UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

SEMINARIO DE GRADUACIÓN

"SEGURIDAD INFORMÁTICA"

Tema:

"Análisis de los fraudes informáticos y su incidencia en el acceso a la información en la Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo"

Proyecto de Trabajo de Graduación. Modalidad: SEMINARIO, presentado previo la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos

AUTOR: Pico Llerena Elsa Maribel

TUTOR: Ing. Elsa Pilar Urrutia Urrutia

Ambato - Ecuador

Noviembre - 2012

APROBACION DEL TUTOR

En mi calidad de tutor del trabajo de investigación sobre el tema: **"ANÁLISIS DE LOS FRAUDES INFORMÁTICOS Y SU INCIDENCIA EN EL ACCESO A LA INFORMACIÓN EN LA COOPERATIVA DE AHORRO Y CRÉDITO SAN FRANCISCO LTDA. AGENCIA PELILEO"**, de la Srta. Elsa Maribel Pico Llerena, estudiante de la Carreara de Ingeniería en Sistemas Computacionales e Informáticos, de la facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los tramites y consiguiente aprobación de conformidad al Art. 16 del Capítulo de Tercer Nivel de la Universidad Técnica de Ambato.

Ambato Noviembre, 2012

EL TUTOR

Ing. Elsa Pilar Urrutia Urrutia

TUTORIA

El presente trabajo de investigación titulado: **"ANÁLISIS DE LOS FRAUDES INFORMÁTICOS Y SU INCIDENCIA EN EL ACCESO A LA INFORMACIÓN EN LA COOPERATIVA DE AHORRO Y CRÉDITO SAN FRANCISCO LTDA. AGENCIA PELILEO"**. Es absolutamente original, autentico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato Noviembre, 2012

Elsa Maribel Pico Llerena

CC: 180427875-0

APROBACION DE LA COMISION CALIFICADORA

La comisión calificadora del presente trabajo conformada por los señores docentes Ing. Galo López e Ing. Francisco López., revisó y aprobó el Informe Final del trabajo de graduación titulado: **"ANÁLISIS DE LOS FRAUDES INFORMÁTICOS Y SU INCIDENCIA EN EL ACCESO A LA INFORMACIÓN EN LA COOPERATIVA DE AHORRO Y CRÉDITO SAN FRANCISCO LTDA. AGENCIA PELILEO"**, presentado por la señorita Elsa Maribel Pico Llerena de acuerdo al Art. 18 del Reglamento de Graduación para obtener el Titulo Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

Ing. Oswaldo Eduardo Paredes Ochoa
PRESIDENTE DEL TRIBUNAL

Ing. Galo Mauricio López Sevilla
DOCENTE CALIFICADOR

Ing. Xavier Francisco López Andrade
DOCENTE CALIFICADOR

DEDICATORIA

El presente trabajo investigativo está dedicado a los pilares fundamentales de mi ser: Dios, mis Padres y Hermanos, mi Esposo y mi Hijo grandes amores en mi vida, quienes de una u otra manera han contribuido en el desarrollo de mi trabajo, con su apoyo, fortaleza, paciencia y sobre todo confianza, la misma que fue indispensable para sobresalir en los momentos más difíciles. Por ello y por muchas razones más GRACIAS FAMILA…, mil gracias.

Elsa Maribel Pico Llerena

AGRADECIMIENTOS

A Dios mi profunda gratitud por haberme dado la oportunidad de culminar mi carrera universitaria.

A mis padres Luis y Elsa, personas dignas de admiración y respeto, quienes con esfuerzo me brindaron la oportunidad de superarme dándome el ejemplo necesario para hoy ser una mujer de bien y a mis hermanos Henry, Omar, Rolando y Alfredo, quienes me han demostrado que todo es posible con constancia y sacrificio.

A mi Esposo Diego por impulsarme y darme fuerzas para salir adelante, por ser mi compañero y amigo incondicional, por todo el amor y paciencia para conmigo y por buscar la manera de siempre salir adelante juntos.

A mi Hijo Sebastián por iluminar cada uno de los días de mi vida con su sonrisa y manera de ser, por ser la razón más fuerte para superarme por él y para él.

A la Universidad Técnica de Ambato en especial a la Facultad De Ingeniería en Sistemas Electrónica E Industrial, a cada uno de los docentes los cuales me brindaron sus conocimientos y amistad.

A mi Tutor la Ing. Pilar Urrutia por ser mi guía y compartir sus conocimientos, por brindándome lo mejor de sí y permitirme confiar el ella como docente y amiga.

A la Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo dirigido muy acertadamente por el Ing. Freddy Zurita que me brindo su apoyo y confianza para la realización de la investigación.

Elsa Maribel Pico Llerena

ÍNDICE DE CONTENIDOS

INDICE DE GRÁFICOS

INDICE DE TABLAS

RESUMEN EJECUTIVO

El presente trabajo investigativo denominado "ANÁLISIS DE LOS FRAUDES INFORMÁTICOS Y SU INCIDENCIA EN EL ACCESO A LA INFORMACIÓN EN LA COOPERATIVA DE AHORRO Y CRÉDITO SAN FRANCISCO LTDA. AGENCIA PELILEO", presentará la ayuda necesaria para prevenir el seguir siendo víctimas fraudes informáticos.

La investigación realizada surge a raíz de que en todo el ámbito financiero se ha venido dando un incremento considerable en los casos de fraudes informáticos, hecho que ha generado gran preocupación debido a la importancia de la información generada dentro de éstas dependencias. Sin embargo el erradicar éste tipo de actos delictivos se torna en un hecho imposible, más no la posibilidad de prevenirlo y con ello disminuir su impacto en la sociedad.

Es por ello que el realizar un análisis de esta actividad ilícita es un hecho primordial, ya que en muchas ocasiones es realizada con gran facilidad, aprovechando el desconocimiento de las personas, la ingenuidad al entregar información personal o los deseos de beneficiarse económicamente.

La prevención de los fraudes informáticos mediante el desarrollo de una guía preventiva de seguridad, tiene como objetivo crear conciencia en el recurso humano de la institución financiera sobre las graves consecuencias que puede traer consigo la problemática mencionada.

Dicha guía servirá como herramienta para orientar a los usuarios respecto a medidas de seguridad que deben llevarse a cabo para disminuir la posibilidad de ser víctimas de algún tipo de fraude informático, con lo cual se vería beneficiada la institución financiera como sus respectivos clientes, pues evitaremos que se sigan dando pérdidas económicas, lógicas, daños físicos o incluso la pérdida de prestigio y credibilidad de la entidad.

