UNIVERSIDAD TECNOLÓGICA ISRAEL

CARRERA DE SISTEMAS INFORMÁTICOS

“IMPLEMENTACIÓN DE UN PLAN DE SEGURIDADES CONTRA EL PHISHING EN LA COOPERATIVA DE AHORRO Y CREDITO COOPERCO”

AUTOR:

Carlos Renan Salto Sari

TUTOR:

Ing. Mario Mejia

Quito - Ecuador

2013

UNIVERSIDAD TECNOLÓGICA ISRAEL

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Graduación certifico:

Que el Trabajo de Graduación "IMPLEMENTACIÓN DE UN PLAN DE SEGURIDADES CONTRA EL PHISHING EN LA COOPERATIVA DE AHORRO Y CREDITO COOPERCO", presentado por Carlos Renan Salto Sari, estudiante de la carrera de Sistemas Informáticos, reúne los requisitos y méritos suficientes para ser sometido a la evaluación del Tribunal de Grado, que se designe, para su correspondiente estudio y calificación.

Quito, enero 2013

TUTOR

_____

Ing. Mario Mejia
C.C.

UNIVERSIDAD TECNOLÓGICA ISRAEL

AUTORÍA DE TESIS

La abajo firmante, en calidad de estudiante de la Carrera de Sistemas Informáticos declaro que los contenidos de este Trabajo de Graduación, requisito previo a la obtención del Grado de Ingeniero en Sistemas Informáticos, son absolutamente originales, auténticos y de exclusiva responsabilidad legal y académica del autor.

Quito, enero del 2013

_____

Carlos Renan Salto Sari.
CC: 010418033-6

DEDICATORIA.

La realización de este Proyecto va dedicada a Dios, que nos ha guiado durante todo este tiempo, en el transcurso de nuestra carrera profesional, a mi familia especialmente a mis Padres, que con su apoyo y paciencia me han demostrado que todo sacrificio nos lleva a cumplir los sueños y las metas trazadas en la vida, a todos los profesores de la Universidad, que con sus conocimientos me han sabido instruir para alcanzar mi objetivo de ser un gran profesional.

AGRADECIMIENTO.

Un agradecimiento muy especial a la Universidad, por abrirme las puertas y brindarme la oportunidad de culminar con éxito la carrera y a sus profesores que con sus conocimientos y enseñanzas me han sabido instruir de la mejor manera para la realización de este proyecto y subir un escalón más de tantos en mi vida profesional.

También quiero agradecer a mi Familia que ha sido un pilar fundamental en todo este tiempo y gracias a su apoyo y consejos estoy culminando mi carrera.

A mis compañeros que gracias a su amistad y constancia hemos logrado alcanzar nuestro objetivo de ser grandes profesionales.

RESUMEN.

El mundo avanza y con él las finanzas, al ritmo que la sociedad actual lo demande, y vemos que la tecnología va de la mano, en un mercado cuyos movimientos son cada vez más rápidos, permitiendo así que las instituciones financieras tengan una aceleración cada vez mayor.

En los últimos años la banca en el mundo ha experimentado cambios estructurales gracias a la tecnología, implementando sistemas de operación transaccionales y siguiendo el desarrollo de interfaces automáticas, la integración de datos y sistemas y la implementación de tecnología tanto para la banca como para los clientes.

Los clientes hoy en día pueden ver el saldo en sus cuentas bancarias, hacer transacciones casi en tiempo real, así como realizar transferencias entre diferentes números de cuentas, todo esto a través del internet.

Es por ello que cada día aumenta el número de entidades que se apuntan a esta modalidad de banca a distancia, y así no perder la clientela que apuesta por este medio.

El crecimiento de las operaciones bancarias realizadas por internet, ha ido unido a problemas de seguridad que se han puesto de manifiesto al utilizar esta vía, y que hace que las entidades dediquen cada día más medios para el desarrollo seguro de la banca por internet. Frente a las diversas modalidades de fraude relacionado con la banca por internet (Phishing) las entidades han desarrollado nuevas fórmulas de combinación de claves y una serie de recomendaciones para que el cliente bancario tenga el mínimo riesgo.

SUMMARY.

The world moves on and with it the finances, at a pace that today's society demands, and we see that technology goes hand in hand, in a market whose movements are getting faster, allowing financial institutions have increasingly accelerated greater.

In recent years banks in the world has undergone structural changes with technology, implementing transactional systems operation and following the development of automatic interfaces, data integration and implementation of systems and technology for both banks and customers.

Customers today can see the balance in their bank accounts; make transactions in near real time, as well as transfers between different account numbers, all through the internet.

That is why every day the number of entities that are targeted to this type of remote banking, and not lose the customers that bet by this means.

The growth of bank transactions online has been linked to safety concerns that have been shown to use this route, and that makes institutions increasingly dedicated to the safe means of internet banking. Faced with the various forms of fraud related to internet banking (Phishing) institutions have developed new ways of combination of keys and a set of recommendations for the client to have the lowest risk banking.

TABLA DE CONTENIDO

LISTA DE CUADROS Y GRAFICOS

Capítulo I

1. Introducción.

1.1 Tema.

IMPLEMENTACIÓN DE UN PLAN DE SEGURIDADES CONTRA EL PHISHING EN LA COOPERATIVA DE AHORRO Y CREDITO COOPERCO.

1.2 Antecedentes.

Según consta en la página web de la Superintendencia de Bancos, el phishing consiste en el robo de su información personal a través de señuelos para que las víctimas ingresen su información, páginas web falsas, correos electrónicos que parecen provenir de su institución financiera o de empresas con las que las personas tienen algún tipo de relación.

De apariencia muy similar a las originales, obtienen los datos de las personas a través de un correo electrónico supuestamente en blanco, o de la misma página falsa que termina robando los datos, haciéndole creer a las víctimas que debe enviar sus claves o datos tales como su nombre, número de cédula, número de cuenta o número de tarjeta, dirección, teléfono, para asuntos de confirmación o actualizaciones, transferencias o premios de los que supuestamente es el acreedor. (Hoy, 2010)

1.3 Problema.

1.3.1 Formulación del Problema.

¿Mediante la IMPLEMENTACIÓN DE UN PLAN DE SEGURIDADES CONTRA EL PHISHING EN LA COOPERATIVA DE AHORRO Y CREDITO COOPERCO, se obtendrá mayor seguridad al momento de navegar en la Banca Electrónica de esta cooperativa?

1.4 Sistematización.

1.4.1 Diagnóstico y Pronóstico.

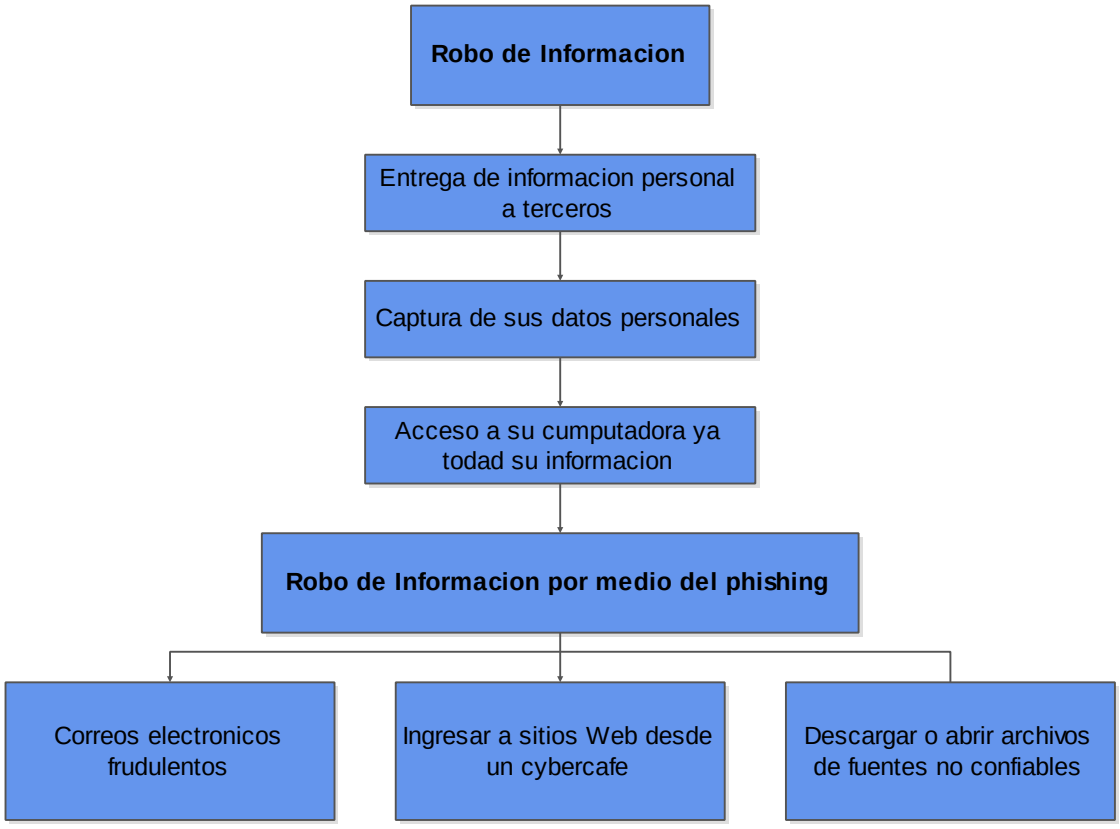


Figura 1 Problemas ocasionados por el phishing.

1.4.2 Control del pronóstico.

Implementar un plan de seguridades para ingresar a la página Web de la COOPERATIVA DE AHORRO Y CREDITO COOPERCO.

Manera recomendada de navegación en la página web de la cooperativa.

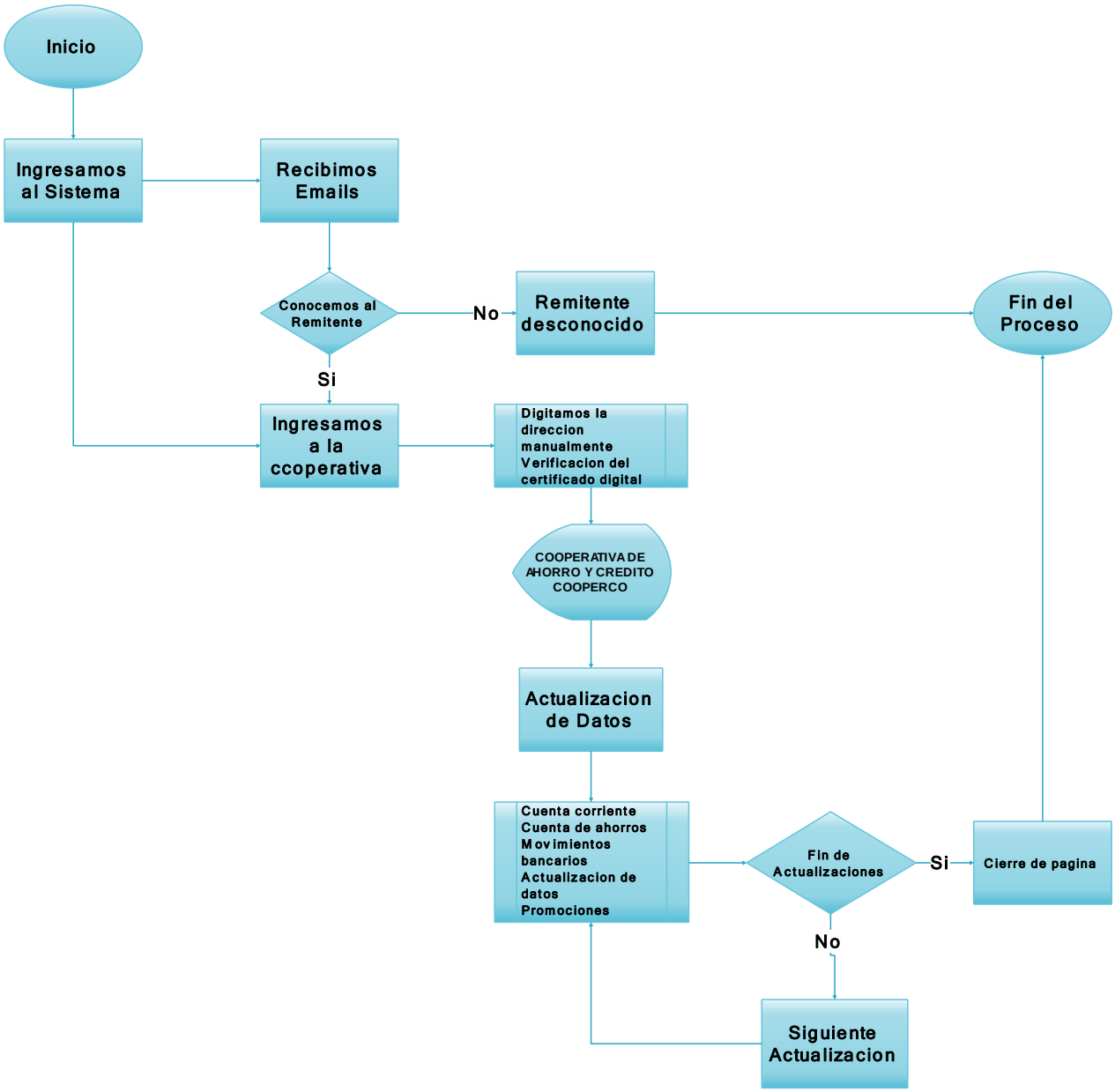


Figura 2 Control del Pronóstico.

1.5 Objetivos.

1.5.1 Objetivo General.

IMPLEMENTACIÓN DE UN PLAN DE SEGURIDADES CONTRA EL PHISHING EN LA COOPERATIVA DE AHORRO Y CREDITO COOPERCO.

1.5.2 Objetivo Específico.

- Investigar las formas de navegar de los socios.
- Diseñar un plan de Seguridades contra el Phishing.

1.6 Justificación.

1.6.1 Justificación Teórica.

Con la siguiente investigación daremos a conocer los daños causados por el phishing que oscilan entre la pérdida del acceso al correo electrónico a pérdidas económicas.

Daremos a conocer mediante el diseño y la implementación de seguridades contra el phishing los pasos a seguir para no ser víctimas de [1]fraudes económicos.

