciones anómalas y navegación segura, al igual que servicios que protegen información valiosa en la nube y detectan y reparan las vulnerabilidades existentes en redes y aplicaciones web.

Ubicación

El plan de negocio será un negocio en el que se llevarán a cabo servicios de solución antifraude online en la página web del cliente, utilizando sus equipos propios e instalaciones locativas

La contabilidad, teneduría de libros, marketing y otras funciones se llevarán a cabo en las sedes locativas.

Precio / Calidad

Los servicios solución antifraude será de un servicio de alta calidad con precios más bajos que los competidores, en un principio. Esto es para facilitar irrumpir en este nicho de mercado y establecer la credibilidad. A medida que aumenta los contratos comerciales, las tarifas aplicadas serán incrementadas en consecuencia.

Estrategias promocionales

La imagen de plan de negocio se proyecta a través del desarrollo y diseño de una imagen profesional que aparecerá en la página web de Internet, el uso constante de un atractivo y logotipo único (a diseñarse) en tarjetas de visita, membretes, facturas y correos directos.

Relaciones públicas

Puesto que el negocio servirá a la industria de servicios de sistemas de información, no existe un plan hasta el momento para la utilización de una estrategia promocional durante el primer año de negocio. Esta estrategia promocional será reevaluada en los primeros años de negocio.

Publicidad

La estrategia publicitaria primaria del plan de negocio se basará en un fácil acceso, apareciendo profesionalmente en sitios web en Internet que proporcionen una descripción de los servicios ofrecidos, consejos para la utilización de los servicios y la capacidad potencial del cliente para solicitar información sobre los servicios por correo electrónico.

8.3.2 EL AREA DEL MERCADO

Con un amplio portafolio de productos y servicios, la oportunidad de negocio ayudará a las empresas que lo requieran, en alcanzar los niveles de Seguridad de la Información que exige su negocio, basándonos en los principales estándares y mejores prácticas internacionales.

Dispondrá de un staff de ingenieros certificados, que lo apoyarán desde las fases de implementación y asesoría hasta el soporte post-implementación en un formato 7x24x365 y el más alto nivel de calidad.

8.3.3 COMPORTAMIENTO DE LA DEMANDA

La necesidad de dominar en la lucha contra el Phishing y otras amenazas a la seguridad está llevando a empresas de todos los tamaños a buscar soluciones que integren varias funciones de seguridad en una única compañía de gestión.

El uso de Fraudes Cibernéticos y de técnicas de ingeniería social para extraer detalles de cuentas confidenciales de los clientes que tienen los bancos alrededor del mundo asciende a más de \$4.5 millones de dólares durante el último año. Esto es una pequeña fracción de los 402.4 millones de dólares perdidos en los fraudes con tarjetas de crédito que se dieron en el 2012, pero los bancos hoy en día dan un paso adelante, esforzándose para ayudar a proteger a sus clientes de las estafas en línea y amenazas probando nuevos servicios antiphishing que se encuentra en el mercado.

El primer caso visto de Phishing fue en el Reino Unido fue hace aproximadamente unos cinco años atrás, los correos phishing están comenzando en forma acelerada a ser más sofisticados, dirigiendo a los usuarios a sitios falsos los cuales reproducen fielmente el look and feel de sitios legítimos.

Sandra Quinn de Asobancaria mencionó que ha habido 3000 personas en el Colombia que han sido víctimas de un fraude de banca electrónica a través de ataques de phishing y de Troyanos, o de ambos desde en el año pasado. Comparado con los 14 millones de personas quienes usan el banco en línea, esas 3000 víctimas es un porcentaje bajo para las tarjetas de crédito perdidas, las cuales tienen un impacto en una tercera parte de la gente, mientras que en otro caso a la industria le cuesta más de 400 millones de dólares al año, mencionó.

El uso de sistemas de contraseña que se utilizan una sola vez en los bancos pueden ser generados de sistemas de autenticación biométrico, pero la tecnología de los bancos colombianos, no soluciona a la necesidad inmediata de tener una tecnología anti-fraude.

8.3.4 COMPORTAMIENTO DE LA OFERTA

En la actualidad múltiples compañías ofrecen el servicio antifraude, pero entre las más grandes de las más destacadas en el mercado se encuentran las que nombramos a continuación:

MarkMonitor AntiFraud

“MarkMonitor AntiFraud es la solución más completa para proteger la reputación de una empresa y sus clientes contra los ataques de phishing y malware. Aprovechando la red más extensa de alianzas de la industria, MarkMonitor AntiFraud hace hincapié en la mitigación de la prevención y las pérdidas mientras que detecta, controlan y responde rápidamente a los ataques que encuentra. Las empresas utilizan esta poderosa solución para preservar el valor de la marca y

la confianza de los clientes y reducir al mínimo los costes potencialmente fuertes y las pérdidas asociadas con los ataques”. (Texto tomado y adaptado de

<https://www.markmonitor.es/services/antifraud.php>)

Servicio antiphishing en tiempo real de Webroot

“El nuevo servicio antiphishing en tiempo real de Webroot utiliza la nueva tecnología exclusiva de Webroot, basada en el poder analítico masivo de la Webroot Intelligence Network, para proteger a los usuarios empresariales de Internet al asegurar que siempre, y únicamente, se conecten al sitio web con que el que deseen interactuar”.(Texto tomado y adaptado de

<http://www.webroot.com/es/es/>)

8.4 POSIBILIDADES DEL PROYECTO

Las actividades en línea de 32 millones de clientes de más de 120 compañías líderes en servicios financieros, firmas de seguridad, comerciantes, aerolíneas y otras entidades en Latinoamérica y Estados Unidos podrían ser protegidas por los sistemas de prevención de fraude del Plan de Negocios, esto es atractivo para las compañías que quieren una sola compra para la mayoría de los servicios de prevención relacionados con fraude y crea un target de posibles clientes bastante amplio para el proyecto.

9. ESTUDIO DE LA OPERACION

9.1 FLUJOGRAMAS DE PROCESO Y PROCEDIMIENTO POR INCIDENTE

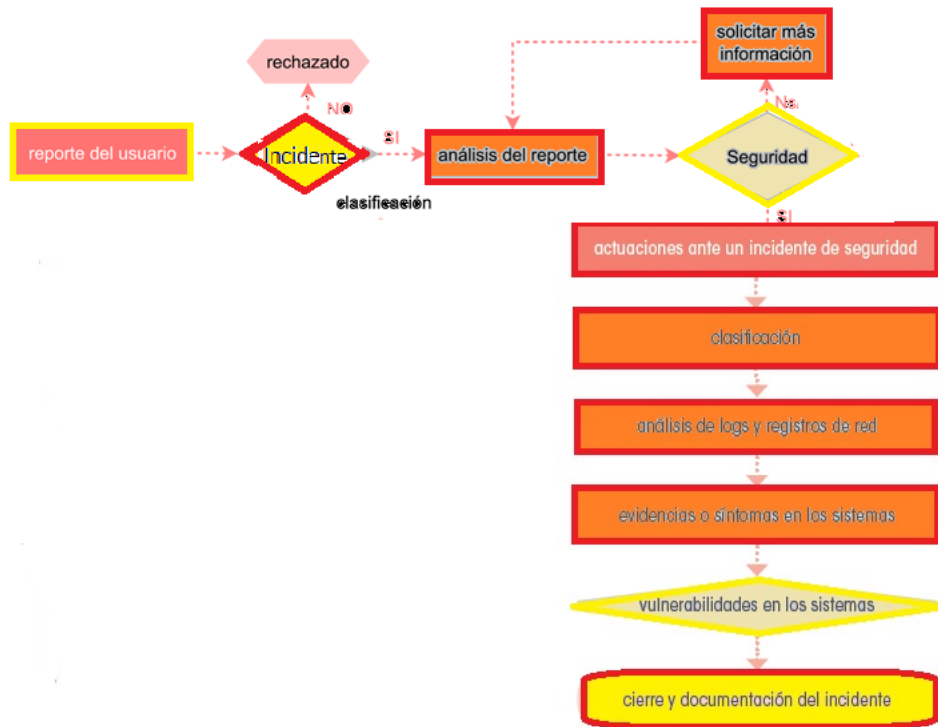


Diagrama1. Flujo de proceso ante un incidente de seguridad.