INTRODUCCIÓN

Conscientes del avance tecnológico que se va dando constantemente en el área informática y el impacto de ésta en nuestra sociedad, se torna necesario que las empresas independientemente de los servicios que ofrezcan a la sociedad implementen medidas de seguridad. Al haber logrado identificar la grave problemática que presenta la Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo, siendo ésta vulnerable a fraudes informáticos, surge la necesidad de buscar una solución rápida al mencionado problema.

Dicho problema se ha venido dando desde algunos años atrás, pero en la actualidad se está incrementando con rapidez, razón por la cual se ve la necesidad de realizar un análisis de los fraudes informáticos y su incidencia en el acceso a la información en la institución ya mencionada.

El estudio a realizarse tiene como principal objetivo prevenir de alguna manera que la institución financiera y sus respectivos clientes se sigan viendo afectados, buscando crear conciencia de prevención en el recurso humano sobre el honesto y correcto manejo de nuestra información, lo cual ayudará a disminuir el índice delictivo de este tipo.

El presente proyecto investigativo tienen como objetivo, el presentar un panorama claro de los fraudes informáticos, es así que se hará énfasis en los siguientes ítems:

En el **Capítulo I** nos centraremos al Tema, Planteamiento del Problema, Análisis Crítico, Prognosis, Formulación del problema, Delimitación del objeto de Investigación, Preguntas directrices, Justificación y Objetivos.

En el **Capítulo II** se plantea los Antecedentes Investigativos, Fundamentación Legal, Categorías Fundamentales, Hipótesis, Señalamiento de Variables.

En el **Capítulo III** se puede encontrar el Enfoque de la Investigación, Modalidades Básicas de la investigación, Niveles o Tipos de investigación, Población y muestra, Operacionalización de variables, Técnicas e Instrumentos de Recolección de información, Plan de recolección de Información, Plan de Procesamiento de la Información.

En el **Capítulo IV** se plantea el Análisis e Interpretación de Resultados.

En el **Capítulo V** se plantea Conclusiones y Recomendaciones.

En el **Capítulo VI** se propone el Tema de la Propuesta, Datos Informativos, Antecedentes de la Propuesta, Justificación, Objetivos, Análisis de Factibilidad, Fundamentación, Informe Técnico, Administración de la Propuesta, Referencias y Anexos.

CAPITULO I

EL PROBLEMA

1.1. Tema

Análisis de los fraudes informáticos y su incidencia en el acceso a la información en la Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo.

1.2. Planteamiento del problema

1.2.1. Contextualización

En la actualidad el uso de nuevas tecnologías a nivel mundial sigue incrementándose de forma sorprendente en todo el territorio, al igual que el incremento de los delitos cometidos mediante el uso inadecuado de los mismos, un claro ejemplo de ello son los fraudes informáticos cometidos en las instituciones financieras a nivel mundial, caso que cada vez es más común ya que ahora no es indispensable que los delincuentes posean altos conocimientos técnicos para cumplir con el objetivo de beneficiarse sin importar el perjuicio ajeno. Por ello es de vital importancia tener un claro conocimiento acerca de este tema lo cual nos beneficiara en un alto porcentaje y disminuirá la posibilidad de que seamos víctimas de este delito.

A nivel nacional los fraudes informáticos están en pleno auge, ya pues día a día es mayor el número de personas víctimas de este delito, en el año 2010 cientos de personas se han visto perjudicadas, en su mayoría en la capital ecuatoriana Quito y el puerto principal Guayaquil. Dado estos hechos es urgente que la comunidad en

general busque una posible solución o a su vez se concientice de la gravedad de dicho problema y las nefastas consecuencias que traería consigo.

En las Instituciones Financieras de la provincia de Tungurahua ya no es un tema nuevo hablar de fraudes informáticos, más bien la preocupación radica en que día a día va siendo más frecuente el enterarnos que una persona ha sido víctima de este delito, sea por clonación de su tarjeta de crédito, robo de su información personal o transferencia ilegales de sus fondos. Hecho por el cual con el transcurrir del tiempo quizá las personas opten por cerrar sus cuentas en las instituciones financieras al sentirse constantemente amenazados por los cyberdelincuentes.

La necesidad de realizar un análisis minucioso de los fraudes informáticos cometidos en la Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo y su incidencia en el acceso a la información que en ella se genera es primordial, pues los procesos que se desarrollan en estas dependencias son de gran importancia tanto para la institución como para sus respectivos clientes. Dada la situación que se da en la actualidad se pudo detectar que existen actividades en la Cooperativa que presentan ciertas irregularidades en el manejo de las mismas por parte del ´personal de la institución, dado que no se las maneja con la cautela que se requiere, por lo cual las vulnerabilidades existentes podrían ocasionar perdidas bastante considerables.