[1] Fraude.- Fraude es una acción que resulta contraria a la verdad y a la rectitud. El fraude se comete en perjuicio contra otra persona o contra una organización (como el Estado o una empresa).

1.6.2 Justificación Práctica.

Al ingresar a la página web de la agencia bancaria, el usuario debe entender el funcionamiento de tal forma que pueda encontrar la opción de visualizar su estado de cuenta o hacer transferencias bancarias, sin el temor de acceder a páginas fraudulentas.

De lo contrario los usuarios terminarían por frustrarse, con el temor de ser víctimas del phishing y necesitaría contactar telefónicamente o pedir personalmente asistencia técnica.

1.6.3 Justificación Metodológica.

Método Investigativo:

- Formas de phishing.
- Como funciona los phishing.

Diseño del Plan:

- Formas de detectar un phishing.
- Formas de combatir el robo atreves de un phishing.
- Navegación Segura en la página web del banco.

Investigar las formas en que los phishing actúan para el robo de información, que lo mostraremos gráficamente para un mejor entendimiento.

De esta manera se elaborara un plan para que los usuarios o socios del banco puedan acceder sin temor a la página web del banco.

1.7 Alcance y Limitaciones.

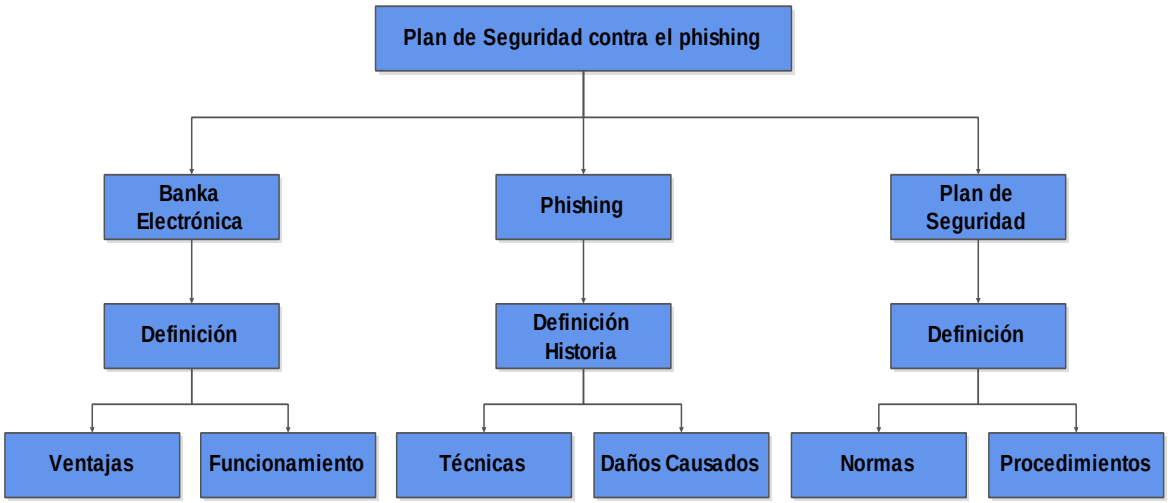


Figura 3 Alcance y Limitaciones.

1.8 Estudio de Factibilidad.

1.8.1 Técnica.

Disponer de los siguientes elementos:

- Una computadora con conexión a Internet.
- Página web de la agencia bancaria.
- Usuarios o socios de la agencia bancaria.

Se analizara mediante la conexión a Internet, como los phishing suplantan la imagen de una entidad financiera, para en lo posterior tomar las medidas necesarias para que el usuario utilice de forma adecuada la página web de la agencia bancaria.

1.8.2 Operativa.

La realización de este plan para la Implementación de seguridades contra el phishing en esta agencia bancaria, recalca la importancia de que los usuarios no faciliten nunca sus claves personales por medio del correo electrónico, como método para evitar que sus cuentas sufran estafas mediante phishing.

1.8.3 Económica.

Análisis Costo – Beneficio.

		Analisis Costo - Beneficio		
Vamos a analizar si nuestro proyecto sera rentable en los proximos dos meses				
que tiene de duracion para su elaboracion.				
La proyeccion de nuestros ingresos al fianl de los dos meses es de $ 3000				
esperando una tasa de rentabilidad del 12% mensual				
Para el proyecto a realizar se estima una inversion de $ 1200 con una tasa de				
interes del 20 % mensual.				
Hallamos B/C:				
B/C = VAI / VAC				
B/C = Costo-Beneficio				
VAI = Valor Actual de Ingresos				
VAC = Valor Actual de Costos				
B/C = (3000 / (1 + 0.12)^2) / (1200 / (1 + 0.20)^2)				
B/C = (3000 / 1.25) / (1200 / 1.44)				
B/C = (2400 / 833.33)				
B/C = 2.88				
Como la relacion costo beneficio es mayor a 1, pedemos continuar con el				
desarrollo de nuestro proyecto.				
Podemos decir que por cada dólar que invertimos nuestra ganancia sera de				
$ 1.88				

Tabla 1 Análisis costo beneficio.

Capitulo II.

2. Marco de Referencia.

2.1 Marco Teórico.

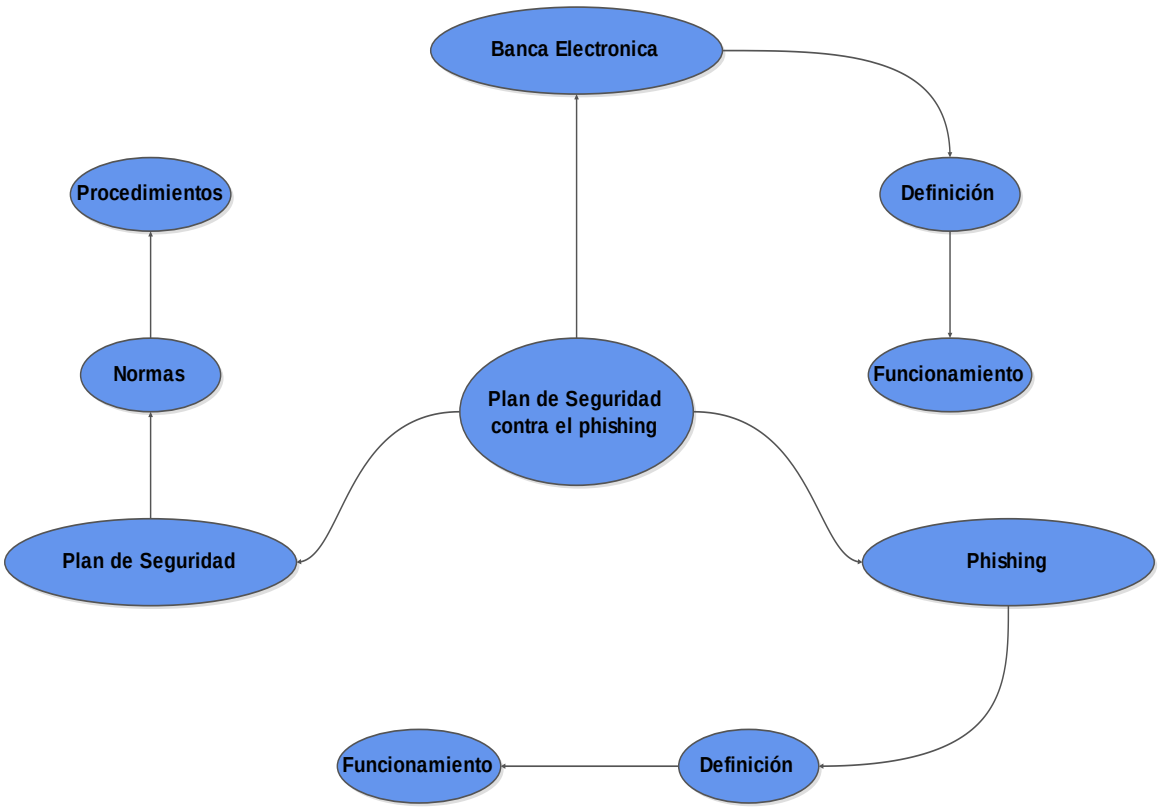


Figura 4 Marco Teórico.

Conceptos:

Servicios del Sistema Financiero Ecuatoriano.

- Banca por Internet.
- Definición.

Banca Virtual.

- Definición.

Banca Electrónica.

- Definición.
- Ventajas.
- Funcionamiento.

Phishing.

- Definición.
- Historia.
- Técnicas.
- Daños causados.

Plan de Seguridad.

- Definición.
- Normas.
- Procedimientos.

Aplicación.

Investigaremos y analizaremos lo que es la banca electrónica o virtual, su funcionamiento y las ventajas que tienen estas para con los usuarios de la cooperativa.

Se analizara las desventajas y en especial hablaremos de la suplantación de la banca electrónica en especial del phishing y como perjudica a los usuarios.

Finalmente hablaremos de la seguridad informática, y la manera de que los usuarios deben manejar estos servicios.

2.2 Marco Conceptual.

2.2.1 Servicios del Sistema Financiero Ecuatoriano.

2.2.1.1 Banca por Internet.

Gracias al avance de cobertura que tiene el internet, muchas agencias bancarias y financieras han implementado este medio de comunicación como el principal punto de contacto con su clientela.

Mediante el Internet los clientes pueden informarse sobre los diferentes productos que ofrece la entidad bancaria, y de igual manera tienen la facilidad de realizar diferentes transacciones bancarias con comodidad sin salir de casa o de la oficina.

Para esto el usuario debe de haber firmado un contrato con la entidad bancaria y disponer de una clave personal.

Por tal razón aumenta día a día el número de entidades bancarias que apuestan a esta modalidad de la banca a distancia, para comodidad de los clientes y de esta manera no perderlos ya que son estos los que apuestan por este medio.

De igual manera estos avances tecnológicos, han ido de la mano por los problemas de seguridad, que se han puesto de manifiesto al utilizar este medio de comunicación y por lo tanto las entidades bancarias dedican tiempo al desarrollo de medios de seguridad para un manejo seguro de la banca por internet.

Las entidades bancarias desarrollan nuevas fórmulas de combinaciones de claves y una serie de recomendaciones para que los clientes bancarios tengan el mínimo riesgo, frente a las diferentes maneras de fraude de la banca por internet (Phishing). (Servicios del Sistema Financiero Ecuatoriano, 2012)

2.2.2 Banca Virtual.

Banca virtual, banca en línea, banca electrónica, es la banca a la que se puede acceder mediante Internet. Pueden ser entidades con sucursales físicas o que sólo operan por Internet o por teléfono.

La banca telefónica apareció en España a mediados de 1995 de la mano del Banco Español de Crédito (Banesto) y del Banco Central Hispano. Aunque inicialmente solo servía como medio de consulta, en la actualidad incorpora prácticamente todos los servicios del sistema financiero.

2.2.3 Banca Electrónica.

Se define a la banca electrónica como la oferta de servicios y productos bancarios a través de canales electrónicos e incluiría todo tipo de operación que se realiza con la intervención personal. Esta nueva forma de ver la banca abre nuevas oportunidades para los bancos y para sus clientes.

2.2.3.1 Ventajas.

Se muestra algunas ventajas que ofrece la Banca Electrónica al consumidor:

- Comodidad y servicios de conveniencia, 24 horas al día, 7 días a la semana. Operaciones desde casa.
- Acceso global.
- Ahorro en tiempo.
- Ahorro en costes para el banco que pueden o deben repercutir en el cliente.
- Transparencia en la información.
- Capacidad de elección de los clientes.
- Oferta de productos y servicios personalizados.

(Nina, 2012)

2.2.3.2 Funcionamiento.

La manera de operar de la Banca electrónica es en línea con el servidor del banco, para esto cuenta con un sistema que permite a los clientes el acceso a la base de datos de la entidad para solicitar información y realizar transacciones bancarias.

El tiempo de conexión o utilización se verá reducido al tiempo que se requiera para transferir información en cualquier sentido, y dependerá del volumen de información (número de transacciones u operaciones) y de la velocidad de transferencia que permita su canal dedicado a internet.

Para solicitar la información del Banco, ingrese a "Consulta" y elija la opción "Cuentas", con esto el Servicio de Banca Virtual hará que el servidor del Banco le envíe la información registrada en tiempo real. Cada vez que usted ejecute la opción "Cuentas" obtendrá la última información registrada en el computador del Banco.

Para realizar operaciones bancarias ingrese al módulo de "Transferencias", siguiendo la recomendación de que una transacción no debe ser totalmente ejecutada por un sólo funcionario, ya que todas las transacciones que se realicen, tiene que ser aprobadas por un segundo funcionario antes de quedar habilitadas para el envío al Banco.

Una vez que las transacciones sean aprobadas y procesadas, el Servicio de Banca Virtual hará que el computador del Banco reciba toda la información de las transacciones realizadas. (Como funciona la banca virtual, 2012)

2.2.4 Phishing.

El phishing es una técnica de sustracción de datos personales y de cuentas bancarias de manera ilícita a través de enlaces de correos electrónicos o páginas Web, que suplantan la imagen de una entidad financiera.

Figura 5 Phishing.

Fuente: http://419.bittenus.com/es/phishing.htm.

2.2.4.1 Historia.

Origen del término.

El termino phishing, viene de la palabra "fishing" (pesca), que trata de que los usuarios "muerdan un anzuelo", a estos delincuentes se les llama phisher.

Se dice también que el término phishing es la contracción de password harvesting fishing (cosecha y pesca de contraseñas).

La primera mención del término phishing data de enero de 1996. Se dio en el grupo de noticias de hackers alt.2600, aunque es posible que el término ya hubiera

aparecido anteriormente en la edición impresa del boletín de noticias hacker 2600 Magazine. El término phishing fue adoptado por quienes intentaban "pescar" cuentas de miembros de [2]AOL.

Phishing en AOL.

En los años 1990 los delincuentes que comenzaron a hacer phishing en AOL, obtenían cuentas para usar los servicios de esa compañía a través de números de tarjetas de crédito válidos, utilizando algoritmos para tal efecto. Estas cuentas de acceso a AOL podían durar semanas e incluso meses.

En 1995 la compañía AOL tomó medidas para prevenir este uso fraudulento de sus servicios, de modo que los crackers recurrieron al phishing para obtener cuentas legítimas en AOL.