9.2 PLAN DE TRABAJO

ETAPA	ACTIVIDAD	RESULTADO	TIEMPO
Investigación	Analizar la seguridad de los portales web de	Documento de investigación te	120 horas

	las entidades contratantes.	tendencia de fraude en la actualidad	
Planeacion	Analizar de vulnerabilidades o faltas de seguridad con ataques cibernéticos actuales.	Documento con tipos de ataques actuales.	60 horas
	Crear indicadores de tiempo de respuesta	Documento con indicadores de acuerdo de respuesta del servicio.	60 horas
Desarrollo	Asegurar de servicios, bases de datos y elementos de comunicación;	Crear portal de creación de ticket y comunicación con usuarios del servicio.	40 horas
	Crear los diferentes productos antifraude que se comercializan	Ficha técnica de los diferentes productos.	80 horas
Implementacion	Crear manual de implementación de los diferentes productos	Manual de uso de los diferentes productos.	200 horas
Seguimiento	Realizar seguimiento a la satisfacción del	Documento encuesta de satisfaccion	40 horas

	cliente frente a los diferentes servicios		
--	--	--	--

Tabla1. Plan de trabajo

9.3 IDENTIFICACION DE ACTORES RELEVANTES

Mientras que las empresas más grandes son los objetivos principales de estos tipos de ataques, hemos aprendido que cualquier negocio es un objetivo potencial. Los colegios, universidades, compañías de seguros, bancos, gobiernos, e incluso los proveedores de seguridad en línea son víctimas de los atacantes. También sabemos que los ataques de continúan aumentando, y que las líneas de ataque de frecuentemente utilizan para distribuir sus ataques es el correo electrónico.

Teniendo esto en cuenta hemos encontrado los siguientes actores relevantes:

Oportunidad de Negocio, solución antifraude integral: Empresa que se dedicada a la detección y desactivación de fraudes en internet.

Usuarios que haces transacciones por internet: Personas naturales que hacen uso diario de los portales en internet para realizar transacciones como consultar, pagos entre otros.

Entidades Bancarias: Empresas que ofrecen sus servicios de ahorro e inversión que necesitan asegurar sus transacciones para que estos recursos no sean robados.

Tiendas de compras Online: Empresas que venden bienes y servicios a través de internet.

Redes sociales: Sitios web encargados de reunir un grupo de personas con los mismos intereses para compartir opiniones.

Servicio de correo electrónico Empresarial: Servicio de intercambio de mensajes e información en las diferentes compañías.