1.2.2. Análisis critico

CAUSAS

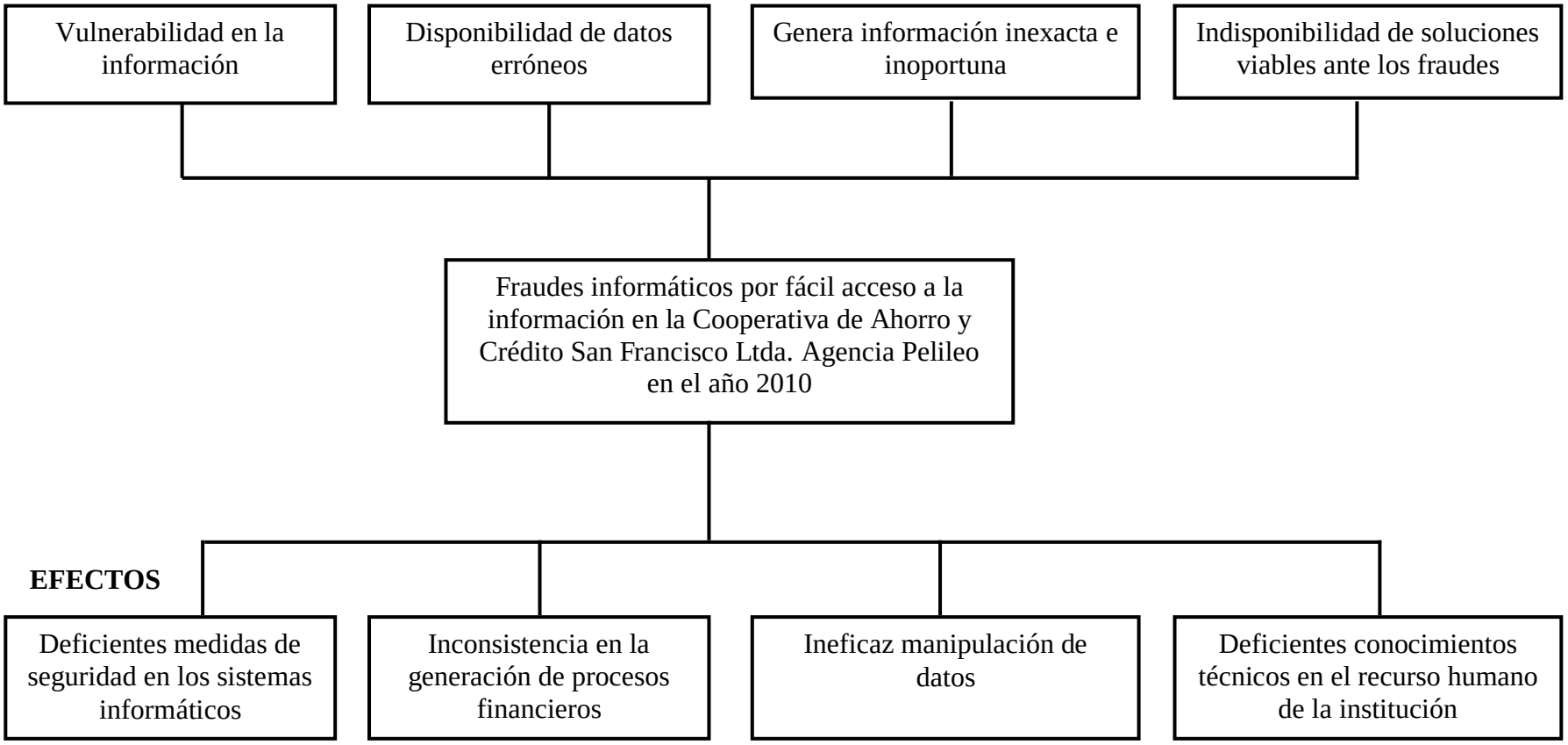


Gráfico 1.1. Árbol de problemas

La Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo institución financiera dedicada a prestar servicios a la comunidad de la localidad y sus alrededores, en la actualidad se encuentra vulnerable a sufrir cualquier tipo de ataques informáticos debido a que no cuentan con las medidas de seguridad apropiadas que logren salvaguardar la integridad de la información que en ellas se genera.

En dicha institución se generan diversos tipos de información, resultante de los procesos que en ésta se desarrollan, como por ejemplo datos personales de clientes, saldos disponibles en cuentas, acreditaciones, transacciones realizadas, entre otras, estos datos deben ser administrados adecuadamente y de forma confidencial. Por ello se deduce que se requiere seguridad óptima en los diferentes recursos informáticos de la institución, decisión que debería ser tomada de manera oportuna dado que a lo largo del tiempo podría producir grandes dificultades como que la información no esté disponible al momento que se la requiera.

La información que se manipula en la Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo, es de suma importancia por lo cual es necesario que guarde concordancia, coherencia y sea absolutamente verídica; es decir en ellas no deben producirse errores humanos, ni mucho menos fallas o falta de seguridad en los sistemas informáticos que podrían causar conflictos al momento de presentar informes o ser sometida a evaluaciones.

Al estar la Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo a merced de cualquier ataque informático, debido al poco conocimiento del recurso humano de la institución en temas técnicos o informáticos, es un objetivo preponderante para ser víctima de fraude, por lo cual la información disponible en ellas en muchas ocasiones no será la adecuada, ni verídica. Es decir las consecuencias que traerá consigo pueden ser catastróficas.

1.2.3. Prognosis

Si no se desarrolla un análisis adecuado de los fraudes informáticos y su incidencia en el acceso a la información en la Cooperativa de Ahorro y Crédito San Francisco

Ltda. Agencia Pelileo, en un momento dado podrían llegar al colapso en el manejo de la información, debido a la mala manipulación de datos o a su vez invasión en los sistemas informáticos, lo cual sería catastrófico debido a la importancia que éstos tienen para el normal funcionamiento de la Institución Financiera como para sus respectivos clientes.

Dado el grave problema que representan los fraudes informáticos para una institución es primordial analizar las graves consecuencias que traen consigo una deficiente manipulación de los datos que se manejan ya que podría presentarse incoherencia en la información, datos erróneos o a su vez la información no podría ser la exacta o verdadera.

Es por ello y por el gran desconocimiento que se presenta en las personas que las perdidas tanto en información como económicas serian de gran consideración no solo para las instituciones financieras, sino también para un gran porcentaje de sus clientes.

1.2.4. Formulación del problema

¿Cómo inciden los fraudes informáticos en el acceso a la información en la Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo en el año 2010?

1.2.5. Delimitación

1.2.5.1. Teórico

- Campo: Seguridad Informática
- Área: Fraudes Informáticos
- Aspecto: Acceso a la información

1.2.5.2. Delimitación temporal

Para el presente trabajo investigativo, el investigador se regirá a un lapso de tiempo de 6 meses.

1.2.5.3. Espacio

La presente investigación se llevará a cabo en la Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo.

1.2.6. Preguntas directrices

¿Cuál es el fraude más común que se comete en la Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo?

¿Cuál es el mecanismo de almacenamiento de la información generada en cada uno de los procesos que se desarrollan en la Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo?

¿Cómo se podrían disminuir el impacto de los fraudes informáticos dentro y fuera de la institución financiera?

1.3. Justificación

El realizar un análisis de los fraudes informáticos y su incidencia en el acceso a la información en la Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo hoy en día se puede considerar como un recurso indispensable, debido al tedioso trabajo que resulta encontrar la manera de contrarrestar sus graves consecuencias, por ello para el investigador es de gran interés el realizar la presente investigación dado el alto porcentaje de incidencia de este delito.

De la misma manera la presente investigación contará con fundamentos teóricos suficientes que logren proporcionar la información necesaria para su normal desarrollo, al igual que se desenvolverá de manera práctica puesto que es una investigación completamente real.

Otro punto a destacarse en el presente trabajo investigativo, es que se encuentra en pleno auge a nivel nacional e internacional, aunque hasta el momento no se la ha dado un enfoque especifico al delito cometido en la Cooperativa de Ahorro y Crédito

San Francisco Ltda. Agencia Pelileo, por ello el investigador buscará minuciosamente estudiar el mencionado fenómeno con la finalidad de tener referencias exactas de la esencia del problema.