El phishing en AOL estaba muy relacionado con la comunidad de [3]warez que intercambiaba software falsificado. Un cracker se hacía pasar como un empleado de AOL y enviaba un mensaje instantáneo a una víctima potencial. Para poder engañar a la víctima de modo que diera información confidencial, el mensaje podía contener textos como "verificando cuenta" o "confirmando información de factura". Una vez el usuario enviaba su contraseña, el atacante podía tener acceso a la cuenta de la víctima y utilizarla para varios propósitos criminales, incluyendo el [4]spam. Tanto el phishing como el warezing en AOL requerían generalmente el uso de programas escritos por crackers.

[2] AOL.- Empresa estadounidense que presta servicios de internet a nivel global.
[3] Warez hace referencia a la distribución de material que viola las leyes derechos de autor.
[4] Spam.- El spamming es el hecho de enviar mensajes electrónicos (spam) (habitualmente de tipo comercial) no solicitados y en cantidades masivas.

En 1997 AOL reforzó su política respecto al phishing y los warez fueron terminantemente expulsados de los servidores de AOL. Durante ese tiempo el phishing era tan frecuente en AOL que decidieron añadir en su sistema de mensajería instantánea, una línea de texto que indicaba: «no one working at AOL will ask for your password or billing information» («nadie que trabaje en AOL le pedirá a usted su contraseña o información de facturación»). Simultáneamente AOL desarrolló un sistema que desactivaba de forma automática una cuenta involucrada en phishing, normalmente antes de que la víctima pudiera responder. Los phishers se trasladaron de forma temporal al sistema de mensajería instantáneo de AOL (AIM), debido a que no podían ser expulsados del servidor de AIM. El cierre obligado de la escena de warez en AOL causó que muchos phishers dejaran el servicio, y en consecuencia la práctica. (Historia del phishing, 2012)

2.2.4.2 Técnicas.

Los phishers envían un e-mail a tantos usuarios como puedan simulando pertenecer a una empresa legítima existente, e intenta estafarlos solicitándoles de manera urgente información privada que será utilizada para el robo de identidad.

El e-mail viene con un enlace que conduce al usuario a visitar un sitio Web en el que se le solicita actualizar información personal, como contraseñas y tarjetas de crédito, seguridad social y números de cuentas bancarias, que la organización legítima ya tiene. El sitio Web, sin embargo, es falsa, creada sólo para robar la información de los usuarios. (phishing)

2.2.4.3 Daños Causados.

Los principales daños provocados por el phishing son:

- Robo de identidad y datos confidenciales de los usuarios.
- Pérdidas económicas para los usuarios.
- Impedir el acceso a sus propias cuentas.
- Pérdida de productividad.
- Consumo de recursos de las redes corporativas (ancho de banda, saturación del correo, etc.).

(Los principales daños provocados por el phishing)

2.2.5 Plan de Seguridad.

Debido a que el Internet va creciendo de una manera acelerada, cada vez más entidades bancarias permiten a sus socios y proveedores acceder a sus sistemas de información.

Por lo tanto, importante y fundamental saber qué recursos de la compañía necesitan protección para así controlar el acceso al sistema y los derechos de los usuarios del sistema de información. Los mismos procedimientos se aplican cuando se permite el acceso a la compañía a través de Internet.

Además, debido a la tendencia creciente hacia un estilo de vida [5]nómada de hoy en día, el cual permite a los empleados conectarse a los sistemas de información casi desde cualquier lugar, se pide a los empleados que lleven consigo parte del sistema de información fuera de la infraestructura segura de la compañía.

2.2.5.1 Introducción a la seguridad.

Los riesgos, en términos de seguridad, se caracterizan por lo general mediante la siguiente ecuación.

$$\text{Risque} = \frac{\text{Menace x Vulnérabilité}}{\text{Contre-mesure}}$$

Figura 6 Ecuación sobre los riesgos de seguridad.

"Riesgo es igual a la amenaza por vulnerabilidad sobre contra menos medición".

La amenaza representa el tipo de acción que tiende a ser dañina, mientras que la vulnerabilidad (conocida a veces como falencias (flaws) o brechas (breaches)) representa el grado de exposición a las amenazas en un contexto particular. Finalmente, la contramedida representa todas las acciones que se implementan para prevenir la amenaza.

El usuario debe capacitarse implementando soluciones técnicas y debe tomar conciencia y establecer reglas definidas.

[5] Nómada (del griego: νομάδε, nómada ", al que deja los rebaños en los pastos"), generalmente comunidades o pueblos de personas que se trasladan de un lugar a otro, en lugar de establecerse permanentemente en un solo lugar.

Para que un sistema de una entidad bancaria sea seguro, se debe identificar las posibles amenazas y por lo tanto, conocer y prever el curso de acción del enemigo, el objetivo es identificar las motivaciones de los hackers y categorizarlas para dar una idea de cómo funciona, y así saber la forma de reducir el riesgo de ataques de phishing.

2.2.5.2 Objetivos de la Seguridad Informática.

Los sistemas de información generalmente incluyen todos los datos de una compañía, en el material y los recursos de software que permiten almacenar y hacer circular estos datos. Los sistemas de información son fundamentales para las compañías y deben ser protegidos.

La seguridad informática consiste en garantizar que la información y los recursos de software de una organización en este caso de una entidad bancaria, se usen únicamente para los propósitos para los que fueron creados y dentro del marco previsto.

La seguridad informática se resume, por lo general, en tres objetivos principales:

- Integridad: garantizar que los datos sean los que se supone que son.
- Confidencialidad: asegurar que sólo los individuos autorizados tengan acceso a los recursos que se intercambian.
- Disponibilidad: garantizar el correcto funcionamiento de los sistemas de información.

2.2.5.2.1 Integridad.

La verificación de la integridad de los datos consiste en determinar si se han alterado los datos durante la transmisión (accidental o intencionalmente).

2.2.5.2.2 Confidencialidad.

La confidencialidad consiste en hacer que la información sea incomprensible para aquellos individuos ajenos o que no estén involucrados en la operación.

2.2.5.2.3 Disponibilidad.

El objetivo de la disponibilidad es garantizar el acceso a un servicio o a los recursos.

2.2.5.3 Política de Seguridad.

La seguridad de los sistemas informáticos generalmente se concentra en garantizar el derecho a acceder a datos y recursos del sistema configurando los mecanismos de autentificación y control que aseguran que los usuarios de estos recursos sólo posean los derechos que se les han otorgado.

Estos mecanismos de seguridad pueden causar inconvenientes a los usuarios, ya que con frecuencia, las instrucciones y las reglas se vuelven cada vez más complicadas a medida que la red crece.

Por lo tanto la seguridad informática debe estudiarse de modo que no evite que los usuarios desarrollen usos necesarios y así puedan utilizar los sistemas de información en forma segura.

2.2.5.3.1 Cómo implementar una política de seguridad.

Uno de los primeros pasos que debe dar una entidad bancaria es definir una política de seguridad que pueda implementar de acurdo con las siguientes cuatro etapas:

- Identificar las necesidades de seguridad y los riesgos informáticos que enfrenta la compañía así como sus posibles consecuencias.

- Proporcionar una perspectiva general de las reglas y los procedimientos que deben implementarse para afrontar los riesgos identificados en los diferentes departamentos de la organización.

- Controlar y detectar las vulnerabilidades del sistema de información, y mantenerse informado acerca de las falencias en las aplicaciones y en los materiales que se usan.

- Definir las acciones a realizar y las personas a contactar en caso de detectar una amenaza.

La política de seguridad comprende todas las reglas de seguridad que sigue una organización, por lo tanto la administración de la entidad bancaria debe encargarse de definirla, ya que afecta a todos los usuarios del sistema.

En este sentido, no son sólo los administradores de informática los encargados de definir los derechos de acceso sino sus superiores. El rol de un administrador de informática es el de asegurar que los recursos de informática y los derechos de acceso a estos recursos coincidan con la política de seguridad definida por la organización.

El administrador es la única persona que conoce el sistema perfectamente, por consiguiente deberá proporcionar información acerca de la seguridad a sus superiores, además de aconsejar a quienes toman las decisiones con respecto a las estrategias que deben implementarse, y de esta manera constituir el punto de entrada de las comunicaciones destinadas a los usuarios en relación con los problemas y las recomendaciones de seguridad.

La seguridad informática de una entidad bancaria depende de que los empleados (usuarios) y clientes estén bien informados y se capaciten.

Sin embargo, la seguridad debe ir más allá del conocimiento de los usuarios y cubrir las siguientes áreas:

- Un mecanismo de seguridad física y lógica que se adapte a las necesidades de la compañía y al uso de los empleados.
- Un procedimiento para administrar las actualizaciones.
- Una estrategia de realización de copias de seguridad (backup) planificada adecuadamente.
- Un plan de recuperación luego de un incidente.
- Un sistema documentado actualizado.

(Introducción a la seguridad informática, 2012)

2.3 Marco Legal.

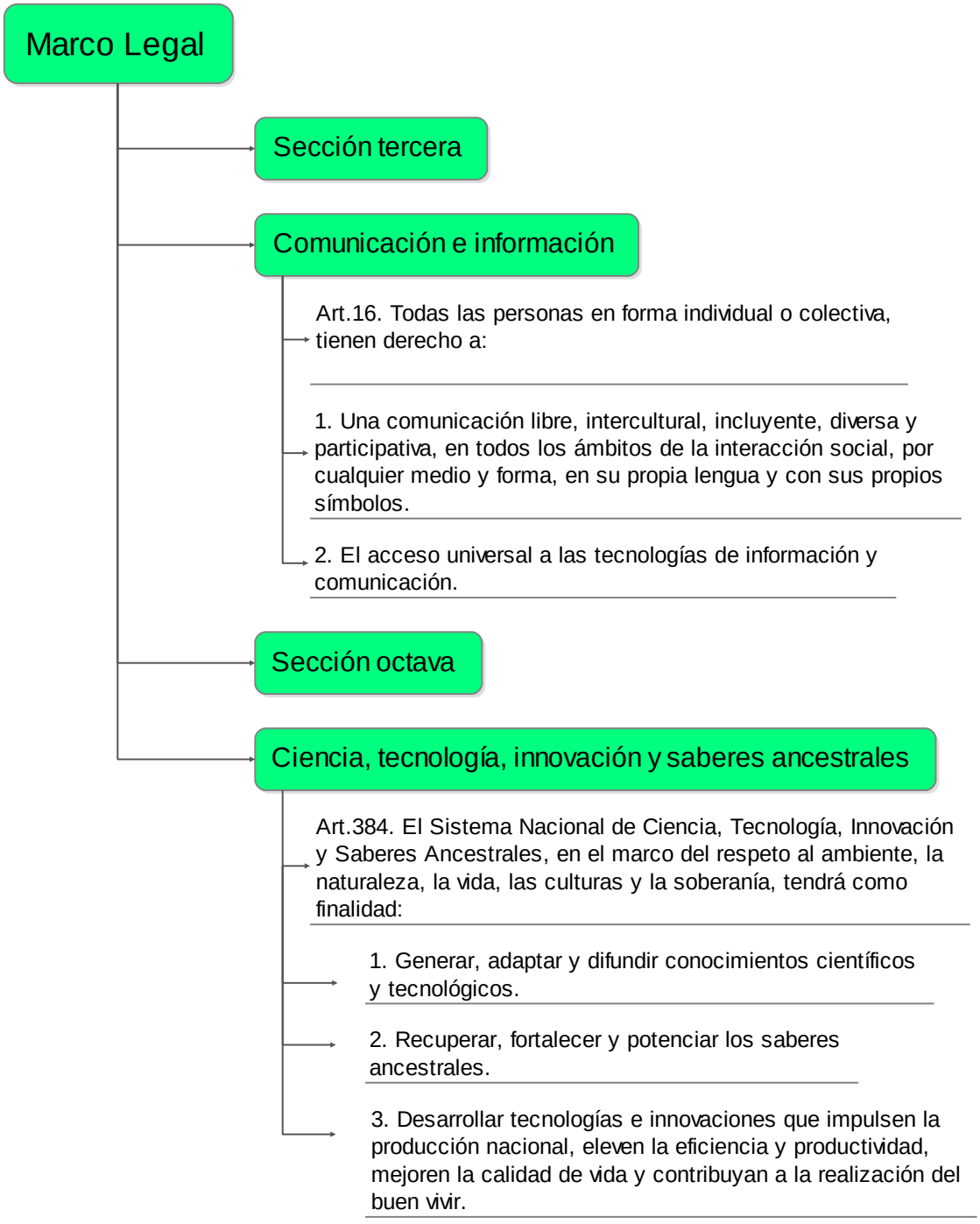


Figura 7 Marco Legal.

Fuente:**http://es.scribd.com/doc/49795915/128/Seccion**-octava-Ciencia-tecnologia innovación y saberes ancestrales.

2.4 Marco Espacial.

Información:

Título: IMPLEMENTACIÓN DE UN PLAN DE SEGURIDADES CONTRA EL PHISHING EN LA COOPERATIVA DE AHORRO Y CREDITO COOPERCO.

Agencia Bancaria: COOPERATIVA DE AHORRO Y CREDITO CCOPERCO.

Ubicación: Agencia Baguanchi.

Tiempo estimado:

- Fecha de Inicio: Diciembre 2012.
- Fecha de Finalización: Enero 2013.

Capitulo III

3. Metodología.

3.1 Proceso de Investigación.

3.1.1 Unidad de Análisis.

En la COOPERATIVA DE AHORRO Y CREDITO COOPERCO se implementara en un futuro próximo la virtualización para hacer más fáciles las tareas de transacciones bancarias o consultas de sus clientes, por lo que se presentan barias propuestas entre ellas un plan de seguridades contra el phishing, ya que este mal en la actualidad se habla mucho de las páginas web fraudulentas y por consiguiente crea inseguridad en los clientes de las agencias bancarias.

3.1.2 Tipo de Investigación.

Utilizaremos la Investigación Explicativa, ya que determinaremos los orígenes del phishing y los daños que causan estos a las agencias bancarias.

3.1.3 Método.

Utilizaremos el Método Inductivo, ya que se analizara los problemas que tienen los clientes al consultar la página web de su agencia bancaria, y se analizara las posibles soluciones.