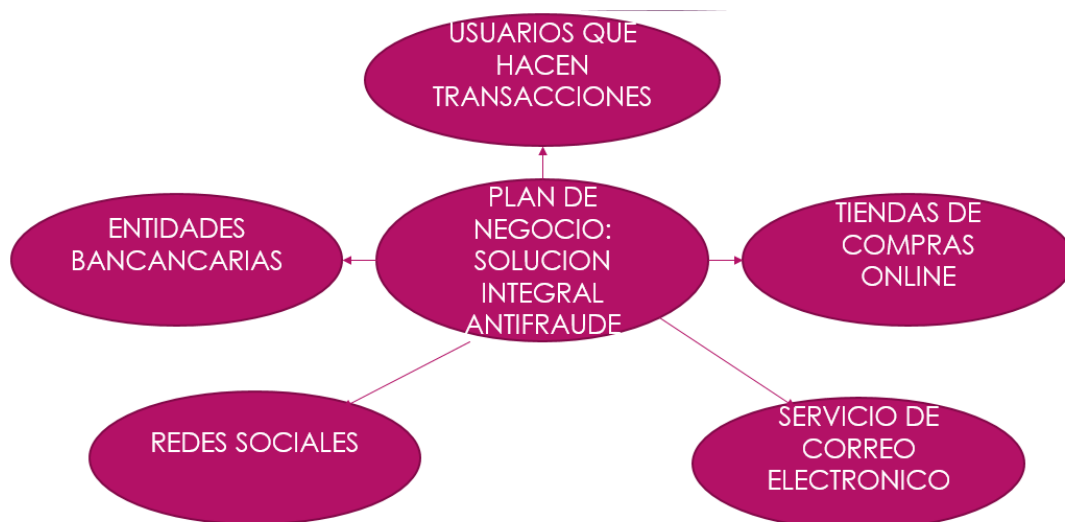


Diagrama 2. Actores relevantes

9.4 CADENAS CAUSALES

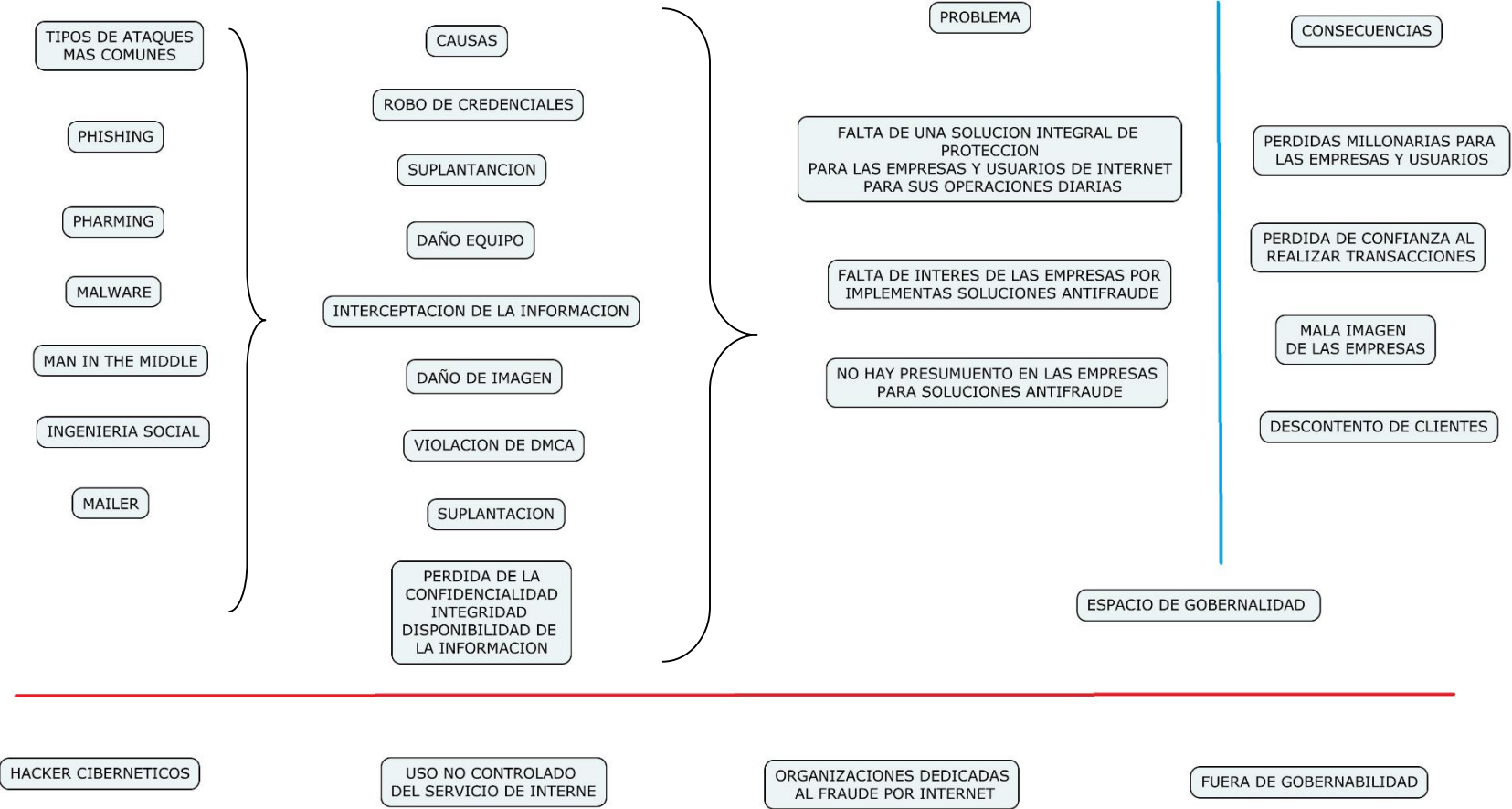


Diagrama 3. Cadenas causales

9.5 ANALISIS DE LA PROSPECTIVA DEL PROBLEMA

9.5.1 ESCENARIO OPTIMISTA

Debido a la explosión en el crecimiento del uso de Internet y a los avances en la tecnología, es muy común para las personas y para las organizaciones el uso del servicio de Home Banking o Banca Electrónica brindado por la mayoría de los Bancos.

El uso e implementación de este tipo de servicios ha sido ampliamente aceptado ya que se pueden realizar diferentes operaciones tales como consulta de saldos, pago de servicios, transferencias entre cuentas propias y de terceros, compra y venta de moneda extranjera, etc.

Pero este servicio no se encuentra ajeno a los riesgos propios que implica operar en una red de comunicación abierta como es Internet, esto trae consigo la gran viabilidad que tiene la implementación de un servicio antifraude que le prevenga las instituciones que lo han incorporado, una solución preventiva a este tipo de ataques para así evitar que se concrete un fraude.

9.5.2 ESCENARIO TENDENCIAL

Como se afirma a menudo, el tiempo es dinero, y esto es cierto sobre todo cuando se trata de fraude en línea. No es ningún secreto que cuanto más tiempo un ataque de cibernético se mantiene vivo, las mayores pérdidas se acumulan, a menudo de manera exponencial. Por lo tanto, es imperativo para el negocio identificar rápidamente y eliminar estas amenazas.

Como los ataques en internet se vuelven más sofisticados, nunca ha sido más importante emplear soluciones que han demostrado un historial de prevención del fraude. La necesidad de un producto antifraude crece año tras año. Detectar y eliminar los ataques en los principales índices de la industria, ahorra tiempo a las empresas, pero lo más importante es el dinero.

9.6 VALORACION DE VIABILIDAD, GOBERNABILIDAD Y PERTINENCIA

Acción(VARIABLES de Prospectiva)		Valoración de Gobernabilidad		Valoración de Impacto		Valoración de Pertenencia
Determinación de los precios de los productos	3	La política de precios que se maneja en el plan de negocios está organizada por la cantidad de tickets de desactivación que la entidad adquiere y con relación a esto, se le asigna una categoría un precio de valor unidad	3	Al manejar sistema de tickets se tiene mayor control sobre el precio del mercado además de más control en los costos de operación por ticket.	3	Para realizar el cálculo de Valor del Servicio se tendrán en cuenta los siguientes tres factores para encontrar el punto de equilibrio: -Costes fijos de la empresa -Costes variables por unidad de producto -Precio de venta del producto

Tamaño físico del proyecto	2	El proyecto estará domiciliado en Colombia por costos de Mano de obra	2	En Colombia la mano de obra es más barata que si se ubicara en otro país como Estados Unidos	2	El tamaño de las oficinas que alojará a los empleos estará definido por la cantidad de personas que inicialmente tendrá la puesta en marcha del proyecto.
Creación de procesos y procedimientos internos	2	El gerente de operaciones será el encargado de implementar los procedimientos internos para el manejo de los incidentes de seguridad.	2	Al estar centralizado la toma de decisiones es más fácil realizar cambios a los procesos y procedimientos internos	2	Es necesario establecer SLA tiempos de respuesta con cada una de las empresas que adquiera el servicio antifraude.

<p>Adecuaciones Locativas</p>	<p>1</p>	<p>Se debe considerar del alquiler de las oficinas.</p>	<p>1</p>	<p>Se adquirirán un total 100 m2.</p>	<p>1</p> <p>Se tendrá en cuenta que estas cuenten con sala de juntas, un cubículo independiente para cada uno de los empleados, cocina y espacios como bodega, baños, cafetería, parqueadero, etc.</p>
<p>Administración del recurso humano</p>	<p>1</p>	<p>La administración del recurso humano se realizará por el Gerente de recursos humanos.</p>	<p>1</p>	<p>Él se manejará la modalidad de Salario integral para evitar el proceso de liquidación mensual de parafiscales</p>	<p>1</p> <p>En este tipo de salario se considera que ya está incluido dentro del valor total del salario, además del trabajo ordinario, las prestaciones, recargos y beneficios tales como el correspondiente al trabajo nocturno, extraordinario, dominical y festivo, el de primas legales, extralegales, las cesantías y sus intereses,</p>

					subsidios y suministros en especie; y en general, las que se incluyan en dicha estipulación.	
Administración Tecnológica	2	El Gerente de Tecnología será el encargado de liderar todos los procesos relacionados.	2	el proyecto contará con interacción de todo un sistema integral para su organización	2	Contará con (Datos, Voz, iluminación, Aire Acondicionado, Muebles y Equipos de oficina, Redes Eléctricas Reguladas y Normales, Sistemas de Acceso Seguro, Turnos Automáticos, Control de Ingreso y Detección de Personal).