La realización del análisis de los fraudes informáticos y su incidencia es de suma importancia debido a las grandes ventajas que se podría obtener con un estudio de este tipo, como por ejemplo mejorar la manipulación de la información generada en los diversos procesos, disponibilidad de datos e información real, oportuna y además verídica lo que hará que sean beneficiados tanto las instituciones como sus respectivos clientes, transformando a dichas entidades en un modelo digno de imitar por las demás instituciones de la localidad.

Debido al servicio que brinda a la sociedad la Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo, se torna de gran utilidad el realizar el análisis de los fraudes informáticos que invaden a la sociedad en general, ya que sería provechoso tanto para sí misma como empresa como para el entorno en que ésta se desenvuelve, ya que con ello el investigador estará en la capacidad de detectar las principales falencias de seguridad y buscar una posible solución de manera inmediata.

Finalmente el investigador justifica el presente trabajo, pues se torna necesario plantear una alternativa viable y factible en todos sus aspectos, lo que permitirá concientizar en la institución financiera antes mencionada, la real importancia de tener conocimientos muy bien fundamentados de este fenómeno y ayudará a viabilizar el normal desarrollo de sus procesos sin problema alguno.

1.4. Objetivos

1.4.1. Objetivo General

Analizar los fraudes informáticos y su incidencia en el acceso a la información de la Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo.

1.4.2. Objetivos Específicos

- Determinar cuáles son los tipos de fraudes informáticos más comunes que se realizan en la Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo.
- Analizar los procesos de almacenamiento de la información y la seguridad existente en la Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo.
- Plantear una propuesta de solución para disminuir el impacto que provocan los fraudes informáticos.

CAPITULO II

MARCO TEORICO

2.1. Antecedentes investigativos

URBINA, Vanessa, Auditoria de fraudes en sector financiero privado en el periodo 2000-2003, del 2005, que reposa en el repositorio de la Universidad de Guayaquil.

Tema: Auditoria de fraudes en sector financiero privado en el periodo 2000-2003

Objetivos:

- Determinar las debilidades en los manuales de control interno, producto de la cual se pueden dar intentos de fraudes.
- Determinar las personas involucradas en el fraude y evidenciar el grado de vínculo directo en su participación.
- Detectar las posibles falencias que podrían existir, en las disposiciones emitidas por la Superintendencia de Bancos, en las cuales se determina ciertas facilidades o escudos legales que den lugar a la intención de cometer actos fraudulentos.

Conclusión:

Durante la investigación de las principales causas de la crisis en el país y la caída de algunos bancos nos dimos cuenta que un porcentaje considerable se origino por fraudes internos y externos.

Recomendaciones:

Los clientes deben tener mucho cuidado al realizar transacciones en ventanillas, para evitar ser víctimas de fraude perpetrados por cajero o personas ajenas a la institución.

Se ha tomado en cuenta el mencionado trabajo de investigación debido a que cumple con algunas de las expectativas que se busca satisfacer con la nueva investigación pues en ella se logra identificar claramente las falencias de las instituciones financieras y con ello las personas responsables de cometer fraude.

VEGA, Jessy, Diseño de un manual de control interno para el Departamento Financiero en la escuela superior politécnica de Chimborazo- Riobamba, aplicando la nueva normativa y herramientas informáticas que rigen para el sector público en el año 2009, del 2009, que reposa en el repositorio de la Escuela Superior Politécnica de Chimborazo.

Tema: Diseño de un Manual de Control Interno para el Departamento Financiero en la Escuela Superior Politécnica de Chimborazo- Riobamba, Aplicando la Nueva Normativa y Herramientas Informáticas que Rigen para el Sector Público en el año 2009.

Objetivos:

- Establecer en la ESPOCH una organización sistémica, flexible, adaptativa y dinámica para responder con oportunidad y eficiencia a las expectativas de nuestra sociedad.
- Dinamizar la administración institucional mediante la desconcentración de funciones y responsabilidades, procurando la optimización de los recursos en el marco de la Ley y del Estatuto Politécnico.
- Impulsar la investigación básica y aplicada, vinculándola con las otras funciones universitarias y con los sectores productivos y sociales.
- Promover la generación de bienes y prestación de servicios basados en el potencial científico-tecnológico de la ESPOCH.

Conclusiones:

- El estudio y diagnóstico de la situación actual de la Institución permitió conocer las necesidades para el Área Financiera, en la que se registra: Inexistencia de una Manual de Control Interno para el sistema e-SIGEF y e-SIPREN.
- El análisis de conceptos y definiciones emitidas por diferentes autores sobre aspectos relacionados con el tema ayudaron a un mejor entendimiento en la labor del Manual.
- El no poseer un control adecuado para el pago de obligaciones hace que se demore su cancelación dañando así la imagen fiel de la Institución.

Recomendaciones:

- Se implemente el presente manual para que las actividades de control, acoplamiento y evaluación de las operaciones operativas se las realice de forma eficiente y oportuna.
- El manual se convertirá en una guía útil para poder realizar los procedimientos adecuadamente llevando controles efectivos a la vez que deberá ser socializado.
- Se aconseja a la dirección realizar monitoreo periódicamente para verificar el cumplimiento de los controles internos y vigilar el desempeño de sus subordinados.

La presente tesis investigativa ha sido tomada como punto de partida pues en ella se busca implementar un manual interno que ayude al control de las actividades del departamento financiero de la ESPOCH, motivo por el servirá de eje para uno de nuestros principales objetivos de la nueva investigación.

2.2. Fundamentación legal

Constitución de la República del Ecuador

Sección tercera

Comunicación e Información

Art. 16.- Todas las personas, en forma individual o colectiva, tienen derecho a:

1. Una comunicación libre, intercultural, incluyente, diversa y participativa, en todos los ámbitos de la interacción social, por cualquier medio y forma, en su propia lengua y con sus propios símbolos.

2. El acceso universal a las tecnologías de información y comunicación.

Art. 18.- Todas las personas, en forma individual o colectiva, tienen derecho a:

1. Buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y procesos de interés general, y con responsabilidad ulterior.

2. Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley. En caso de violación a los derechos humanos, ninguna entidad pública negará la información.

Art. 20.- El Estado garantizará la cláusula de conciencia a toda persona, y el secreto profesional y la reserva de la fuente a quienes informen, emitan sus opiniones a través de los medios u otras formas de comunicación, o laboren en cualquier actividad de comunicación.

Sección octava

Ciencia, tecnología, innovación y saberes ancestrales

Art. 385.- El sistema nacional de ciencia, tecnología, innovación y saberes ancestrales, en el marco del respeto al ambiente, la naturaleza, la vida, las culturas y la soberanía, tendrá como finalidad:

1. Generar, adaptar y difundir conocimientos científicos y tecnológicos.

2. Recuperar, fortalecer y potenciar los saberes ancestrales.

3. Desarrollar tecnologías e innovaciones que impulsen la producción nacional, eleven la eficiencia y productividad, mejoren la calidad de vida y contribuyan a la realización del buen vivir.