3.1.4 Técnica.

Se utilizara la técnica de observación directa en el transcurso de la investigación, de la importancia de la Implementación de un plan de seguridades contra el Phishing en la COOPERATIVA DE AHORRO Y CREDITO COOPERCO.

3.1.5 Instrumento.

Se enlistara las deficiencias de los usuarios de información sobre la inseguridad que tienen y así basarnos para la construcción del plan de seguridades contra el Phishing.

Capitulo IV.

4. Desarrollo.

4.1 INICIO.

4.1.1 Cómo funciona la banca electrónica.

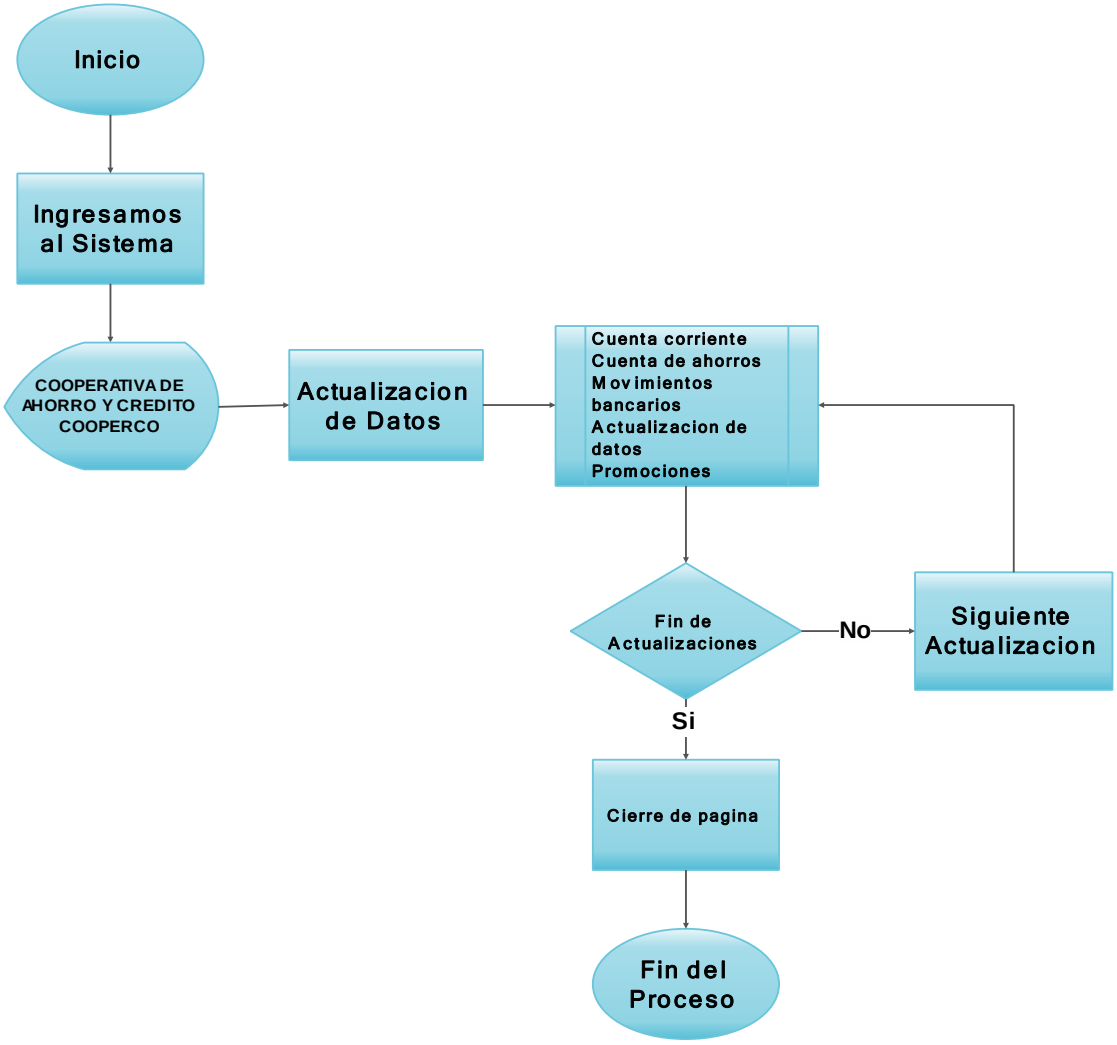


Figura 8 Diagrama del Proceso.

4.1.2 Definición del Proceso.

La banca electrónica1 (o banca en Internet) puede definirse como el conjunto de productos y procesos que permiten, mediante procedimientos informáticos, que el cliente pueda realizar una serie, cada vez más amplia, de transacciones bancarias sin necesidad de ir a la sucursal. (Como funciona la banca electronica, 2010)

4.1.2.1 Documento Visión.

El Problema.	Ataque phishing, inseguridad al acceder a la banca electrónica de la cooperativa.
Perjudicados.	Cooperativa de ahorro y crédito COOPERCO y los usuarios.
Impacto.	Pérdida de clientes, entidad bancaria mal posesionada.
Solución.	Implementar un plan contra el phishing.

Tabla 2 Problemática.

4.1.3 Qué es el phishing

El Phishing es un fraude a una entidad bancaria a través del Internet y consiste en el envío de correos electrónicos que simulan ser de empresas importantes como bancos, financieras, negocios donde se realizan pagos y compras en línea, etc. Estos correos incluyen supuestas actualizaciones, promociones o beneficios en nombre de una empresa con el fin de cometer delitos como robo de identidad, extracción de dinero, entre otros. (¿Qué es el Phishing, cómo funciona y cómo evitarlo?, 2012)

4.1.3.1 Función del phishing.

El Phishing funciona mediante mensaje electrónico y este es enviado a cientos hasta miles direcciones de correo electrónico de Internet como el defraudador puede obtener, haciéndose pasar por una entidad bancaria, un servicio de pagos en línea, un minorista en línea, o similar.

El correo electrónico enviado solicita que el destinatario actualice o verifique su información personal y financiera, incluyendo la fecha de nacimiento, la información de conexión, los detalles de cuentas, los números de la tarjeta de crédito, los números de identificación personal, etc.

Algunos mensajes electrónicos incluyen una amenaza de que si no se actualiza o se valida causará, por ejemplo, que la cuenta sea congelada. El objetivo es inducir a destinatarios confiados, que resultan ser los clientes de la organización legítima que ha sido imitada, a responder al correo electrónico y proporcionar la información solicitada.

El correo electrónico contendrá un enlace que le llevará a un sitio web muy parecido a la entidad bancaria, o al menos muy similar, en algunos casos, cuando el enlace en el correo electrónico es pulsada, el sitio genuino es accedido, pero es cubierto con una ventana más pequeña con el sitio falso, haciéndolo más creíble. Pulsar sobre un enlace también puede descargar en tu PC software malicioso, conocido como [6]"spyware", que registrará tu uso del Internet y reenviará esta información, y posiblemente un registro de lo que hayas tecleado, al defraudador. El defraudador usará esta información financiera para comprometer cuentas bancarias, tarjetas de crédito, etc.

Nunca respondas a mensajes de correo electrónico que requieran información personal o financiera, y nunca pulses un enlace en ese tipo de correos. Las entidades bancarias

[6] Spyware.- Spyware es un software que ayuda en la recopilación de información sobre una persona u organización sin su conocimiento y que pueda enviar esa información a otra entidad sin el consentimiento del consumidor, o que afirma el control de un ordenador sin el conocimiento del consumidor.

nunca envían mensajes de correo solicitando o pidiendo a sus clientes actualizar o verificar sus detalles personales y de seguridad.

Si tienes duda respecto a la legitimidad del correo, o si crees que has sido víctima de un engaño de Phishing, debes contactar inmediatamente a la organización de la que se trate. Sin embargo, debes tener cuidado en utilizar el método acostumbrado con el que contactas a esta organización, en lugar de usar cualquier sugerencia incluida en el correo o respondiendo a éste. (Engaños de Phishing., 2011)

Figura 9 Como funciona el phishing a través del correo electrónico.

Fuente:**https://www.paypal.com/es/webapps/mpp/security/general-understandphishing**.

4.1.4 Objetivo del Sistema.

Implementación de un plan de seguridades contra el phishing en la COOPERATIVA DE AHORRO Y CREDITO COOPERCO.

4.1.5 Actores y Responsables.

Actores	**Responsabilidad**
Usuarios	Capacitación para un buen manejo de la banca por internet.
Gerente General	Aprobación de la implementación del plan.
Tec. Sistemas	Recopilación de información y diseño del plan.

Tabla 3 Actores y responsabilidades.

4.1.6 Requerimientos funcionales de la cooperativa.

Conexión de Internet	Para establecer la conexión entre su computador personal y el servidor del Banco.
Navegador de internet	Internet Explorer 5.0 o mayor, con nivel de cifrado de 128 bits.
Resolución de video	800*600 píxeles con 256 colores es la recomendada para una mejor visualización del servicio, ideal en 1024 * 768.
Sistema operativo	Windows 95, 98, NT, Milenium y XP.

Tabla 4 Requerimientos.

4.1.6.1 Modo de operación.

El modo de operación de la banca electrónica es en línea con el servidor del Banco, para tal efecto cuenta con un sistema que permite acceder la base de datos de la entidad tanto para solicitar información como para ordenar operaciones bancarias. El tiempo de conexión o utilización se verá reducido al tiempo que se requiera para transferir información en cualquier sentido y dependerá del volumen de información (número de transacciones u operaciones) y de la velocidad de transferencia que permita su canal dedicado a internet.

4.1.6.2 Requerimientos de Acceso al Sistema.

Los requerimientos mínimos para poder acceder a los servicios y funcionalidades del sistema de administración de seguridad y usuarios son: ser un usuario administrador preparador, administrador aprobador o el súper-usuario para la agencia bancaria afiliada al servicio.

Adicionalmente contar con:

- Número de Afiliación de la COOPERATIVA.
- Identificación de Usuario.
- Clave
- Un browser que soporte encriptación de 128 bits y html 4.2.

Todos los usuarios del sistema accederán al sistema a través de una única pantalla de ingreso de la COOPERATIVA DE AHORRO Y CREDITO COOPERCO.

Luego de que el usuario ha sido autenticado positivamente, el sistema presentará al usuario la página principal en la cual realizara sus actualizaciones.

4.1.7 Interacción con la Banca electrónica.

Ingresar al sistema.

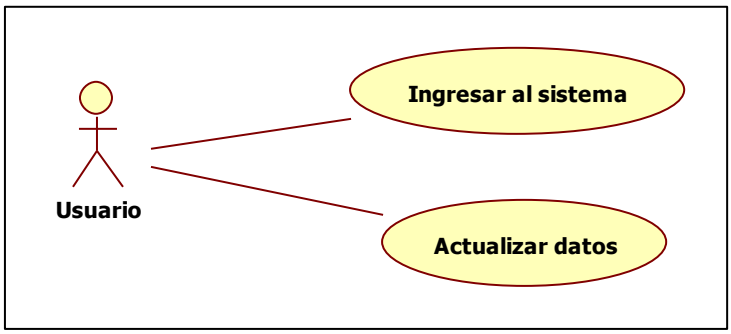


Figura 10 Caso de uso ingresar al sistema y actualizar datos.

Breve descripción. **En el caso de uso Ingresar al sistema y actualizar datos permite a los usuarios ingresar a la banca electrónica y actualizar datos.**
Descripción paso por paso: 1. El usuario ingresa al sistema de la cooperativa. 2. El usuario actualiza las cuentas.

Tabla 5 Descripción ingresar al sistema y actualizar datos.

Ingresar y actualizar clave.

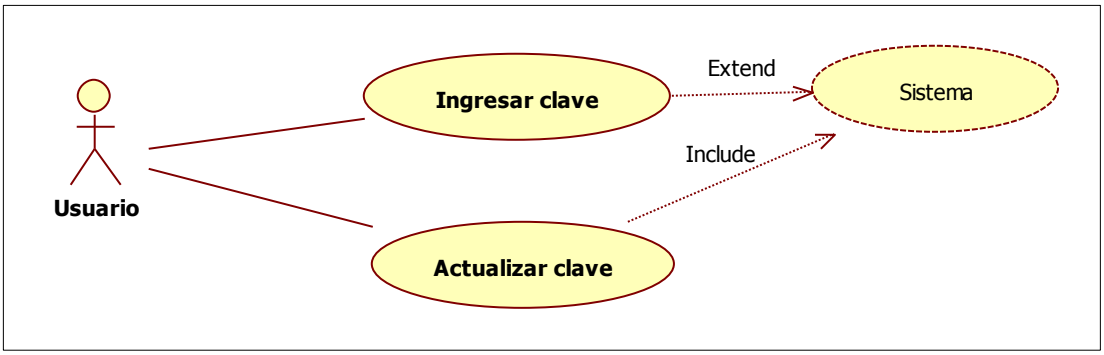


Figura 11 Caso de uso ingresar y actualizar clave.

Breve descripción. **En el caso de uso Ingresar y actualizar clave permite a los usuarios ingresar a la banca electrónica con su clave de acceso y actualizarla.**
Descripción paso por paso: 1. El usuario ingresa al sistema de la cooperativa ingresando su clave. 2. El usuario cambia de clave la actualiza.

Tabla 6 Descripción ingresar y actualizar clave.

Actualizaciones bancarias.