Tabla2. Viabilidad, gobernabilidad y pertinencia

9.7 INDICADORES DE DESEMPEÑO DEL PLAN DE NEGOCIO

Indicador	Medida	Objetivo	Metodo	Responsable	Frecuencia
Desempeño					
Registros documentados de la política de gestión y procedimientos	La política de la organización y procedimientos	100 % de avance, relevante y hasta fecha.	Revisión y reporte	Alta Gerencia / Area Financiera	Annual
Organización objetivos, metas y planes	Objetivos y metas planes operativos.	Cumple objetivos / metas / nivel aceptable de servicio (para identificar cada	Revisión e informe interno / auditoría externa.	Director de información	Annual

		objetivo / meta y servicio)			
Confiabilidad					
Acuerdos de Nivel de Servicio (SLA)	medidas de SLA	Cumple SLA (identificar para cada SLA y servicio)	Revisión y informe Interno externo auditoría	Director de información	Anual
Fiabilidad Gestión de Documentos	Número de incidentes Número de quejas Número de sugerencias	No más de 100 por mes	sistema informes / registros.	Gerente de Registros	Mensual
Continuidad del negocio	Actual y viable Plan de pruebas	100 % de avance, relevante y hasta fecha	revisión prueba	Gerente de Registros/Alta Gerencia/CIO	Anual

		Planear satisfactoria cuando se prueba.			
Indicador	Medida	Objetivo	Metodo	Responsable	Frecuencia
Capacidad de respuesta y Puntualidad					
Las solicitudes de los clientes	Los tiempos de respuesta convenidos para diversas peticiones	Numero horas de respuesta dentro de 24 horas tiempo.	sistema informes / registros en todas las divisiones	Gerente de Registros / supervisor del sistema	Mensual
Fidelizacion					
satisfaction del cliente	responder a cuestionario	90% a un nivel establecido	estudio a grupos de enfoque	Director de información	Dos veces al año
Recursos					

Mejora en eficiencia de la operación	Mejora en servicios sin aumento en el costo	Numero de nuevos clients	Revision y informe	Gerente de Registros/Alta Gerencia/Area Financiera	Anual
--------------------------------------	---	--------------------------	--------------------	--	-------

Tabla 3. Indicadores de desempeño

10 ESTUDIO TÉCNICO

10.1 OBJETIVO GENERAL

Determinar el factor de viabilidad para implementación de un negocio de servicio integral antifraudes, mediante su estudio técnico.

10.2 OBJETIVOS ESPECIFICOS

- Determinar que el tamaño podría tener la empresa inicialmente teniendo en cuenta la proyección de ventas del primer año.
- Ubicar estratégicamente la zona en donde estará ubicada la sede de la empresa para el plan de negocio.
- Analizar que recursos físicos son necesarios para para puesta en marcha del negocio teniendo en cuenta las recomendaciones de las industrias de las telecomunicaciones.

TAMAÑO DE LA SEDE PARA EL PLAN DE NEGOCIO

Dentro de los factores condicionantes para determinar el tamaño de nuestro plan de negocio, se deben tener en cuenta los factores atados a la demanda y recursos establecidos para la empresa.

RECURSO HUMANO

Por tratarse de una empresa de seguridad informática, el recurso más importante es el humano, el cual debe ser altamente calificado con experiencia en de detección y análisis de fraudes por internet. Los consultores serán contratados por obra o labor, y tendrán que responder por las horas trabajadas según la entidad en el que se encuentren trabajando.

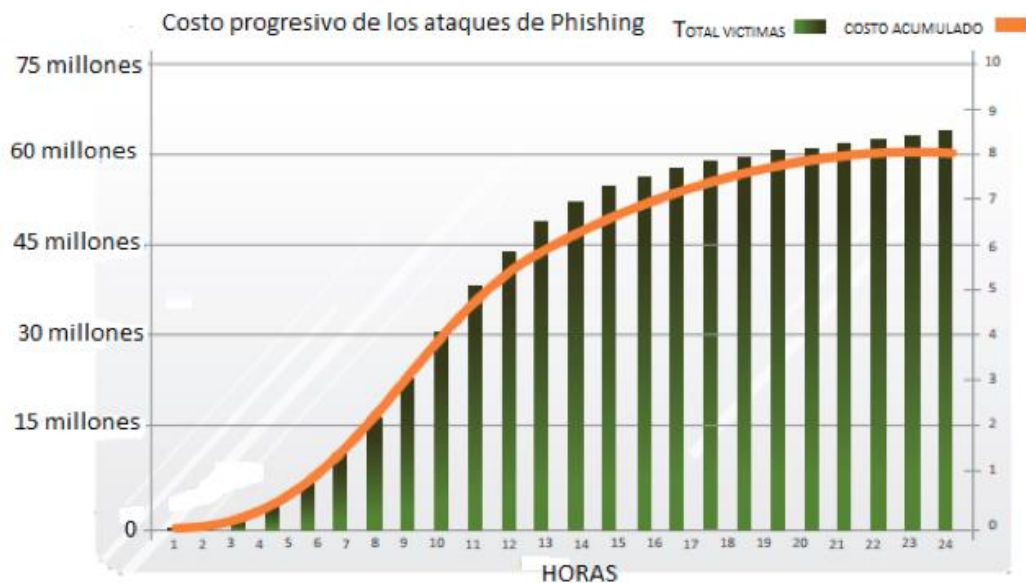
INFRAESTRUCTURA

La infraestructura no impacta demasiado en la operación, gracias a los recursos tecnológicos gratuitos existentes, se generará un esquema de teletrabajo. Dependiendo del desarrollo de la empresa se evaluará la necesidad de establecer una sede propia.

10. 3 ESPECIFICACIONES DE LOS SERVICIOS

SERVICIO ANTIPHISHING

Cada día, las empresas utilizan el concepto de tiempo en la definición de crecimiento de los ingresos “el tiempo es dinero”. Si bien es el momento en el que el dinero gobierna las empresas, también es el momento de la pesca de contraseñas. Los suplantadores de identidad, al igual que cualquier de nosotros, tienen 24 horas en un día para operar. Todos los días se identifican las marcas de destino y se desatan ataques rápidos y prolíficos para hacerse con las credenciales de sitios transaccionales. Los hackers Informáticos son muy conscientes de que entre más tiempo sus ataques virtuales permanezcan activo en la red, más cantidad de dinero pueden ganar.



Grafica 1. Costo progresivo del ataque de Phishing.

“El phishing ha existido desde la década de 1990 en los días de AOL, los estafadores se hicieron pasar por empleados de esta compañía y solicitaron a los usuarios que verificaran la información de facturación. A pesar de que estos primeros ataques contenían errores gramaticales y de ortografía atroces, resultaron exitosos debido a ya que los usuarios de Internet eran muy ingenuos en ese momento”. (Tomado y adaptado de <https://es.wikipedia.org/wiki/Phishing>).