Art. 387.- Será responsabilidad del Estado:

1. Facilitar e impulsar la incorporación a la sociedad del conocimiento para alcanzar los objetivos del régimen de desarrollo.

2. Promover la generación y producción de conocimiento, fomentar la investigación científica y tecnológica, y potenciar los saberes ancestrales, para así contribuir a la realización del buen vivir, al sumak kawsay.

3. Asegurar la difusión y el acceso a los conocimientos científicos y tecnológicos, el usufructo de sus descubrimientos y hallazgos en el marco de lo establecido en la Constitución y la Ley.

4. Garantizar la libertad de creación e investigación en el marco del respeto a la ética, la naturaleza, el ambiente, y el rescate de los conocimientos ancestrales.

5. Reconocer la condición de investigador de acuerdo con la Ley.

Art. 388.- El Estado destinará los recursos necesarios para la investigación científica, el desarrollo tecnológico, la innovación, la formación científica, la recuperación y desarrollo de saberes ancestrales y la difusión del conocimiento. Un porcentaje de estos recursos se destinará a financiar proyectos mediante fondos concursables. Las organizaciones que reciban fondos públicos estarán sujetas a la rendición de cuentas y al control estatal respectivo.

Sección novena

Gestión del riesgo

Art. 389.- El Estado protegerá a las personas, las colectividades y la naturaleza frente a los efectos negativos de los desastres de origen natural o antrópico mediante la prevención ante el riesgo, la mitigación de desastres, la recuperación y mejoramiento de las condiciones sociales, económicas y ambientales, con el objetivo de minimizar la condición de vulnerabilidad.

El sistema nacional descentralizado de gestión de riesgo está compuesto por las unidades de gestión de riesgo de todas las instituciones públicas y privadas en los ámbitos local, regional y nacional. El Estado ejercerá la rectoría a través del organismo técnico establecido en la ley. Tendrá como funciones principales, entre otras:

1. Identificar los riesgos existentes y potenciales, internos y externos que afecten al territorio ecuatoriano.
2. Generar, democratizar el acceso y difundir información suficiente y oportuna para gestionar adecuadamente el riesgo.
3. Asegurar que todas las instituciones públicas y privadas incorporen obligatoriamente, y en forma transversal, la gestión de riesgo en su planificación y gestión.
4. Fortalecer en la ciudadanía y en las entidades públicas y privadas capacidades para identificar los riesgos inherentes a sus respectivos ámbitos de acción, informar sobre ellos, e incorporar acciones tendientes a reducirlos.
5. Articular las instituciones para que coordinen acciones a fin de prevenir y mitigar los riesgos, así como para enfrentarlos, recuperar y mejorar las condiciones anteriores a la ocurrencia de una emergencia o desastre.
6. Realizar y coordinar las acciones necesarias para reducir vulnerabilidades y prevenir, mitigar, atender y recuperar eventuales efectos negativos derivados de desastres o emergencias en el territorio nacional.
7. Garantizar financiamiento suficiente y oportuno para el funcionamiento del Sistema, y coordinar la cooperación internacional dirigida a la gestión de riesgo.