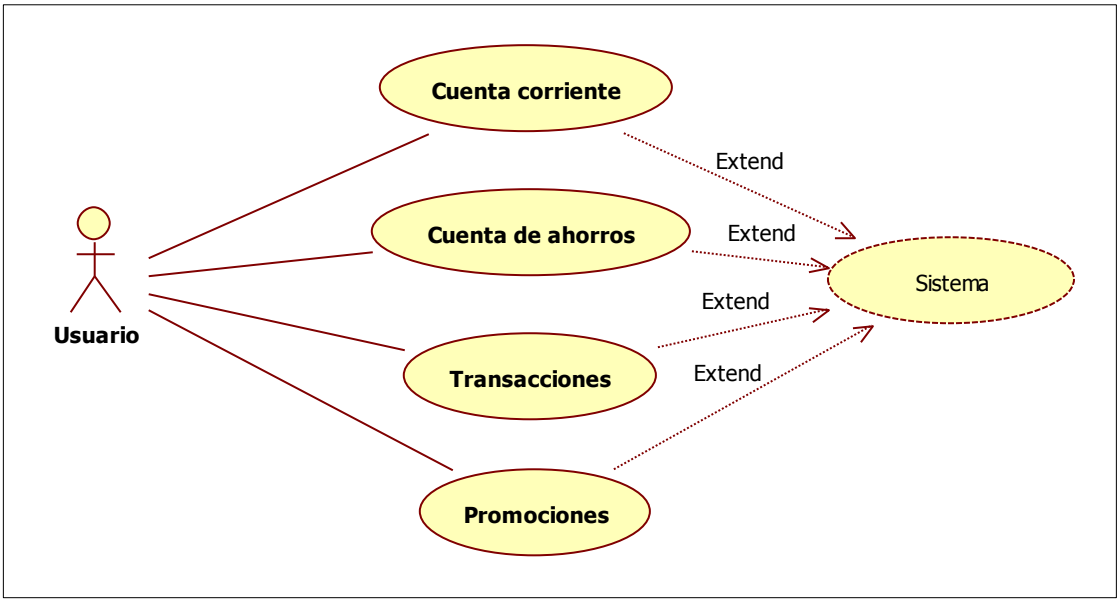


Figura 12 Consulta de saldos y transacciones.

Breve descripción. **En el caso de uso actualizaciones bancarias permite a los usuarios ingresar al sistema de la banca electrónica y actualizarla.**
Descripción paso por paso: 1. El usuario ingresa al sistema de la cooperativa y actualiza su cuenta corriente. 2. El usuario ingresa al sistema de la cooperativa y actualiza su cuenta de ahorros. 3. El usuario ingresa al sistema de la cooperativa y realiza transacciones bancarias. 4. El usuario ingresa al sistema de la cooperativa y se informa de las promociones.

Tabla 7 Descripción actualizaciones bancarias.

4.1.8 Diagrama de acitividades del negocio.

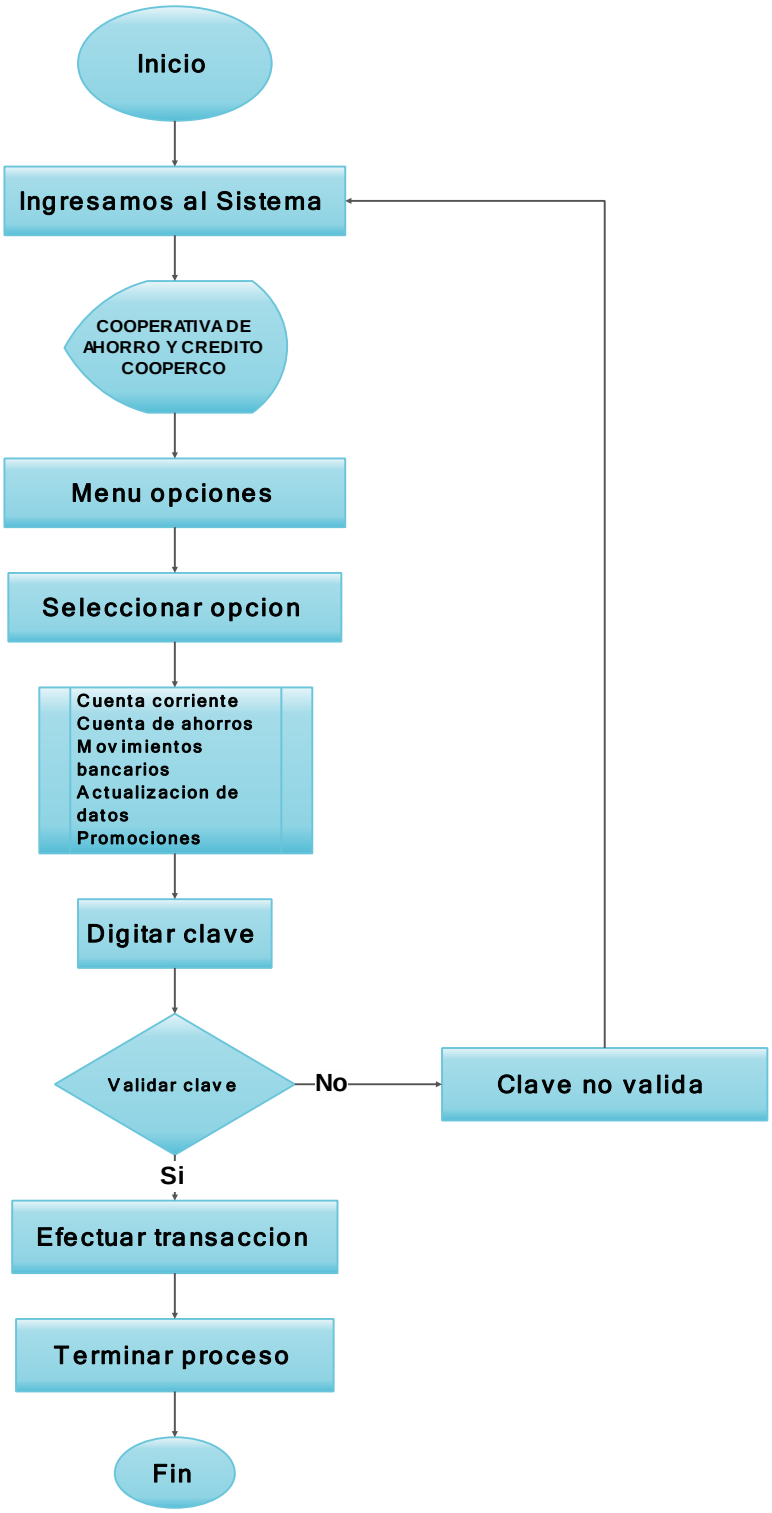


Figura 13 Diagrama de actividades.

4.1.9 Analisis de Riesgos.

Robos	Fraude.
	Robo de informacion.
Fallas de Hardware	Falla de la tarjeta principal (mainboard).
	Falla de tarjeta de red.
	Falla de disco duro.
Fallas de Software	Fallas del sistema operativo.
	Fallas de la base de datos.
Errores humanos	Perdidas de claves de acceso.
	Borrados de datos.
Accesos no autorizados	Accesos fisicos no autorizados.
	Accesos logicos no autorizados a la red, a la BD, etc.
Malvare informatico	Infecciones de virus informatico, spam, phishing, etc.
Vandalismo informatico	Borrado de informacion.

Tabla 8 Análisis de riesgos.

4.1.10 Analisis de phishing.

4.1.10.1 Caracterización y consideraciones sobre el phishing.

El phishing puede definirse como una forma de actividad delictiva/criminal que utiliza técnicas de ingeniería social y se caracteriza por intentar adquirir información sensible de forma fraudulenta, como contraseñas, números o detalles de tarjetas de crédito, información personal privada, etc. suplantando a una persona o negocio/institución de confianza en una comunicación electrónica aparentemente

oficial como el correo electrónico (SMTP/POP3/IMAP4), la mensajería instantánea (IM/MSN/ICQ), la Web (HTTP/HTTPS), la telefonía (fija, móvil, basada en VoIP/SIP, SMS, MMS), etc.

El phishing se ha convertido en un problema de seguridad de muy elevado crecimiento y los ataques van siendo cada día más sofisticados. En un ataque básico, la víctima recibe un correo electrónico que parece venir de una institución confiable, frecuentemente le informa de algún tipo de problema que tiene la cuenta de la víctima (saturación inminente de la memoria de recepción de mensajes del correo electrónico, caducidad de la contraseña utilizada, posible violación de su cuenta o tarjeta de crédito, detección de intrusos en su vivienda protegida por empresa proveedora de servicios anti-robo, alerta en su centro sanitario, etc.) y le exige una acción inmediata.

La víctima utilizando un link malicioso se dirige al sitio Web que imita perfectamente al de la institución confiable que suplanta y le muestra una pantalla para que introduzca su nombre de usuario, contraseñas, información personal, etc.

Existen dos variantes:

Pasiva.- El atacante recoge la información de la víctima para una posterior explotación o para venderla a terceros.

Activa.- El atacante retransmite la información de la víctima a la institución real y saquea la cuenta de la víctima en tiempo real.

El phishing puede estar basado en correo electrónico (SMTP/POP3/IMAP4, VoIP), Web (HTTP/HTTPS, Webmail, Redes Sociales), telefonía fija/móvil, SMS/MMS, etc. El phishing puede servir para el robo de identidad (personal o institucional),

donde la identidad digital puede hacer referencia a una persona física, a una persona jurídica (empresa, institución, etc.) o a una máquina de computación/autómata programable en un entorno industrial o infraestructura crítica. La identidad digital es un conjunto de atributos algunos de los cuales pueden cambiar con el tiempo y otros pueden ser certificados por terceras partes; por ejemplo nombre y apellidos, edad, DNI, identificadores de usuario, información médica, medios de autenticación (tradicional o federada), etc.). Dado que es muy difícil, por no decir imposible borrar los datos digitales utilizados, las identidades digitales tienden a crecer y nunca se reducen.

(Bertolín, 2011)

4.2 Elaboración.

4.2.1 Definicion de actores y perfiles.

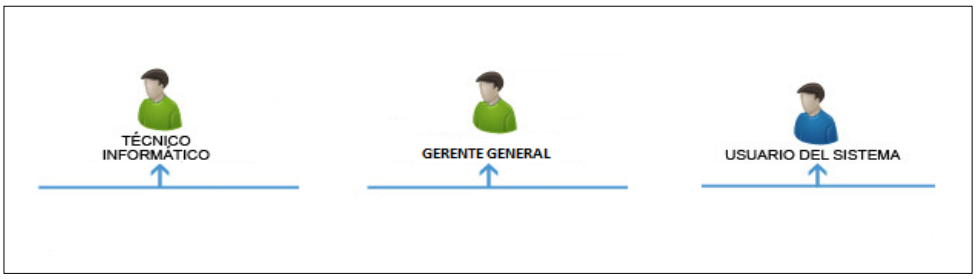


Figura 14 Actores y Perfiles.

Actor	Responsabilidad	Actividad
Técnico informático	Diseñar el plan de seguridades.	Investigar posibles ataques phishing, y diseñar un plan de seguridades.
Gerente financiero	Administrar y canalizar los recursos financieros y lograr niveles óptimos de rentabilidad.	Toma de decisiones. Aprobación del plan.
Usuario del sistema	Manejo seguro de la banca electrónica.	

Tabla 9 Definición de actores y perfiles.

4.2.1.1 Modelo del Sistema.

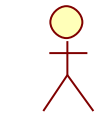
	Responsabilidades.
 Tecnico Inf.	• Asegurar el buen funcionamiento de los sistemas informáticos de cómputo tanto físico como lógico. • Protección de la red. • Realizar pruebas. • Identificar las técnicas que los phishers utilizan para estafar a los clientes de las agencias bancarias. • Definir que antivirus utilizar contra spam. • Creación de claves seguras y cambios de las mismas. • Creación de respaldos. • Crear nuevas políticas.

Tabla 10 Responsabilidades del técnico informático.

	Responsabilidades.
 **Gerente**	• Gestionar y disponer de los recursos financieros necesarios para alcanzar los objetivos generales, optimizando su rendimiento, a través de la negociación de las condiciones más beneficiosas que puedan obtenerse de bancos y entidades financieras. • Tomar decisiones sobre implementaciones y procedimientos.

Tabla 11 Responsabilidades del Gerente Financiero.

	Responsabilidades.
 **Usuario**	• Asegurar que los equipos cuenten con todas las características necesarias para un correcto funcionamiento y de recibir mantenimiento constante. • Disponer de un buen anti-virus y actualizarlo constantemente. • Determinar la legitimidad de los correos electrónicos. • Revisar el dominio del correo electrónico. • Cuidarse de los archivos adjuntos. • No rellenar campos de información dentro del correo electrónico. • Controlar el protocolo SSL de la página web. • Nunca entregar información de la tarjeta de crédito, contraseñas de cuentas o demasiada información personal en un correo electrónico. • Acogerse al plan de acción implementada por la cooperativa.

Tabla 12 Responsabilidades del Usuario.

4.2.2 Casos de uso del sistema.

4.2.2.1 Asegurar los sistemas informáticos de cómputo tanto físico como lógico.

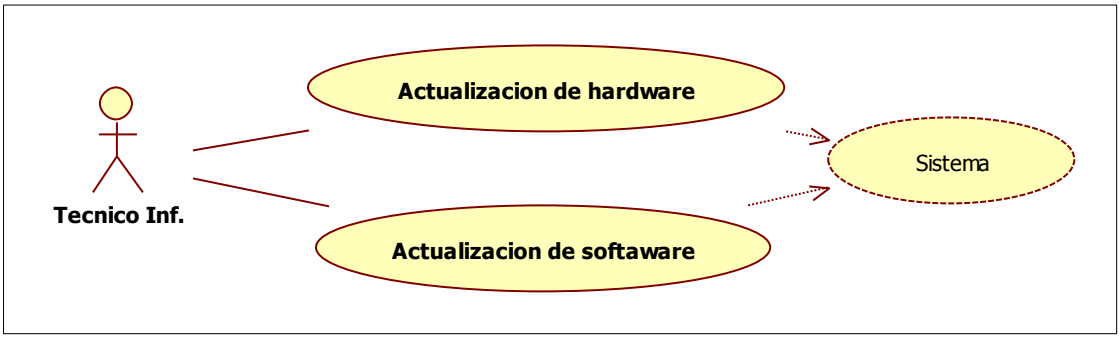


Figura 15 Seguridad física y lógica.