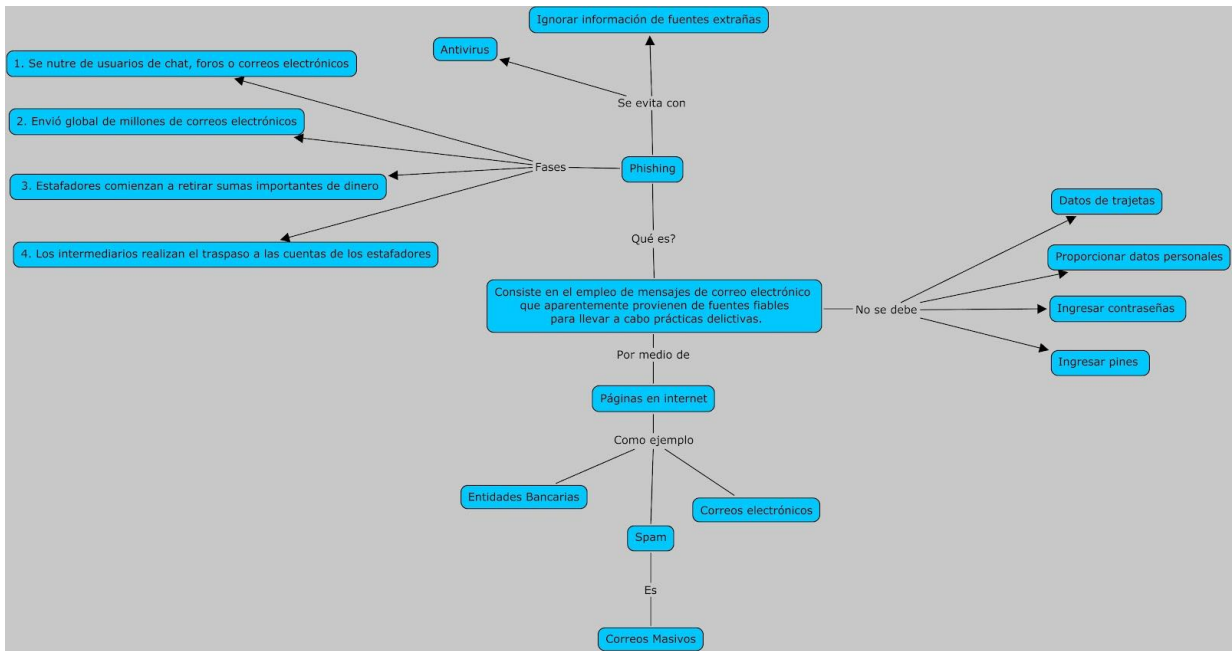


Diagrama4. Mapa Conceptual funcionamiento Phishing

Si damos un avance rápido hasta hoy y examinamos el paisaje ha evolucionado de phishing se ha convertido en un arte mucho más objetivo, racional y rentable. De hecho, hay ahora toda una lista de ataques de phishing especializados.

Spear Phishing	Dirigido a personas o empresas específicas
Clone Phishing	Utiliza correos electrónicos legítimos previamente enviado , pero incluye adjunto malicioso
Vishing Attack	Medio de ataque es llamadas telefónicas
Smishing	Medio de ataque es mensajes de texto
Whaling	Dirigido a directivos y personas de alto perfil
Minnowing	Dirigido a niños de ejecutivos de alto nivel
Pharming	En redireccionar a los usuarios a sitios phishing
Man-in-the-Middle	Escucha activa entre el usuario y la empresa
Man-in-the-Browser	Inyección de contenido activo entre la aplicación Web de alojamiento de usuario y

Tabla 4. Tipos de phishing

Los criminales todavía están atacando los ISP y proveedores de correo electrónico, y ahora también están perfeccionando los ataques hacia los servicios financieros y sitios de compras en línea. Esta tendencia es evidente en la siguiente tabla:

Financial Services		WebMailers		Online Shopping Sites	
Company	Phishing Websites	Company	Phishing Websites	Company	Phishing Websites
PayPal	18947	AOL	1475	Taobao	1691
Wells Fargo	2049	Yahoo	1349	EBay	504
Visa	1661	Hotmail	1205	Amazon	251
Citibank	1628	Gmail	1200	Alibaba	150
Bank of America	1477	Others	188	Littlewoods	
MasterCard	968				
Chase	656				
Bancolombia	369				
Natwest	324				
Gelo	310				

Tabla5. Top de marcas atacadas por phishing. Tomado de trendmicro

Mientras que las empresas más grandes tienen ataques masivos más grandes, hemos aprendido que cualquier negocio es un potencial objetivo. Los bancos, las tiendas online, las compañías de seguros, gobiernos, e incluso los proveedores de seguridad en línea han sido víctimas. También sabemos que los ataques de phishing continúan aumentando.

Ahora también se emplean técnicas de phishing más avanzadas, con los criminales cibernéticos que utilizan software malicioso para redirigir los usuarios desprevenidos a sitios de phishing. Incluso cuando la dirección web correcta se escribe en la barra de navegación, la dirección IP subyacente puede ser manipulado. Estas tácticas más avanzadas son mucho más difíciles de detectar y eliminar. Una cosa es cierta, los ataques de phishing están aquí para quedarse y las tácticas de ciberdelincuentes seguirán evolucionando.

Las estrategias que usará el servicio antiphishing del plan de negocio propuesto está resumido en el siguiente cuadro a continuación:

<p>Filtros de correo electrónico</p>	<p>Filtro que detectara ciertas características de correo electrónico (envío masivo, fuentes IP, direcciones de correo electrónico fraudulentos) y envíe carpeta de correo no deseado. Filtrara alto porcentaje de los ataques de phishing; fácil de desplegar y gestionar a nivel de empresa.</p>
<p>Feeds de spam</p>	<p>Obtener listas de spam y analiza para detectar ataques de phishing. Contienen cargas de datos y pueden detectar muchos ataques de phishing.</p>
<p>Supervisión de registros de dominio</p>	<p>Supervisión del estado del dominio, registro de dominios, las fechas de caducidad de dominio y la actividad del servidor de nombres de dominio. Esto anticipara los ataques de phishing cuando se alerta de la actividad del dominio en tiempo real.</p>

<p>Exploración en Internet</p>	<p>Uso de rastreador web, programas que monitorean metódicamente la web. Este es un proceso automatizado que cubre mucho terreno rápidamente.</p>
<p>Educación</p>	<p>Evaluaciones de ingeniería social que utilicen ejercicios de simulacro de ataque de phishing. Reducirá el riesgo de los empleados sean víctimas de ataques de phishing de forma espectacular.</p>
<p>Herramientas de navegación</p>	<p>Seguridad basada en plug-in de navegador que monitorice la sesión en línea del usuario final. Va más allá de las tecnologías antivirus tradicionales; alertara al usuario de los ataques de phishing en tiempo real.</p>

Tabla 6. Estrategia para detectar, prevenir y mitigar ataques de Phishing.

Ningún enfoque puede garantizar que un phisher no pueda realizar phishing de una marca, lo que se adhieren a la regla de oro que el tiempo es dinero.

Limitar el tiempo de actividad del ataque a reducir los fondos que se puedan sustraer. Un servicio con un tiempo de desactivación rápida podría sonar tentador, pero este número se refiere al tiempo que tarda en cerrar un sitio de phishing después de que se detecte.

Tomemos, por ejemplo, un incidente que pasa desapercibido para los primeros 60

horas. Después de la detección, se tarda 5 horas para ser desactivado. Esto muestra que el ataque tuvo una duración de 65 horas.

De este ejemplo se muestra que es imperativo para seleccionar una solución antiphishing demostrar que puede hacer la detección temprana.

La mayoría de las empresas anteriormente mencionadas son de carácter reactivo, lo que significa que entrar en acción después de una ciberdelincuente ya ha formulado y puesto en marcha un ataque.

La comprensión de que el tiempo es dinero a nuestros va a ser la consigna que utilizara el proyecto de negocio junto con un enfoque proactivo para detectar ataques de phishing todo esto se lograra con un control táctico del sitio protegido del cliente. El control continuo de la página web protegida es lo que distanciara esta solución antiphishing de otras soluciones.