2.3. Categorías fundamentales

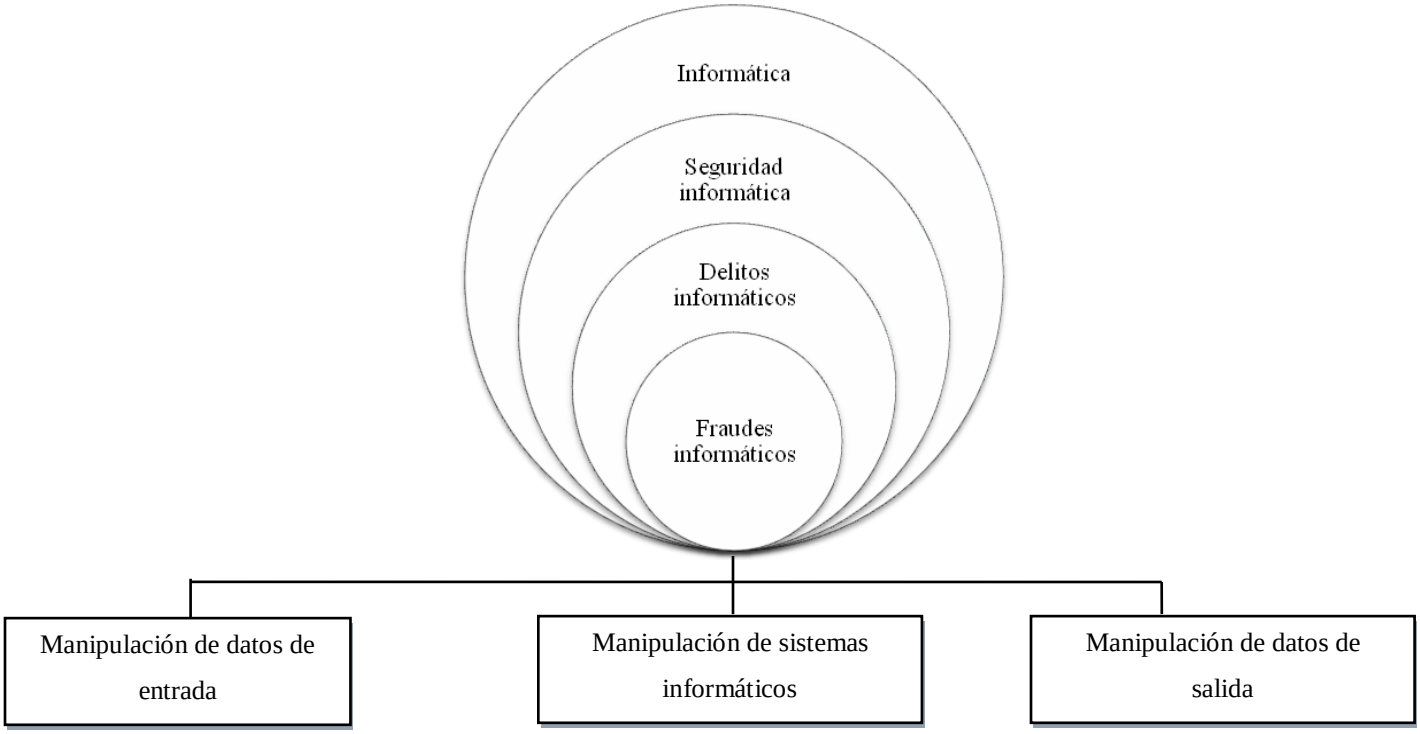


Gráfico 2. 1. Fraudes informáticos

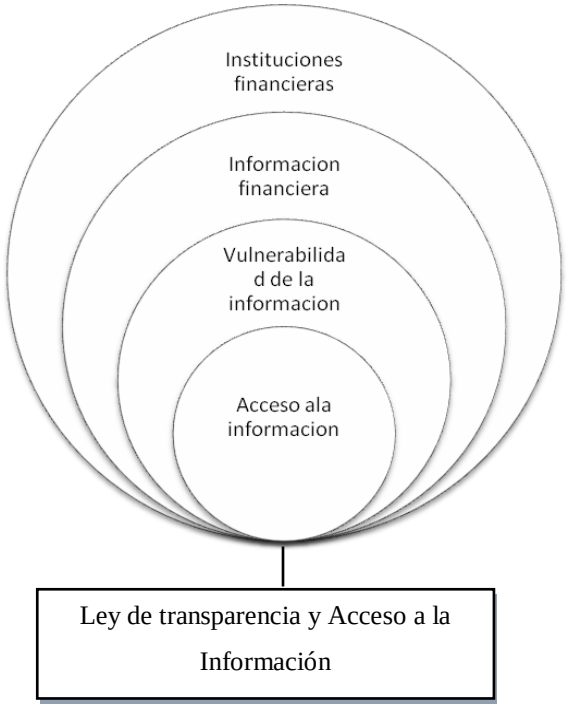


Gráfico 2. 2. Acceso a la información

2.3.1. Informática

Según CHÁVEZ, Aníbal (http://www.monografias.com/trabajos11/curinfa/curinfa.shtml; 06/10/2011; 24/10/2011; 19:00 PM), manifiesta que: "La informática es la ciencia aplicada que abarca el estudio y aplicación del tratamiento automático de la información, utilizando sistemas computacionales, generalmente implementados como dispositivos electrónicos."

Así CALDERON, Luis (2010, 15), define que "La informática es el tratamiento de la información utilizando sistemas electrónicos y computacionales. Consta de tres tareas básicas: entada de datos, procesamiento de la información y salida y transmisión de resultados. La informática es un amplio campo que incluye los fundamentos teóricos, el diseño, la programación y el uso de las computadoras".

Por ello se podría concluir que la informática es una rama que se encarga de estudiar el tratamiento de la información mediante la utilización de elementos computacionales, das de realizar tareas específicas como: ingresar datos, encargarse de que éstos sean procesadas y por ultimo asegurarse que se obtenga información útil.

2.3.2. Seguridad informática

Una definición muy considerable es la de MERLAT, Máximo (http://www.monografias.com/trabajos/hackers/hackers.shtml; 26/10/2011; 24/10/2011), que asevera que "La seguridad informática es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático**"**.

De igual manera CALDERON (2010, 16), dice que "La seguridad informática consiste en aquellas prácticas que se llevan adelante respecto de un determinado sistema de computación a fin de proteger y resguardar su funcionamiento y la información en él contenida. Se le dice seguridad informática tanto a la investigación como a la ejecución de políticas de protección de datos en ordenadores por parte de un individuo o equipo de expertos en computación. "

Es decir se podría definir a la seguridad informática como la disciplina encargada de buscar salvaguardar la integridad de la información, el funcionamiento de los sistemas informáticos, en sí su función principal es proteger todo lo que es valioso para la institución ya sea infraestructura o datos.

2.3.3. Delitos informáticos

SARZANA, Carlos (http://www.monografias.com/trabajos6/delin/delin.shtml; 11/08/2009; 25/10/2011; 9:30 AM), gran conocedor del derecho informático conceptualiza a los crímenes por computadora como "cualquier comportamiento criminógeno en el cuales el de la computadora ha estado involucrada como material o como objeto de la acción criminógena, como mero símbolo".

Otro criterio muy valioso es el HUILCAPI, Arturo http://www.derechoecuador.com/index.php?option=com_content&task=view&id=3091&Itemid=426; 03/10/2011; 25/10/2011; 11:00 AM), dice que "El delito informático, o crimen electrónico, es el término genérico para aquellas operaciones ilícitas realizadas por medio de Internet o que tienen como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet".

Dado los criterios de los diferentes expertos en derecho informáticos se podría mencionar que un delito informático es cualquier acción que va en contradicción de la ley cuya principal característica es hacer uso de medios computacionales para causar perjuicios a terceros.

2.3.4. Fraudes informáticos

Según el criterio de LORENZO, Patricia (http://www.monografias.com/trabajos12/conygen/conygen.shtml; 25/10/2011; 11:10 AM), "El fraude a través de computadoras, son conductas que consisten en la manipulación ilícita, a través de la creación de datos falsos o la alteración de datos o

procesos contenidos en sistemas informáticos, realizada con el objeto de obtener ganancias indebidas."

Otra manera de definir a los fraudes informáticos es la de LOERINCS, Gabor (2001), que dice son aquellas actividades que hacen uso de un sistema de computación para llevar a cabo actos ilícitos y buscar beneficios propios.

Se conceptualiza al fraude informáticos como una Actividad ilícita, realizada por personas inescrupulosas que aprovechan las vulnerabilidades de algún sistema informático con la finalidad de obtener beneficios sin importarles el perjuicio ajeno. Una vez detectada la vulnerabilidad esta puede ser aprovechada las veces que desee el delincuente.

CARRION, Hugo (http://www2 .compendium.com.ar/juridico/depablo.html; 01/07/2001; 25/10/2011; 14:10 PM), dice que existen varias maneras de cometer fraudes informativos entre ellos:

"Manipulación de los datos de entrada: Este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir."

"Manipulación de programas: Consiste en modificar los programas existentes en el sistema o en insertar nuevos programas o rutinas. Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente tiene conocimientos técnicos concretos de informática y programación."

"Manipulación de los datos de salida: Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude del que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos."

Debido a los conocimientos de los distintos expertos se puede concluir que existen diversas formas de cometer fraudes informáticos: manipulación de datos de entrada como por ejemplo al ingresar datos falsos en un sistema, manipulación de sistemas, es decir cambiando las instrucciones propias de los programas para que realice acciones que beneficien al delincuente como por ejemplo desvió de transacciones y manipulación de datos de salida como por ejemplo falsear la información que observamos en los cajeros automáticos.