4.2.2.2 Protección de la red.

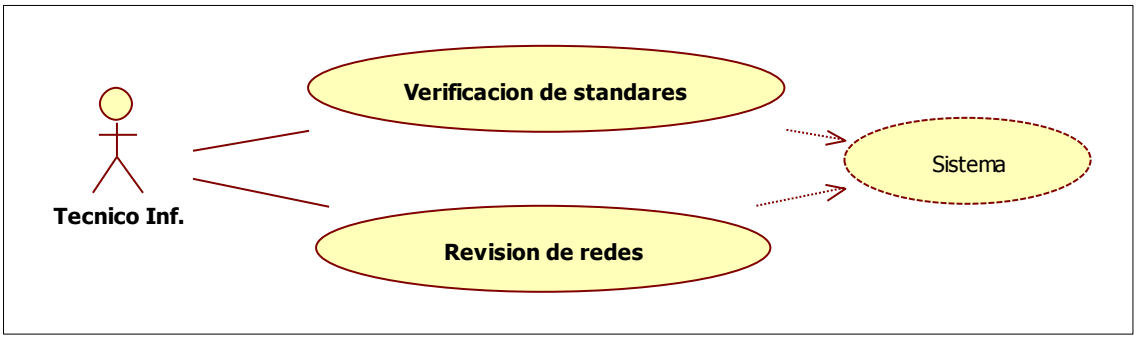


Figura 16 Revisión de redes.

4.2.2.3 Realizar pruebas.

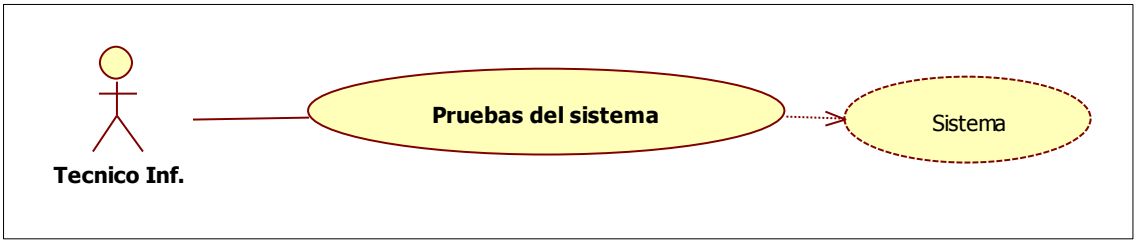


Figura 17 Pruebas del sistema.

4.2.2.4 Identificar las técnicas que los phishers utilizan para estafar a los clientes de las agencias bancarias.

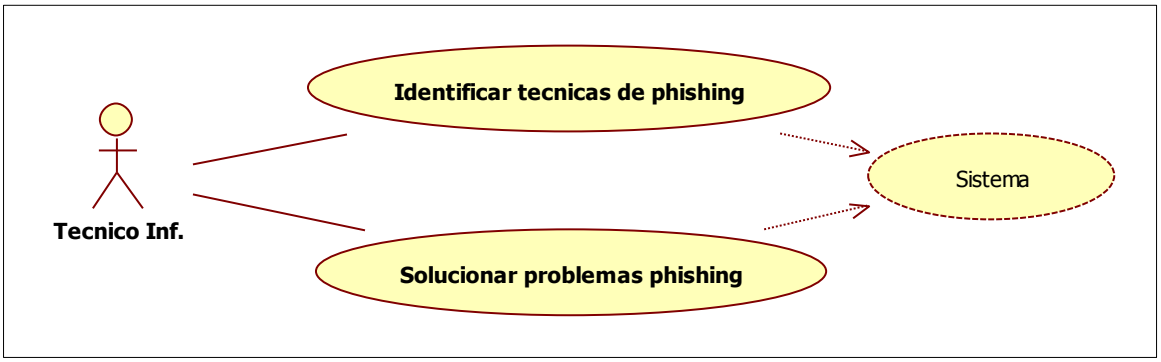


Figura 18 Técnicas phishing.

4.2.2.5 Definir que antivirus utilizar contra spam, phishing scam, troyano informático, spyware, bot e instalarlos.

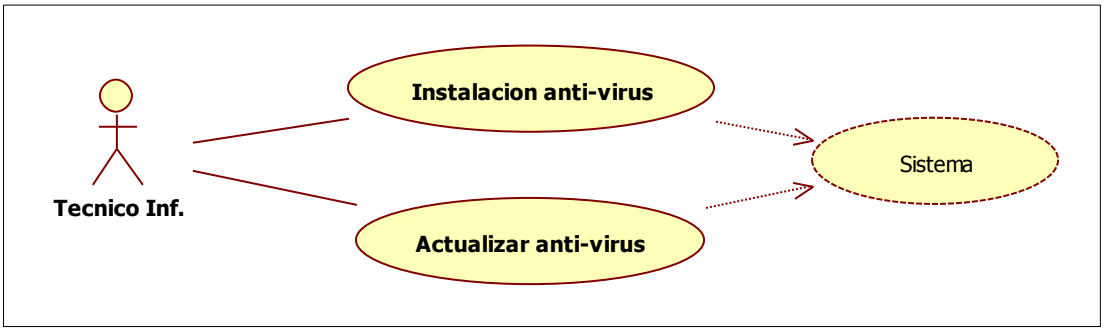


Figura 19 Instalación y actualización de antivirus.

4.2.2.6 Creación de claves seguras y cambios de las mismas.

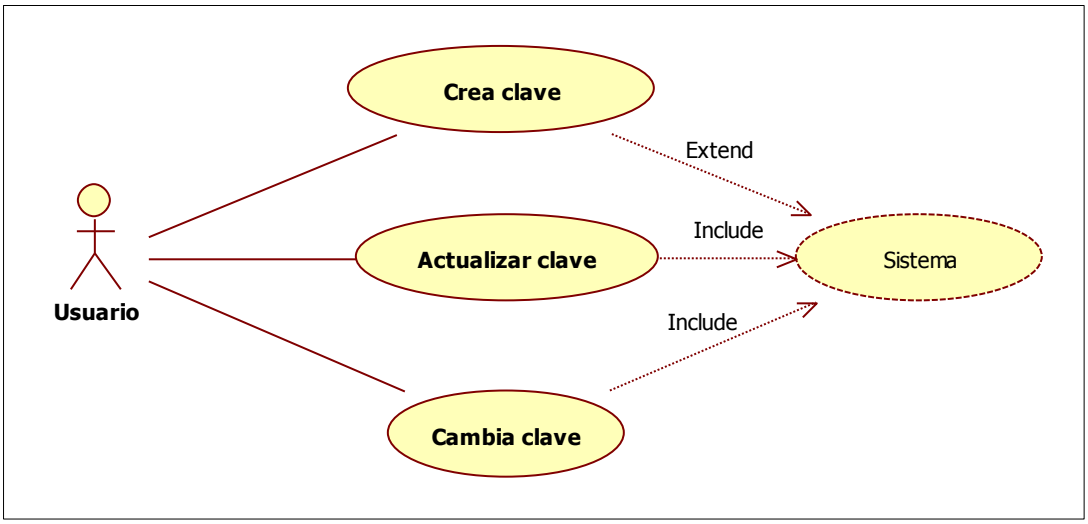


Figura 20 Creación y cambios de clave.

4.2.2.7 Creación de respaldos.

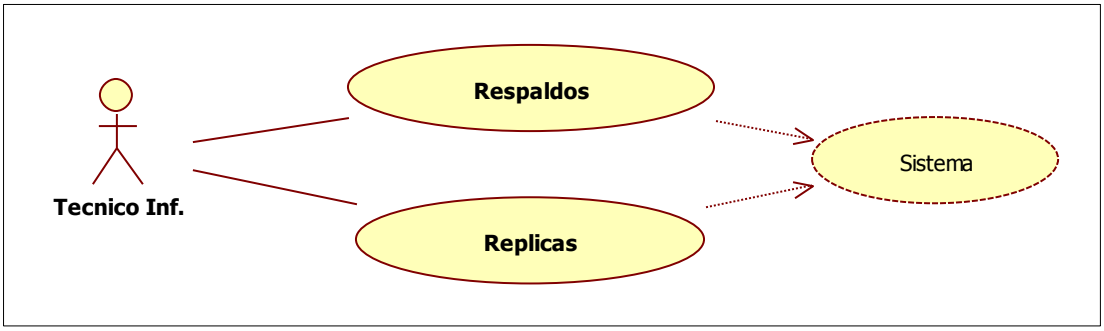


Figura 21 Respaldos.

4.2.2.8 Crear nuevas políticas.

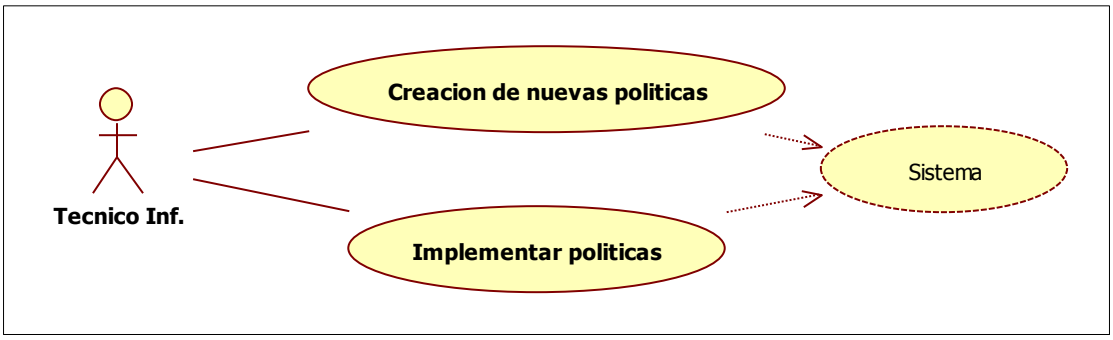


Figura 22 Nuevas políticas.

4.2.3 Cronograma de Actividades.

Nombre de tarea	Duración	Comienzo	Fin	Responsable	Actividad
Fase 1	**14 días**	**lun 28/01/13**	**jue 14/02/13**		
Funcionamiento de los sistemas informáticos.	10 días	lun 28/01/13	vie 08/02/13	Tec. Informático	Asegurar el buen funcionamiento de los sistemas informáticos de cómputo, hardware y software
Protección de la red.	4 días	lun 11/02/13	jue 14/02/13	Tec. Redes	Revisión de las redes que estén en buen estado
Fin fase 1	0 días	jue 14/02/13	jue 14/02/13		
Fase 2	**8 días**	**vie 15/02/13**	**mar 26/02/13**		
Identificar las técnicas phishers	5 días	vie 15/02/13	jue 21/02/13	Tec. Informático	Identificar las técnicas que los phishers utilizan para estafar
Definir que antivirus utilizar contra spam.	3 días	vie 22/02/13	mar 26/02/13	Tec. Informático	Actualizara los antivirus y los pondrá a prueba
Fin fase 2	0 días	mar 26/02/13	mar 26/02/13		
Fase 3	**4 días**	**mié 27/02/13**	**lun 04/03/13**		
Creación de claves seguras y cambios de las mismas.	2 días	mié 27/02/13	jue 28/02/13	Jefes financieros	Definirá e implementara técnicas de creación de claves seguras
Creación de respaldos.	2 días	vie 01/03/13	lun 04/03/13	DBA	Definir técnicas de respaldos seguros y replicas
Fin fase 3	0 días	lun 04/03/13	lun 04/03/13		
Fase 4	**5 días**	**mar 05/03/13**	**lun 11/03/13**		
Crear nuevas políticas.	5 días	mar 05/03/13	lun 11/03/13	Departamento de Sistemas	Debatir nuevas políticas del manejo de la banca electrónica e implementarlas
Fin fase 4	0 días	lun 11/03/13	lun 11/03/13		

Tabla 13 Cronograma de actividades.

4.2.4 Arquitectura Propuesta.

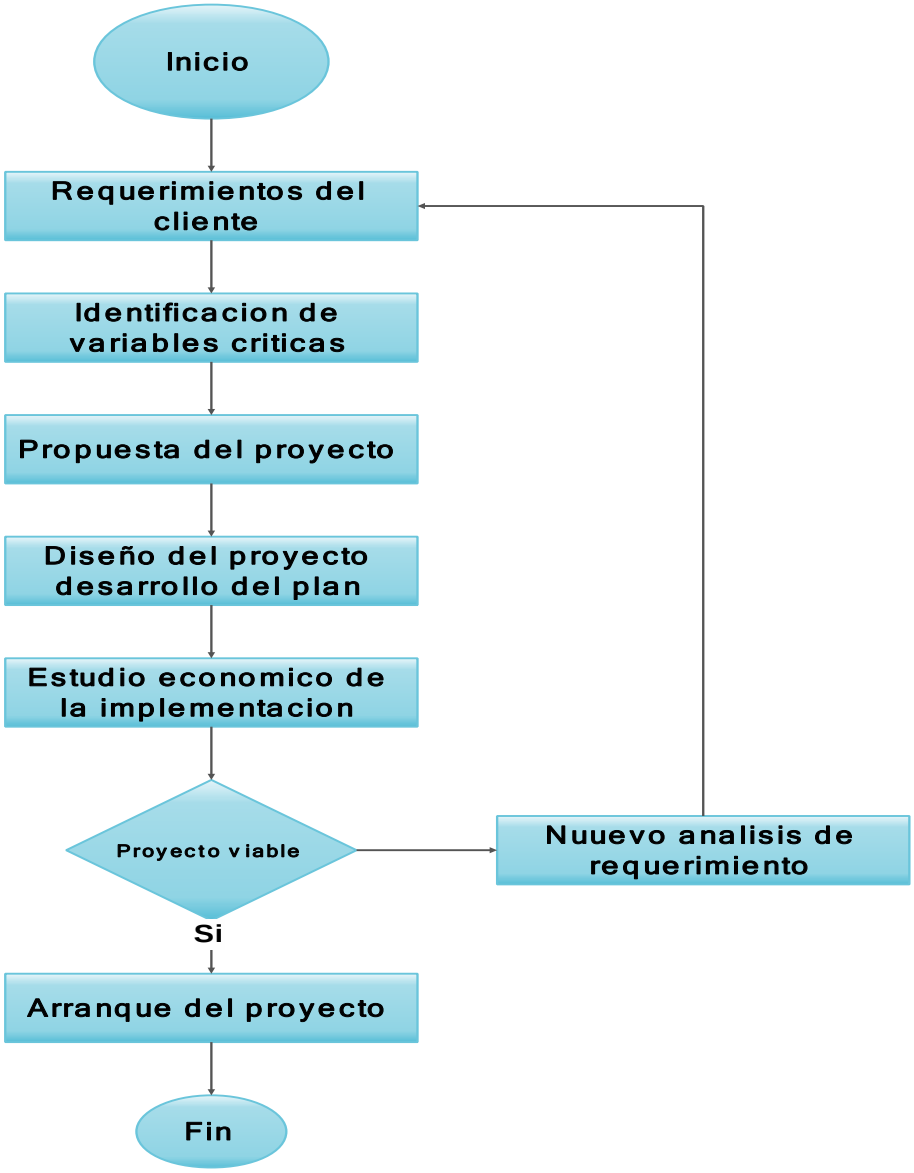


Figura 23 Arquitectura Propuesta.