Para realizar la desactivación del sitio de phishing se contactará a una de las partes implicadas de la siguiente manera:

Punto de Contacto	Descripción	Acciones Posibles
Hosting Providers	Es el encargado de proveer y administrar el servidor físico en el que se aloja el sitio	Puede eliminar el contenido fraudulento (archivos), y alertar a los dueños del sitio. Acción inmediata.
Registrar:	Es la empresa que administra el dominio y su reservación. Estas empresas venden los dominios a personas o empresas.	Es la empresa que administra el dominio y su reservación. Estas empresas venden los dominios a personas o empresas.
Registrant	La persona o empresa que reserva	Dado que puede ser el dueño del

	(compra) el dominio al registrar. Muchas veces es el mismo site owner, pero en caso de tratarse de un dominio fraudulento quien registra el dominio es el atacante.	sitio o representa al dueño, pueden eliminar el contenido fraudulento
DNS Provider	Empresa responsable de realizar la resolución (traducción) de dominio a IP.	Puede eliminar la resolución DNS, de manera que pueden deshabilitar el acceso a todo el dominio.
Webmaster	Administrador general del sitio, de sus usuarios y su contenido.	Puede eliminar el contenido fraudulento e implementar medidas de

		seguridad junto al web developer.
Web Developer	Persona que desarrolla o codifica la funcionalidad del sitio.	Puede informar al webmaster y corregir vulnerabilidades de seguridad en código.
Site Owner	La persona o empresa dueños del sitio, quienes son los representantes legales del sitio.	Puede eliminar el contenido fraudulento.
Resellers	Empresa afiliada o asociada a otra compañía de hosting más grande, para ofrecer sus propios servicios de hosting.	Puede eliminar el contenido fraudulento (archivos), y alertar a los dueños del sitio. Acción inmediata.

<p>NIC</p>	<p>Son entidades que administran las bases de datos de los dominios registrados, recopilando información como la IP, el hosting y los datos de contacto tanto del registrar como del registrant. Estas entidades suelen ser regionales, ya sean continentales o nacionales. Por ejemplo, el LACNIC es el NIC para Latinoamérica y el Caribe.</p>	<p>Puede solicitar la remoción del dominio al registrar o al hosting, o remover el dominio si lo administra directamente.</p>
<p>CERT</p>	<p>Computer Emergency Response Team. Son un grupo de expertos que</p>	<p>Puede eliminar el ataque y/o contactar a las</p>

	manejan incidentes de seguridad informática. Varios países cuentan con su propio CERT	autoridades necesarias.
--	---	-------------------------

Tabla 7. Partes interesadas contactos desactivación de Phishing.

SERVICIO DE ANALISIS DE MALWARE

“Un análisis de malware es el arte de la disección del software malicioso para entender cómo funciona, cómo identificarlo y cómo derrotarlo o eliminarlo.

Uno de los propósitos y objetivos del análisis de malware suele ser el poder proporcionar la información necesaria para responder a una intrusión en la red. Este propósito incluye el determinar exactamente lo que sucedió, y qué alcance y grado de dispersión tuvo en la red.

Al analizar los supuestos elementos de software malicioso, en primer lugar, se necesita explorar lo que el archivo binario sospechoso puede hacer, cómo detectarlo en su red, y cómo medir y contener el daño.

El servicio que ofrece el plan de negocio busca analizar los supuestos elementos de software malicioso, en primer lugar, se explorara lo que el archivo binario sospechoso puede hacer, cómo detectarlo en la red, y cómo medir y contener el daño.

Las técnicas que se utilizarán serán:

Técnicas de Análisis de Malware en el Plan de Negocio

Muy a menudo, cuando se realiza el análisis de malware, la única cosa que se tiene es el propio ejecutable malicioso, que no dará demasiada información, ya que está destinado a no ser comprendido por seres humanos. Con la intención de encontrarle sentido, vamos a usar una variedad de herramientas y trucos, cada uno revelando una pequeña cantidad de información.

Habrá que hacer uso de una gran variedad de herramientas con el fin de obtener una comprensión amplia del malware en cuestión. Existen dos enfoques fundamentales para el análisis de malware: los análisis estáticos y los análisis dinámicos. El análisis estático consiste en examinar el malware sin ejecutarlo, mientras que el análisis dinámico implica la ejecución del malware en entornos controlados''. (**Texto textual tomado de <http://blog.elhacker.net/2015/02/introduccion-al-analisis-de-malware-herramientas-forense.html>**)

Análisis Estático

''El análisis estático consiste en examinar el archivo ejecutable sin ver las instrucciones reales. El análisis estático puede confirmar si un archivo es malicioso, proporciona información sobre su funcionamiento, y a veces ofrece información que permitirá realizar un network footprinting simple. El análisis estático básico es sencillo y puede ser rápido, pero es en gran medida ineficaz contra el malware sofisticado, y se pueden pasar por alto funciones importantes''. (**Texto textual tomado de <http://blog.elhacker.net/2015/02/introduccion-al-analisis-de-malware-herramientas-forense.html>**)

Análisis Dinámico

“Las técnicas de análisis dinámicas implican ejecutar el malware y la observación de su comportamiento en el sistema con el fin de averiguar algunos aspectos de su comportamiento, poder eliminar la infección, y producir firmas eficaces. Sin embargo, antes de poder ejecutar el malware de forma segura, se debe configurar un entorno que permita estudiar el malware ejecutándose sin riesgo de daño al sistema o la red. Al igual que las técnicas de análisis”.

(Texto textual tomad de <https://hard2bit.com/blog/analisis-de-malware-enfoque-y-caso-practico/>)

Procedimiento Empírico que se utilizara para Analizar un Malware.

A continuación, se enumera un conducto regular que debe será seguido al momento de analizar un malware:

- Análisis con Herramientas Online

- Identificar el tipo de comprensión del Malware (si existe)
- Comparación de Llaves de Registro
- Análisis de Procesos
- Análisis de Puertos
- Análisis de Conexiones
- Descifrado de Información
- Análisis Estático
- Presentación de Informe

11. ESTUDIO ECONÓMICO Y FINANCIERO

“Hay una herramienta gerencial de suma importancia como lo es el Punto de Equilibrio, que permite calcular el número mínimo de casos de desactivación Antiphishing que el plan de negocio debe vender para no perder ni ganar y que a partir de una unidad adicional que venda empiece a percibir márgenes de utilidad”. **Texto tomado y adaptado de**

http://virtual.senati.edu.pe/pub/GCP/Unidad03/CONTENIDO_U3_PLATAFORMA_COSTOS.pdf

11.2 ESTADOS FINANCIEROS

“El plan de negocios calculará el número mínimo de casos o servicios que deberá producir y vender para no perder ni ganar, teniendo en cuenta una herramienta gerencial de suma importancia, se trata del Punto de Equilibrio”. **Texto tomado y adaptado de**

http://virtual.senati.edu.pe/pub/GCP/Unidad03/CONTENIDO_U3_PLATAFORMA_COSTOS.pdf

“Esta herramienta nos permitirá calcular el punto de equilibrio para la venta de un caso y a partir de la venta de un caso adicional empezar a percibir márgenes de utilidad. En para este proyecto, el punto de equilibrio de servicio se calculará a partir de sus costos fijos y variables y del precio de venta unitario”. **(Texto tomado y adaptado de**

http://virtual.senati.edu.pe/pub/GCP/Unidad03/CONTENIDO_U3_PLATAFORMA_COSTOS.pdf

Teniendo esto en cuenta se fijó un costo operativo de desactivación por caso de \$ 190.000

Esta empresa va manejar un sistema de cantidad de casos contactados que tiene un coste variable de entre 800.000 y 300.000 por caso.