2.3.5. Instituciones Financieras

Según el criterio del DICCIONARIO DE ECONOMIA Y FINANZAS (http://www.consumoteca.com/economia-familiar/economia-y-finanzas/entidades-financieras; 26/10/2011; 15:00 PM), define a las instituciones financieras como: "Determinado tipo de sociedad que se encarga de la captación de depósitos y la concesión de créditos principalmente. Pueden ser Bancos y Cajas de Ahorro".

Al igual que la fuente anterior el DICCIONARIO DE FINANZAS (http://inversionario.com/2011/04/que-es-una-institucion-financiera-financial-institution-english-spanish-dictionary-finanzas-finance-financial-institution-institucion-financiera/ ; 14/11/2009, 26/10/2011; 15:20 PM), describe que "Una entidad financiera es cualquier empresa que presta servicios financieros (captación y remuneración de nuestros ahorros, concesión de préstamos y créditos, aseguramiento, etc.) a los consumidores y usuarios.

Una institución financiera es un grupo social encargado de la recepción de depósitos y la concesión de créditos a clientes que requieren de sus servicios.

2.3.6. Información financiera

VILLASMIL, Jonathan **(**http://www.mailxmail.com/curso-comunicacion-informatica-historia-computacion/concepto-160-informacion-160-informatica; 14/11/2009, 26/10/2011; 15:25 PM), dice que información financiera es el "Conjunto de datos que se emiten en relación con las actividades derivadas del uso y manejo de los recursos financieros asignados a una institución. Es aquella información que muestra la relación entre los derechos y obligaciones de la dependencia o entidad, así

como la composición y variación de su patrimonio en un periodo o tiempo determinado."

Por otro lado MAYA, Jesús Hernando (http://www.definicion.org/informacion-financiera; 08/09/2009; 26/10/2011; 16:00 PM), considera que "información es todo aquello que permite adquirir cualquier tipo de conocimiento. Existe información cuando se revela algo que hasta ahora era desconocido; la función de la información es aumentar el conocimiento del receptor o reducir su incertidumbre".

Es así que podríamos definir a la información financiera como todos aquellos datos que de una u otra manera sirven a la institución a la toma oportuna y adecuada de decisiones que ayuden al desarrollo de la misma.

2.3.7. Vulnerabilidad de la información

Según el DICCIONARIO DE INFORMATICA (http://www.alegsa.com.ar/Dic/vulnerabilidad.php; 05/11/2010; 26/10/2011; 15:12 PM), define a la "Vulnerabilidad como una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones."

De la misma manera ANDRADE, Wilson (http://www.slideshare.net/Tcherino/seguridad-informatica-3143924; 23/09/2011; 26/10/2011; 16:00 PM), dicen que "Vulnerabilidades son errores que permiten realizar desde afuera actos sin permiso del administrador del equipo, incluso se puede suplantar al usuario, actualmente, ya hay muchas amenazas que tratan de accesar remotamente a los ordenadores, ya sea para hacerlos servidores ilegales de Spam o para robar información, de los agujeros más famosos está el LSASS y el de SVSHOST, de los cuales el Sasser y Blaster se diseminaron rápidamente".

Dada la presente situación se considera que vulnerabilidades son las debilidades encontradas, las mismas que pueden ser aprovechadas por personas inescrupulosas

para causar algún tipo de daño, una vez encontrada la debilidad esta puede ser utilizada las veces que desee el delincuente.

2.3.8. Acceso a la información

PÉREZ, Carlos (http://www.farn.org.ar/docs/pp/informacion1.html; 10/08/2011; 26/10/2011; 16:10 PM), define al acceso a la información como: "El derecho que tiene toda persona de buscar, recibir y difundir información en poder del gobierno".

Algo similar pone a disposición VILLANUEVA, Ernesto (http://www.fpchiapas.gob.mx/transparencia/inicio/definicion_acceso.php; 28/09/2011, 27/10/2011; 19:05 PM), pues da a conocer que el acceso a la información es un derecho fundamental de los individuos. Admitiendo limitaciones excepcionales que deberán estar establecidas en la ley.

El acceso a la información es una actividad que garantiza la libre disponibilidad de información, con la finalidad que ésta sirva de ayuda en la solución de problemas y toma de decisiones, siempre y cuando su utilización no vaya en contradicción de la ley.

Ley Orgánica de Transparencia y Acceso a la Información Pública

Art. 7.- Difusión de la Información Pública.- Por la transparencia en la gestión administrativa que están obligadas a observar todas las instituciones del Estado que conforman el sector público en los términos del artículo 118 de la Constitución Política de la República y demás entes señalados en el artículo 1 de la presente Ley, difundirán a través de un portal de información o página web, así como de los medios necesarios a disposición del público, implementados en la misma institución, la siguiente información mínima actualizada, que para efectos de esta Ley, se la considera de naturaleza obligatoria:

a) Estructura orgánica funcional, base legal que la rige, regulaciones y procedimientos internos aplicables a la entidad; las metas y objetivos de las unidades administrativas de conformidad con sus programas operativos.

b) El directorio completo de la institución, así como su distributivo de personal;
d) Los servicios que ofrece y las formas de acceder a ellos, horarios de atención y demás indicaciones necesarias, para que la ciudadanía pueda ejercer sus derechos y cumplir sus obligaciones;
g) Información total sobre el presupuesto anual que administra la institución, especificando ingresos, gastos, financiamiento y resultados operativos de conformidad con los clasificadores presupuestales, así como liquidación del presupuesto, especificando destinatarios de la entrega de recursos públicos;
i) Información completa y detallada sobre los procesos precontractuales, contractuales, de adjudicación y liquidación, de las contrataciones de obras, adquisición de bienes, prestación de servicios, arrendamientos mercantiles, etc., celebrados por la institución con personas naturales o jurídicas, incluidos concesiones, permisos o autorizaciones;

Según la ley de transparencia y acceso a la información publicada en la Constitución de la Republica del Ecuador del 2008, todo ciudadano tiene derecho a libre y gratuita disponibilidad de la información, es decir toda institución dependiente del servicio que ésta ofrezca se encuentra en la obligación de dar a conocer en un portal publico información general de la institución, pero cabe recalcar que debido a ello la información se encuentra a merced de delincuentes para que sea utilizada a su conveniencia.

2.4. Hipótesis

El análisis de los fraudes informáticos influirá positivamente en el correcto acceso a la información en la Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo.

2.5. Señalamiento de variables

Variable Independiente: Fraudes informáticos
Variable Dependiente: Acceso a la información

CAPITULO III

MARCO METODOLOGICO

3.1. Enfoque

El presente trabajo investigativo tomara un enfoque Cuali-Cuantitativo por las siguientes consideraciones:

Tiene un enfoque Cualitativo debido a que se considerará la participación de las personas dentro de la realidad del problema, interna puesto que permitirá interiorizar el problema y de esta forma interpretar el fenómeno dentro de su contexto.