4.3 Construcción.

4.3.1 Asegurar los sistemas informáticos de cómputo tanto físico como lógico.

Hardware	• Fallas en el disco duro que podría ocasionar perdida de la información, se configura sistemas de backups periódicos.
Software	• Frente a los fallos de software, se implementa la reinstalación del software o reconfiguración, todo el software cuanta con copias de seguridad.
Mantenimiento de redes	• Realizar un buen diseño inicial, estudio exhaustivo previo de posibles fuentes de interferencias externas con otras redes e internas para minimizar su impacto. • Análisis de cobertura, potencia de señal y planificación de frecuencias para conseguir una buena recepción interna y reducir su emisión externa, estimaciones adecuadas de uso, etc. • Mantenimiento interno periódico para detectar degradaciones, saturación, intrusiones. • Ejecutar la adecuada actualización de drivers y firmware, reparaciones, análisis de las causas de interferencias o degradaciones detectadas, planificación del crecimiento y ejecutar ampliación de la red. • Una red adecuadamente implantada y mantenida puede generar gran satisfacción a sus usuarios, incrementar la productividad y reducir costes.

Tabla 14 Sistemas informáticos en buen estado.

4.3.2 Identificar las técnicas que los phishers utilizan para estafar a los clientes de las agencias bancarias.

Spam	• Es el hecho de enviar mensajes electrónicos no solicitados y en cantidades masivas. • Considerado por varias entidades como uno de los principales problemas sociales al que tienen que hacer frente los medios electrónicos hoy en día. • El recibo de correo por la red cuesta dinero al usuario que lo recibe, tanto en la conexión como en el uso de la red misma.
Phishing scam	• Una de los fraudes más comunes y peligrosos hoy día. • Es realizado por medio de e-mails que aparentan venir de fuentes legítimas, como bancos, empresas conocidas, universidades, tiendas, u otras. • Estos piden que usted haga click en algún link o ingrese a determinado sitio web para "actualizar" sus datos o participar de alguna promoción. • El objetivo es robar sus datos bancarios.
Troyano informático.	• A primera vista el troyano parece ser un programa útil, pero en realidad hará daño una vez instalado o ejecutado en tu ordenador. • Los que reciben un troyano normalmente son engañados a abrirlos porque creen que han recibido un programa legítimo o archivos de procedencia segura. • Algunos troyanos se diseñan para ser más molestos que

	malévolos. • Otros pueden causar daño serio, suprimiendo archivos y destruyendo información de tu sistema. • Crear puertas traseras o backdoors en tu ordenador permitiendo el acceso de usuarios malévolo a tu sistema, accediendo a tu información confidencial o personal.
Spyware **Definición.**	• Es un software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador. • Estos productos, realizan diferentes funciones, como mostrar anuncios no solicitados, recopilar información privada, redirigir solicitudes de páginas e instalar marcadores de teléfono. • Un spyware típico se auto instala en el sistema afectado de forma que se ejecuta cada vez que se pone en marcha el ordenador (utilizando CPU y memoria RAM, reduciendo la estabilidad del ordenador), y funciona todo el tiempo, controlando el uso que se hace de Internet y mostrando anuncios relacionados.
Bot.	• Es un tipo de programa malicioso que permite a un atacante tomar el control de un equipo infectado. • Por lo general, los bots, también conocidos como "robots web" son parte de una red de máquinas infectadas, conocidas

	como “botnet”, que comúnmente está compuesta por máquinas víctimas de todo el mundo. • Debido a que un equipo infectado por bots cumple las órdenes de su amo, muchas personas se refieren a estos equipos víctima como “zombis” • Los delincuentes cibernéticos que controlan estos bots son cada vez más numerosos. • Algunos botnets pueden englobar cientos o un par de miles de equipos, pero otros cuentan con decenas e incluso centenares de miles de zombis a su servicio. • Muchos de estos equipos se infectan sin que sus dueños se enteren. • Los bots se introducen sigilosamente en el equipo de una persona de muchas maneras. • Los bots suelen propagarse por Internet en busca de equipos vulnerables y desprotegidos a los que puedan infectar. • Su objetivo es permanecer ocultos hasta que se les indique que realicen una tarea.

Tabla 15 Técnicas phishing.

4.3.3 Disponer de un antivirus seleccionando el más adecuado contra spam, phishing scam, troyano informático, spyware, bot e instalarlos.

Kaspersky.	• Los servidores y estaciones cuentan con licencia corporativa del anti-virus Kaspersky durante un año.
ESET NOD32.	• Incorporando múltiples novedades como un motor nuevo de análisis y desinfección, que es más rápido y efectivo eliminando códigos maliciosos. • Dispone además un nuevo módulo de protección específica antirrobo y nuevas tecnologías de protección anti-phishing.

Tabla 16 Antivirus contra el phishing.

4.3.4 Creación de claves seguras y cambios de las mismas.

Creación de claves seguras y cambios de las mismas.	• Tiene ocho caracteres como mínimo. • No contiene el nombre de usuario, el nombre real o el nombre de la empresa. • No contiene una palabra completa. • Es significativamente diferente de otras contraseñas anteriores.

Tabla 17 Aseguramiento de claves.

4.3.5 Creación de respaldos.

Respaldos.	• En lo que respecta a la información se dispondrá de backups para la restauración de la información.

Tabla 18 Respaldos.

4.3.6 Crear nuevas políticas.

Políticas.	• Las nuevas políticas, normas y procedimientos de la cooperativa, deben documentarse, formalizarse y hacérseles llegar a los usuarios de la cooperativa, asegurando que estas se mantengan adecuadamente actualizadas.

Tabla 19 Nuevas políticas.

4.4 Transición.

4.4.1 Implementación.

4.4.1.1 Monitorear el Internet en busca de páginas fraudulentas phishing.

Monitorear el Internet.	• Generalmente, el sitio Web de phishing aparece en algún lugar de Internet antes del envío de los e-mails de phishing. • Dichos sitios Web simulan ser de empresas importantes como bancos, agencias financieras, negocios donde se realizan pagos y compras en línea, etc.

Tabla 20 Monitorear el Internet.

4.4.1.2 El usuario deberá confirmar si el e-mail es legítimo.

Conformar e-mail	• El usuario tendrá que identificar si el e-mail es legítimo de la cooperativa y no de un phishing. • La agencia bancaria deberá crear una política para incluir información de autenticación en los e-mails enviados por estos a los usuarios.

Tabla 21 Confirmación de usuario legítimo.

4.4.1.3 Implementar soluciones de antivirus, de filtrado de contenido y anti-spam de buena calidad.

Antivirus.	• La exploración antivirus en el gateway establece una capa de defensa más allá de la exploración antivirus en la propia máquina. • Filtre y bloquee sitios Web de Phishing conocidos en el gateway. El filtrado de spam en el gateway ayuda a los usuarios finales a evitar mensajes no deseados y e-mails de Phishing.

Tabla 22 Implementar soluciones antivirus.

4.4.1.4 Establecer políticas corporativas y divulgarlas a los socios.

Políticas.	• Cree políticas corporativas de contenido de e-mail para que no se puedan confundir los mensajes legítimos con phishing. • Divulgar dichas políticas a los socios y realizar un seguimiento.

Tabla 23 Establecer políticas.

4.4.2 Pasos que deben seguir los socios de la COOPERATIVA DE AHORRO Y CREDITO COOPERCO.

4.4.2.1 Bloquee automáticamente mensajes malintencionados o fraudulentos.

Bloquear mensajes.	• Los detectores de spam pueden ayudar a evitar que el socio tenga que abrir e-mails sospechosos.

Tabla 24 Bloquear automáticamente mensajes fraudulentos.

4.4.2.2 Detecte y excluya automáticamente los programas malintencionados.

Excluya los Programas de phishing	• Los programas espías son parte de un ataque de Phishing, pero pueden ser eliminados por muchos programas disponibles en el mercado.

Tabla 25 Excluya los programas malintencionados.

4.4.2.3 Bloquee automáticamente la salida de información confidencial a terceros.

Bloque la salida de la información.	• Aunque el socio no logre identificar visualmente el verdadero sitio Web que recibirá la información confidencial, existen productos de software que lo logran.

Tabla 26 Bloquear salida de información.

Si usted no está seguro de que un e-mail es legítimo, llame a la Cooperativa que envió el e-mail para verificar su autenticidad.

4.4.3 Medidas establecidas en la COOPERATIVA DE AHORRO Y CREDITO COOPERCO.

Los e-mails legítimos poseen hiperenlaces al sitio Web de la Cooperativa, que solicitan que los usuarios envíen información confidencial con el nombre de usuario y la contraseña.

Los phishers aprovechan dichos enlaces incorporados para llevar a los usuarios a revelar toda su información personal a los sitios Web fraudulentos.

La cooperativa no enviara correos con enlaces e incluirá enlaces no pulsables, donde el socio tenga que teclear o cortar y pegar en el navegador.

Muy probablemente, los socios regulares tendrán el enlace de la Cooperativa en su lista de sitios preferidos, facilitando aún más dicho proceso.

Figura 24 Página similar al de la agencia bancaria.

4.4.3.1 No llenar formularios dentro del correo.

Los phishers utilizan formularios que vienen en el correo electrónico para inducir que los usuarios que llenen estos con sus datos personales.

Al ser formularios idénticos al de la cooperativa, será difícil distinguirlos entre el verdadero y falso.

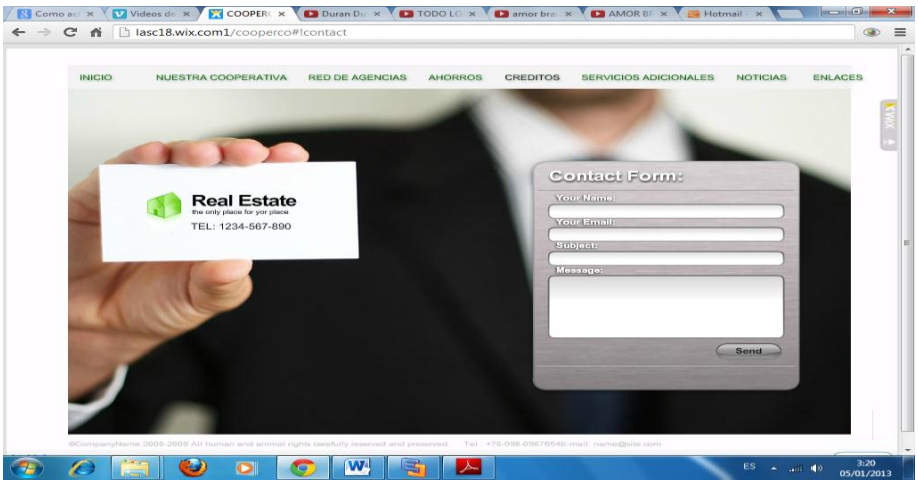


Figura 25 No rellenar formularios dentro del correo.

La Cooperativa deberá informar a los socios de que los e-mails legítimos nunca contendrán formularios solicitando información personal.

4.4.3.2 Verificar la autenticidad de los mensajes.

Los usuarios no cuentan con un medio sencillo de verificar la autenticidad de los mensajes provenientes de instituciones legítimas.

Esta solución pretende crear un mecanismo visual o sonoro para verificar la autenticidad de los e-mails. La cooperativa podría incluir una fotografía del socio en todas las comunicaciones electrónicas. Este es un método sencillo y confiable para que el socio de la Cooperativa reconozca los mensajes legítimos sin que necesite precisar instalar ningún software más en su máquina. Los socios deficientes visuales utilizarían un objeto de identificación alterno quizás una “imagen sonora” o una palabra de acceso adjuntado adecuadamente.

4.4.3.3 Incorporar el nombre de los usuarios.

Los usuarios no cuentan con un medio para verificar la autenticidad de los mensajes de la cooperativa.

Se incorporaría el nombre del socio al e-mail, por ejemplo, "Estimado Sr. Colunga".

4.4.3.4 Monitoreo activo de la Web.

El contenido de Web presente en e-mails de Phishing es obtenido desde fuentes legítimas, con URL dirigidas a fuentes ilegítimas.

Figura 26 Url Falsa.

Las empresas de servicios de monitoreo implementan soluciones que utilizan agentes para monitorear continuamente el contenido de la Web, buscando activamente todas las instancias del logotipo de un cliente, de su marca comercial o de su contenido-clave de Web.

La institución cliente presenta a la empresa proveedora del servicio de monitoreo una "lista blanca" de usuarios autorizados del logotipo, de la marca comercial y del contenido clave. Cuando los agentes detectan usuarios no autorizados de logotipos, marcas comerciales u otros contenidos de la Web, la institución cliente puede tomar medidas de resolución.

Figura 27 Url Verdadera.

4.4.4 Medidas establecidas para los socios de la COOPERATIVA DE AHORRO Y CREDITO COOPERCO.

4.4.4.1 Direcciones en Internet.

El problema es la falsificación de direcciones de Internet y técnicas de Phishing.

La nueva protección contra el fraude financiero y el robo de identidad, ha sido incorporada un filtro contra falsificaciones, que aparece en el menú de opciones de Internet, y que tiene la intención de proteger a los usuarios contra la divulgación de información privada, a terceros no autorizados, sin el correspondiente consentimiento.

Si un usuario visita un sitio falso, que parece exactamente igual que el original, por lo general después de pulsar sobre un enlace en un correo electrónico fraudulento, el navegador detecta un intento de falsificación de dirección y compara el sitio con una lista de sitios conocidos de falsificación de direcciones.

Si el filtro detecta que el sitio es culpable de falsificar la dirección, bloquea el acceso al mismo e informa al usuario del peligro de dejar su información personal en sitios como ese.