El margen que la empresa obtiene de cada caso es:

$$\text{Margen} = \text{Precio de venta} - \text{coste variable} = 800.000 - 190.000 = 610.000$$

El punto de equilibrio se calcula:

$$\text{P.e.} = \text{Costes fijos} / \text{margen por producto} = 71.500.000 / 610.000 = 117.2 \text{ casos.}$$

En definitiva:

Si la empresa vende 117.2 casos mensual no obtiene ni beneficios ni pérdidas.

Si vende menos de 117.2 casos mensual, tendría pérdidas

Si vende más de 117.2 casos mensual, obtendría beneficios.

“Como se puede observar, el Punto de Equilibrio es una herramienta gerencial importante para la toma de decisiones, porque brinda información sobre la cantidad mínima de casos del servicio que una empresa debe vender para cubrir sus costos”. **(Texto tomado textual de <http://www.gestiopolis.com/punto-de-equilibrio-como-se-determina>)**

11.3 ESTADOS FINANCIEROS

En el plan de negocio de Servicio Antiphishing existirá distintos Departamentos, los cuales pueden agruparse en:

Departamentos de Operación

Departamentos de servicios

el plan de negocio de Servicios Antiphishing que brindará el proyecto a sus clientes.

Estas bases serán:

- El número de casos desactivados.
- El costo operativo directo.
- El costo de la mano de obra directa

11.4 DETERMINACION DE LOS PRECIOS DE LOS SERVICIOS

La política de precios que se manejara en EasyFast Real-Time Servicio Antiphishing está organizada por la cantidad de tickets de desactivación que la entidad bancaria adquiera y con relación a esto, se le asignara una categoría un precio de valor unidad

Categoría	Rango de Tickets	Valor Unidad
Paquete VIP	0-100	\$800.000

Paquete Gold	100-1000	\$500.000
Paquete Platino	1000-ilimitado	\$300.000

Tabla 8. Precios por casos

Para realizar el cálculo del precio de los servicios Antiphishing se tuvieron en cuenta los siguientes tres factores para encontrar el punto de equilibrio:

Costes fijos de la empresa

Costes variables por unidad de producto

Precio de venta del producto.

Para el plan de Negocio propuesto, su especialidad la desactivación de sitios de Phishing.

El servicio presenta los siguientes costos fijos mensuales estimados:

ACTIVOS FIJOS COSTOS DE ARRANQUE

1. Infraestructura	
Terreno	Arrendado \$ -
Adecuaciones	\$ 4.000.000
2. Muebles y Enseres	
Mesa de Juntas	\$ 440.000
Archivador y sillas	\$ 1.010.000
3. Equipo de Computo	
Lap Tops	\$ 21.000.000
Impresora	\$ 250.000
Licencias de Software	\$ 5.000.000
Perifericos	\$ 2.280.000
Discos Externos	\$ 700.000
Router Inalámbrico	\$ 200.000
Telefono fijo	\$ 464.000
Telefono Celular	\$ 3.600.000
Memorias USB	\$ 100.000
4. Gastos Preoperativos	
Licencias y Gastos de Constitución	\$ 1.500.000
Publicidad	\$ 5.000.000
Asesorias	\$ 15.000.000
Estudio de Mercado	\$ 7.000.000
Papeleria	\$ 500.000
Rodamiento y transporte de materiales	\$ 1.000.000
Dominio de correo	\$ 500.000
Material de Consulta	\$ 400.000
Capacitacion	\$ 7.000.000
Gastos de selección y contratación	\$ 4.000.000
6. Caja Inicial	
	\$ 50.000.000
	<u>\$ 130.944.000</u>
Equity	40% \$ 52.377.600
Finaciaión	60% \$ 78.566.400

Tabla 9. Costos iniciales del plan de negocio

GASTOS ADMINISTRATIVOS, OPERACIÓN Y DE VENTAS.

	Unidad	Valor	Otro	Año				
				1	2	3	4	5
Honorarios								
Contador	1	\$ 500.000	\$	6.000.000	\$ 6.177.600	\$ 6.360.457	\$ 6.548.726	\$ 6.742.569
Asesoría Legal	1	\$ 500.000	\$	6.000.000	\$ 6.177.600	\$ 6.360.457	\$ 6.548.726	\$ 6.742.569
Servicios								
Aseo (medio tiempo)	1	\$ 500.000	\$	6.000.000	\$ 6.177.600	\$ 6.360.457	\$ 6.548.726	\$ 6.742.569
Servicios Públicos								
Paquete de comunicaciones	5	\$ 140.000	\$	8.400.000	\$ 8.648.640	\$ 8.904.640	\$ 9.168.217	\$ 9.439.596
Celulares	5	\$ 100.000	\$	6.000.000	\$ 6.177.600	\$ 6.360.457	\$ 6.548.726	\$ 6.742.569
Gastos Generales								
Papelaría	1	\$ 200.000	\$	2.400.000	\$ 2.471.040	\$ 2.544.183	\$ 2.619.491	\$ 2.697.028
Mantenimiento Equipos TIC	1	\$ 50.000	\$	600.000	\$ 617.760	\$ 636.046	\$ 654.873	\$ 674.257
Elementos de aseo y cafetería	1	\$ 100.000	\$	1.200.000	\$ 1.235.520	\$ 1.272.091	\$ 1.309.745	\$ 1.348.514
Investigación y Desarrollo	1	\$ 1.000.000	\$	12.000.000	\$ 12.355.200	\$ 12.720.914	\$ 13.097.453	\$ 13.485.138
Arrendamiento	1	\$ 1.600.000	\$	19.200.000	\$ 19.768.320	\$ 20.353.462	\$ 20.955.925	\$ 21.576.220
Otros	1	\$ 150.000	\$	1.800.000	\$ 1.853.280	\$ 1.908.137	\$ 1.964.618	\$ 2.022.771
Impuestos								
**Ica			0,50%	\$ 2.204.072	\$ 2.861.242	\$ 3.025.616	\$ 2.776.861	\$ 3.624.556
Gastos de Ventas								
Publicidad y Mercadeo	1	\$ 2.000.000	\$	24.000.000	\$ 24.710.400	\$ 25.441.828	\$ 26.194.906	\$ 26.970.275
Investigación de Mercados	1	\$ 300.000	\$	3.600.000	\$ 3.960.000	\$ 4.356.000	\$ 4.791.600	\$ 5.270.760
Comisiones			5,00%	\$ 20.904.000	\$ 26.983.757	\$ 28.664.459	\$ 26.455.218	\$ 34.623.091
Depreciación			\$	11.488.000	\$ 11.488.000	\$ 12.276.889	\$ 18.554.667	\$ 18.554.667
Total			\$	\$ 131.796.072	\$ 141.663.559	\$ 147.546.093	\$ 154.738.479	\$ 167.257.146

Tabla 10. Gastos administrativos, operación y ventas.