La base de datos de sitios conocidos con direcciones falsificadas, se actualiza de forma regular y los usuarios tienen la opción de informar una instancia sospechosa de falsificación a Microsoft, para una evaluación.

4.4.4.2 Filtrado anti-spam en la computadora.

No siempre los usuarios logran detectar los e-mails fraudulentos que aparentemente provienen de la Cooperativa.

Con el filtrado anti-spam se puede bloquear algunos e-mails fraudulentos antes de que logren alcanzar al consumidor.

Los e-mails de Phishing son una forma específica de spam. El usuario debe instalar un software en la computadora y configurarlo.

4.4.4.3 Antivirus y Anti-spyware.

Los programas espías interceptan invisiblemente las comunicaciones entre el socio y las instituciones financieras.

Los programas antivirus detectan muchas formas de programas malintencionados, incluso el spyware pudiendo excluirlo cuando se lo encuentre. La mayoría de los programas antivirus funciona de manera casi invisible para el usuario, afectando poco a sus operaciones normales. Los programas anti-spyware pueden explorar la computadora en busca de posibles programas espías y son capaces de eliminarlos.

Figura 28 Antivirus y Anti-spyware.

4.4.4.4 Servicio de privacidad de desktops.

Los socios pueden ser inducidos a enviar datos confidenciales a sitios Web inseguros y fraudulentos.

Existe software que puede monitorear el tráfico de la Web saliente respecto a un conjunto de datos que el usuario puede definir. Los datos definidos con mayor frecuencia son información que identifican al usuario, tales como nombre, apellido y números de tarjetas de crédito.

Si se encuentra cualquiera de dichos conjuntos de datos en uno de los paquetes enviados, el paquete se queda retenido hasta que el usuario confirme si los datos deben ser enviados al destino verdadero, o si se debe interrumpir la transmisión de los datos. Si el usuario indica que los datos no deben ser enviados, los datos confidenciales son eliminados del paquete

4.4.4.5 Teclear las direcciones de la Web y verificar su autenticidad.

Varias exploraciones pueden ocultar la verdadera dirección de Web de un enlace y redirigir el navegador a un sitio Web de Phishing.

Es más seguro teclear en el navegador la dirección de Web deseada que pulsar en enlaces incorporados. Si usted no está seguro sobre la autenticidad de un e-mail, contacte directamente con la institución remitente.

Capítulo V

5. Conclusiones y Recomendaciones.

5.1 Conclusiones.

Pudimos darnos cuenta a través de la realización de este trabajo lo importante que es la banca electrónica y que día a día las instituciones financieras deben de estar al tanto del desarrollo de nueva tecnología e implementarla.

De igual manera nos pudimos dar cuenta que siempre hay personas mal intencionadas, que con el afán de lucrarse están al acecho.

Pero también gracias a esta investigación, sabemos lo que es un phishing y las maneras de evitar ser víctimas de este método de robo.

5.2 Recomendaciones.

Después de la realización de esta investigación, enunciamos las siguientes recomendaciones:

- Es necesario para la cooperativa de ahorro y crédito COOPERCO, la implementación de un plan de seguridades, ya que después de realizado este trabajo, nos damos cuenta de que podemos ser vulnerables en cualquier momento de un ataque de phishing.
- Debemos estar alertas en todo momento al acceder a la banca electrónica, ya que siempre estos delincuentes estará al acecho y con nuevos métodos de engaño en contra de los clientes de las agencias bancarias.

Bibliografía

http://www.hsbc.com.mx/1/2/es/pie-pagina/seguridad/phishing. (2011). Recuperado el 30 de Diciembre de 2012

http://www.nosesimeexplico.com/foro/showthread.php/58752-Concepto-de-banca-electr%C3%B3nica. (09 de Junio de 2011). Recuperado el 18 de Diciembre de 2012

http://es.kioskea.net/contents/secu/secuintro.php3. (Diciembre de 2012). Recuperado el 28 de Diciembre de 2012

http://jtalex2.blogspot.com/2012/11/historia-del-phishing.html. (26 de Noviembre de 2012). Recuperado el 20 de Diciembre de 2012

http://portaldelusuario.sbs.gob.ec/contenido.php?id_contenido=69. (Mayo de 2012). Recuperado el Diciembre de 2012

http://www.bancolombiamiami.com/miami/micrositios/SucursalVirtualEmpresasMiamiAgency/miami_01_A_02.swf. (2012). Recuperado el 5 de Enero de 2013

http://www.protecciononline.com/consejos/%C2%BFque-es-el-phishing-como-funciona-y-como-evitarlo/. (2012). Recuperado el 28 de Diciembre de 2012

https://www.paypal.com/es/webapps/mpp/security/general-understandphishing. (2012). Recuperado el 30 de Diciembre de 2012

Hoy, D. (04 de Octubre de 2010). *http://www.hoy.com.ec/noticias-ecuador/cinco-delitos-informaticos-cada-dia-433373.html*. Recuperado el 05 de Octubre de 2012

http://www.pandasecurity.com/spain/homeusers/security-info/cybercrime/phishing/. (s.f.). Recuperado el 21 de Diciembre de 2012

http://www.webopedia.com/TERM/P/phishing.html. (s.f.). Recuperado el 20 de Diciembre de 2012

Nina, J. (5 de Noviembre de 2012). *http://homebankingexplorer.blogspot.com/*. Recuperado el 18 de Diciembre de 2012

ANEXO 1

Entregables.

COOPERATIVA DE AHORRO Y CREDITO COOPERCO.

Guía de conocimiento.

FORMAS DE DETECTAR UN PHISHING.

Clasificación por grupo de edades y costumbres.

La compañía [7]McAfee identificó tres tipos de usuarios de home banking de acuerdo con sus edades y costumbres online.

Fuente:http://america.infobae.com/notas/31213-Banca-virtual-cmo-evitar-ser-vctima-de-fraudes

1. Los usuarios de entre los 18 y 24 años de edad, son los que más se sienten cómodos con la tecnología, pero tienden a ser muy confiados y no realizan prácticas de seguridad básicas.

[7] McAfee Security Scan es un servicio de análisis de virus libre. McAfee Security Scan proporciona una protección libre de virus y protege a usted con el último software antivirus.
Fuente: casa. mcafee .com/downloads/free-virus- exploración

- Evitar realizar transacciones bancarias distraídas: esté atento a no responder correos electrónicos de bancos falsos (o ataques de phishing) por estar realizando múltiples tareas.

2. Los usuarios de entre los 25 y 45 años de edad, son los usuarios más frecuentes de la banca electrónica, ya sea para el trabajo como para movimientos personales, la mayoría de estos usuarios cuenta con software antivirus instalado.

Sin embargo, este grupo tiende a ser displicente o excesivamente confiado con relación a la seguridad.

- Nunca responda correos no solicitados de un banco que pida información personal.
- Revise sus estados financieros y transacciones tan pronto como lleguen, de modo que si hay anomalías en operaciones no autorizadas, pueda limpiarlas de inmediato.

3. Los usuarios de más de 45 años de edad, no están familiarizado con los avances de la tecnología y solo un pequeño porcentaje trabaja o usa la banca electrónica, además estos usuarios en su mayoría tienen software de seguridad instalado.

- Asegúrese de ejecutar un escaneo de seguridad en su computadora antes de registrarse en cualquier servicio bancario en línea a fin de asegurar que esté comenzando con una computadora sin [8]malware.

[8] Malware.- Abreviatura de "software malicioso" malware se refiere a los programas de software diseñados para dañar o hacer otras acciones no deseadas en un sistema informático. En español, "mal" es un prefijo que significa "malo", haciendo que el término "software maligno", que es una buena manera de recordar (incluso si no eres español).
Fuente: http://www.techterms.com/definition/malware

- Cree contraseñas complicadas. No tema exceder el estándar de ocho caracteres y un par de números, mientras más larga, mejor, y cambie su contraseña con frecuencia.

Los criminales cibernéticos no atacan los sistemas bancarios, sino la PC de los clientes.

Cuando una persona utiliza la banca electrónica juega un rol muy importante en mantenerse segura mientras está en línea. La razón es que los phishing que buscan robar la identidad bancaria en línea atacan la PC, no los sistemas de banca electrónica.

Los sistemas bancarios tienen una seguridad excelente, por lo tanto, los criminales cibernéticos no atacan los sistemas bancarios, sino las PC.

Los phishing usan la suplantación de identidad o las aplicaciones de software financiero maliciosas que instalan en una PC para robar datos como nombres de usuarios, contraseñas e incluso secretos compartidos que el usuario le facilita al banco y que confirman respuestas a preguntas como '¿Cuál fue su primer auto?'.

La suplantación de identidad es un ataque que se da en dos partes. Primero, el usuario recibe un mail que parece legítimo y que cree que lo ha recibido de su banco, pero cuando hace clic en un link lo direcciona a la página de un hacker que está tan bien hecha que parece ser la página del banco.

FORMAS DE COMBATIR EL ROBO ATREVES DE UN PHISHING.

¿Cómo puedo protegerme mientras utilizo la banca en línea?

Lo más importante para protegerse cuando se está en línea es asegurarse de que nadie robe su nombre de usuario y contraseña. Las contraseñas robadas son la raíz del problema de la seguridad en la banca en línea y de Internet en su totalidad. Cualquier persona que tenga su contraseña puede acceder a sus cuentas.

Es por eso que un segundo factor de autenticación a través de algo que posea el usuario es una medida de seguridad muy fuerte, ya que el delincuente deberá robar algo físico además de la contraseña para cometer un fraude en línea.

En caso de que el banco no cuente con sistemas de autenticación de dos factores, mire estas ocho reglas para la seguridad:

1. Siempre asegúrese de que se encuentra en la página de Internet que usted quiere.

2. No haga click en un enlace de un mail.

3. Trate de utilizar una barra de seguridad en su navegador.

4. Protéjase contra la suplantación de identidad.

5. Protéjase contra el registro de teclas.

6. No guarde contraseñas en la PC si otras personas tienen acceso a ella.

7. No guarde las contraseñas en un archivo en su PC.

8. No escriba las contraseñas, si puede evitarlo, o escóndalas muy bien.

9. Evita compartir las claves de acceso (password).

10. Guarda los dispositivos de generación de claves (Token) en un lugar seguro.

11. Solicita o activa el registro de alertas al celular o correo electrónico.

12. Compra sólo en establecimientos reconocidos o seguros (sitios reconocidos “https “).

13. Programa los movimientos que vas a hacer (pagos, transferencias u operaciones), para evitar tener abierta la sesión por mucho tiempo. Concreta la operación y cierra tu sesión. Nunca dejes abierta la sesión, sobre todo en lugares públicos, como la oficina.

14. Verifica por semana o quincena el estado de cuenta (Internet) para ver que no haya cargos extraños.

15. Evita los llamados “ciber-cafés”.

16. Teclea directamente la dirección de Internet del banco, evita ingresar a sesiones mediante hipervínculos que recibas.

17. Nunca abras o respondas a una ventana emergente, o correo electrónico (Phishing).

18. Utiliza software actualizado de protección antivirus y anti-espía.

19. Procura tener diferentes contraseñas para cada servicio.

20. Revisa periódicamente las cuentas registradas para hacer traspasos y asegurarte de que no existan cuentas que no se dieron de alta.

NAVEGACIÓN SEGURA EN LA PÁGINA WEB DEL BANCO.

Servicios del Sistema Financiero Ecuatoriano.

Banca por Internet.

Consejos Prácticos.

- Las entidades financieras no solicitan información confidencial a sus clientes, de ocurrir este evento es indispensable que se comunique con la entidad lo más rápido posible.
- Ante el evento de recibir vía Internet dentro de un e-mail indicaciones para conectarse a un enlace (link) de una institución financiera, tenga en consideración que puede representar o simular el sitio o portal de una institución bancaria, no haga clic en dicho hipervínculo. Los enlaces dentro de un correo electrónico pueden disimular u ocultar otro sitio que no es del banco, es decir, el texto que usted ve puede no ser donde el enlace le indica que lo va a llevar.
- Si usted no ha ingresado directamente al sitio web de la institución financiera o no está seguro de la fuente no debe realizar operación alguna y contactarse con la entidad.
- Cuando se conecte a una institución bancaria busque en la parte inferior derecha de su browser, un candado que indica que es un sitio seguro.
- Lea y entienda atentamente los contratos de banca electrónica o banca por internet.
- Realice sus transacciones electrónicas desde equipos con conexión a internet segura, en la medida de lo posible evite realizarlas desde un café net o centros de cómputo similares.

- Procure cambiar sus claves electrónicas de acceso con regularidad.
- Guarde los respaldos de las transacciones realizadas.
- Revise periódicamente los saldos y movimientos de sus cuentas, de manera que se asegure que no existe ningún movimiento irregular realizado por terceros.

Banca electrónica.

Conclusiones.

Los cambios que experimentan los mercados fuerzan al mundo de las finanzas a buscar continuamente la manera de elevar las utilidades y fortalecer sus posiciones de Mercado. Para lograrlo, las instituciones financieras deben estar al tanto del desarrollo de nueva tecnología y si esta les es útil, implementarla en el negocio.

Las tecnologías de información, la flexibilidad organizacional y la administración del conocimiento son asuntos estratégicos que pueden dar a las compañías financieras una posición de mercado más competitiva. Los recientes avances en el desarrollo de

software permiten que los computadores puedan procesar datos de manera "inteligente" basándose en su contenido o significado. El crecimiento y desarrollo en el área de servicios financieros está cada vez más basada en el avance tecnológico.

Cuenca, 21 de Enero de 2013

DM-000713 2013

Sr.

Carlos Renan Salto Sari

Ciudad.

De mi consideración.

Por medio del presente reciba un cordial saludo, a la vez, que le comunico que está aceptada su solicitud de realizar un análisis en cuanto a seguridades de la Página Web de la Cooperativa de Ahorro y Crédito Erco Ltda. en nuestra agencia Baguanchi, debiendo mantener la debida confidencialidad a la información a la que accede antes y después de la investigación a realizar.

Sin otro particular, suscribo.

Atentamente,

Cooperco: Desde 1965... Generando desarrollo solidario!

COOPERATIVA DE AHORRO Y CREDITO
ERCO LTDA.
Firmas Autorizadas

Ing. Héctor Pajardo

GERENTE

Cc: file