GASTOS DE PERSONAL	CANTIDAD	VALOR	INCREMENTO	1	2	3	4	5
GERENTE	1	\$4.000.000	4%	\$48.000.000	\$49.920.000	\$51.916.800	\$53.993.472	\$56.153.211
INGENIEROS	15	\$2.500.000	4%	\$450.000.000	\$468.000.000	\$486.720.000	\$506.188.800	\$526.436.352
VENDEDOR	1	\$4.000.000	4%	\$48.000.000	\$49.920.000	\$51.916.800	\$53.993.472	\$56.153.211
TOTA				\$546.000.000	\$567.840.000	\$590.553.600	\$614.175.744	\$638.742.774

GASTOS DE PERSONAL

Tabla 11. Gastos de personal

PRONOSTICO DE VENTAS

AÑO	1	2	3	4	5
Numero de Proyectos	27	35	43	50	65
Casos Requeridas Promedio por proyecto	3500	4200	4900	5600	6300
Precio por caso	\$300.000	\$300.000	\$300.000	\$300.000	\$300.000
Ingresos	\$1.050.000.000	\$1.260.000.000	\$1.470.000.000	\$1.680.000.000	\$1.890.000.000

Tabla 12. Pronostico de ventas

11 ASPECTOS LEGALES

“La Superintendencia Financiera de Colombia publicó la Circular Externa 042 el 4 de octubre de 2012 con el propósito de fortalecer y actualizar los requerimientos mínimos de seguridad para llevar a cabo operaciones y transacciones bancarias por medios electrónicos. Estas pautas ajustan el marco regulatorio financiero de Colombia para reflejar mejor las nuevas condiciones de las amenazas con que se enfrentan los diferentes canales de transacción y mantenerse al día con estándares de otras partes del mundo. Este documento explica los nuevos aspectos en la Circular Externa 042 y cómo su institución financiera puede cumplir con ella de forma fácil y eficiente.

Phishing, fraude en línea y otros tipos de delitos informáticos son amenazas globales que se están haciendo más comunes con el paso de los años y evolucionando para encontrar nuevas vulnerabilidades a explotar y nuevas formas para evadir la detección. Colombia no es inmune a este problema y algunos ataques recientes de alto perfil junto con estadísticas de años pasados muestran que las instituciones de cualquier tipo están asediadas por el permanente fantasma de la inseguridad en línea.

El periódico Portafolio reportó el año pasado que las pérdidas causadas por delitos informáticos ascendieron a 40 millones de dólares (79 mil millones de pesos) al año, y que casi 10 millones de colombianos fueron víctimas de alguna clase de fraude electrónico durante los pasados doce meses. Considerando que sólo un poco más de la mitad de los 47 millones de colombianos tienen acceso a Internet, tal cantidad de delitos electrónicos es sorprendente. No es que el gobierno de Colombia haya estado ausente en este tema; de hecho, la ley 1273 de

2009 hizo del país el primero en penalizar seriamente a los cibercriminales con condenas entre los 4 y 8 años. Pero en nuestro mundo globalizado e interconectado, el crimen cibernético no conoce fronteras, tanto así que los grupos criminales altamente organizados de Asia, Europa oriental y Estados Unidos han estado atacando cuentas bancarias alrededor del mundo”. (Texto tomado y adaptado de circular externa 042 de 2012

superfinanciera fue tomada y adaptada al texto publicado en

https://www.superfinanciera.gov.co/SFCant/Normativa/NormasyReglamentaciones/cir007/cap12_seguridad_calidad.doc)

En toda Latinoamérica no tienen idea de las amenazas latentes en la web, y muchos más no poseen ningún tipo de protección contra las últimas amenazas, incluyendo ataques de Man-in-the-Middle, Man-in-the-Browser y keyloggers. Esta ausencia de conocimiento y protección conlleva graves consecuencias para la industria financiera y es aprovechada por los criminales, fomentando más el fraude.

12. 1 NORMAS DE TODO GÉNERO PERTINENTES PARA LA LEGALIZACIÓN DEL PROYECTO

“Los requerimientos mínimos de seguridad para realizar operaciones bancarias en Colombia han aumentado con la publicación de la Circular Externa 042 (CE 042) de la Superintendencia Financiera de Colombia (SFC), el ente de regulación financiera del gobierno de Colombia. Este documento ajusta las normas colombianas a las condiciones cambiantes de las amenazas que enfrentan los canales transaccionales y mantiene al tanto las normas del país con respecto a los estándares de otras partes del mundo.

Además, la Circular Externa 042 describe el régimen de transición para la implementación de nuevas medidas para realizar transacciones en Internet y con audio-respuesta (IVR), las cuales serán obligatorias este año. Las nuevas normas exigen que las instituciones financieras tengan mecanismos que incrementen la seguridad de sus portales virtuales, protegiéndolos de ataques que afecten la seguridad de estas operaciones en Internet. Al mismo tiempo, las entidades deben ofrecerles a sus clientes mecanismos de autenticación fuerte para las transacciones que se hagan a través de Internet, IVR y teléfonos móviles. La autenticación fuerte es definida por el documento como el conjunto de técnicas y procedimientos utilizados para verificar la identidad de un cliente, entidad o usuario. Los factores de autenticación son: algo que se sabe, algo que se tiene, algo que se es.

La Circular Externa 042 también menciona un número de métodos comunes de autenticación fuerte que son aceptados como formas válidas de identificar a un usuario, incluyendo biometría, firmas digitales certificadas, contraseñas de un solo uso (OTP) que funcionen por tiempo limitado, tarjetas de débito o crédito EMV que tengan un chip que fortalezca los estándares de seguridad, y métodos para identificar los dispositivos del usuario. OTP, tarjetas EMV y autenticación de dispositivos deben ser usados junto con un segundo factor de autenticación para que sean considerados como autenticación fuerte. Internet y los canales móviles deben tener estos métodos de autenticación para julio de 2013, mientras que los IVR deben tener implementado un sistema similar para el mes de octubre de 2013''. **(Texto tomado y adaptado de circular externa 042 de 2012**

superfinanciera fue tomada y adaptada al texto publicado en

https://www.superfinanciera.gov.co/SFCant/Normativa/NormasyReglamentaciones/cir007/cap12_seguridad_calidad.doc).

13. BIBLIOGRAFÍA

- [1] <http://www.antiphishing.org/>
- [2] <http://www.emc.com/domains/rsa/index.htm>
- [3] <http://es.wikipedia.org/wiki/Phishing>
- [4] <https://web.certicamara.com/eventos/eventos-realizados/seguridad-para-servicios-financieros/>
- [5] <http://www.asobancaria.com/portal/page/portal/Asobancaria/seguridad/phishing/>
- [6] <http://www.webroot.com/es/es/partners/technology-partners/real-time-antiphishing>
- [7] <https://www.markmonitor.es/services/antifraud.php>
- [8] <https://hard2bit.com/blog/analisis-de-malware-enfoque-y-caso-practico/>
- [9] <http://www.trendmicro.com/us/index.htm>
- [10] https://www.superfinanciera.gov.co/descargas?com=institucional&name=pubFile31164&downloadname=ce042_12.doc
- [11] <https://prezi.com/vm8o2doqllaw/copy-of-spyware-malware/>
- [12] [http://intercambiosos.org/showthread.php?t=15470\)](http://intercambiosos.org/showthread.php?t=15470)
- [13] <http://www.taringa.net/posts/info/5078414/Amenazas-informaticas.html>
- [14] <http://docplayer.es/8952480-Unidad-2-delitos-informaticos-y-seguridad-de-la-informacion.html>
- [15] <https://www.markmonitor.es/services/antifraud.php>
- [16] http://virtual.senati.edu.pe/pub/GCP/Unidad03/CONTENIDO_U3_PLATAFORMA_COSTOS.pdf
- [17] <https://hard2bit.com/blog/analisis-de-malware-enfoque-y-caso-practico/>