Cuantitativo debido a que tendrá un solo enfoque, es decir será nomotécnico, explicativo pues brindara una forma clara para hacerse entender, poniendo énfasis en los resultados.

3.2. Modalidades básicas de la investigación

La presente investigación tiene las siguientes modalidades:

Modalidad bibliográfica o documentada: Se ha considerado esta modalidad ya que se ha tomado información importante de libros virtuales, tesis de grado, repositorios de tesis y periódicos.

Modalidad experimental: Se ha considerado la relación de la variable independiente fraudes informáticos y su influencia y relación en la variable dependiente acceso a la información para considerar sus causas y sus efectos.

Modalidad de campo: Se ha considerado esta modalidad ya que el investigador ira a recoger la información primaria directamente de los involucrados a través de una encuesta.

3.3. Tipos de investigación

Se ha realizado la investigación exploratoria, ya que permitió plantear el problema de la investigación Análisis de los fraudes informáticos y su incidencia en el acceso a la información en las instituciones financieras del Cantón Pelileo como de la misma manera ayudó a plantear la hipótesis El análisis de los fraudes informáticos influirá en el correcto acceso a la información en la Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo.

Se ha considerado la investigación descriptiva porque permitió analizar el problema en sus partes como delimitar en tiempo y espacio construyendo el análisis crítico, la contextualización y los antecedentes investigativos.

Por otro lado se ha tomado la investigación correlacional ya que ha permitido medir la compatibilidad de la variable independiente fraudes informáticos con la variable dependiente acceso a la información.

3.4. Población y muestra

En la Cooperativa de Ahorro y Crédito san Francisco Ltda. Agencia Pelileo hasta el mes de Octubre del 2011 se cuenta con los siguientes datos:

La institución cuenta con 7261 clientes, cabe destacar que en dicha entidad financiera se diferencian dos tipos de clientes:

- Socios= 6716 y
- Clientes= 545

Es decir la población considerada para la siguiente investigación son los clientes internos de la mencionada cooperativa.

$$\mathrm{n} = \frac{\mathrm{PQN}}{(N-1)E^2/K^2 + PQ}$$

$$n = \frac{0{,}25(7261)}{(7261-1)0{,}1^2/2^2 + 0{,}25}$$

$$n = \frac{1815{,}25}{(7260)0{,}01/4 + 0{,}25}$$

$$n = \frac{1815{,}25}{72{,}6/4 + 0{,}25}$$

$$n = \frac{1815{,}25}{18{,}15 + 0{,}25}$$

$$n = \frac{1815{,}25}{18{,}4}$$

$$n = 98{,}6549$$

$$n = 99$$

Además de ello también se tomará en cuenta como muestra a 5 personas que en la actualidad son consideradas como parte del elemento Administrativo de Sistemas.

3.5. Operacionalización de variables

Variable Independiente: Fraudes informáticos

Tabla 3. 1. Variable independiente

Concepto	**Categorías**	**Indicadores**	**Ítems**	**Técnicas / Instrumentos**
Actividad ilícita, realizada por personas inescrupulosas que aprovechan las vulnerabilidades de algún sistema informático con la finalidad de obtener beneficios.	▪ Actividades ilícitas	▪ Manipular datos de entrada ▪ Manipular sistemas informáticos ▪ Manipular datos de salida	¿Qué tipo fraude informático es el más frecuente en Cooperativa San Francisco?	Encuesta con un cuestionario a los administradores de sistemas de la Cooperativa San Francisco.
	▪ Personas inescrupulosas	▪ Hackers ▪ Crackers ▪ Lammers	¿Piensa usted que en la institución existen las suficientes políticas de seguridad?	Encuesta con un cuestionario a los administradores de sistemas de Cooperativa San Francisco.

	▪ Vulnerabilidades	▪ Base de datos ▪ Sistema ▪ Recurso Humano	¿Según su criterio cuál es el recurso de mayor vulnerabilidad en los sistemas informáticos dentro de la institución?	Encuesta con un cuestionario a los administradores de sistemas de Cooperativa San Francisco.
	▪ Sistemas informáticos	▪ Dirigido a clientes ▪ De enfoque global	¿Cree usted que los sistemas informáticos utilizados en la Cooperativa San Francisco son seguros?	Encuesta con un cuestionario a los clientes de la Cooperativa San Francisco.
	▪ Beneficios	▪ Económicos ▪ Causar daños materiales institución ▪ Causar daño moral	¿Cuál cree usted sea la finalidad de los delincuentes al cometer fraudes informáticos?	Encuesta con un cuestionario a los clientes internos de la Cooperativa San Francisco.

Variable dependiente: Acceso a la información

Tabla 3. 2. Variable dependiente

Concepto	**Categorías**	**Indicadores**	**Ítems**	**Técnicas / Instrumentos**
Actividad que garantiza la libre disponibilidad de información, para facilitar la solución de problemas y toma de decisiones.	▪ Disponibilidad de información	▪ Datos de la institución ▪ Datos de clientes	¿Qué tipo de información está disponible para los clientes internos de la institución?	Encuesta con un cuestionario a los administradores de sistemas de la Cooperativa San Francisco.
	▪ Solución de problemas	▪ Técnicos ▪ Administrativos	¿Según su criterio el personal de la institución está preparado para dar soluciones a los diferentes problemas que se presenten?	Encuesta con un cuestionario a los clientes de la Cooperativa San Francisco.

	▪ Toma de decisiones	▪ Gerente ▪ Administrador de sistemas	¿Cree usted que las decisiones tomadas por las autoridades de la institución son las adecuadas?	Encuesta con un cuestionario a los administradores de sistemas de la Cooperativa San Francisco.

3.6. Recolección y análisis de la información

TIPOS DE INVESTIGACIÓN

Tabla 3.3. Tipos de investigación

SECUNDARIA	PRIMARIA
• Se recolecta de estudios realizados anteriormente que reposan en repositorios de tesis de grado. • Se encuentra registra en documentos y material impreso: libros, periódicos, tesis de grado, etc. • Las fuentes de información son: biblioteca, internet.	• Se recolecta directamente a través del contacto directo con los clientes internos de las instituciones financieras.

TIPOS DE TÉCNICAS DE INVESTIGACIÓN

Tabla 3.4. Técnicas de investigación

BIBLIOGRÁFICAS	PRIMARIA
• El análisis de documentos (lectura científica) • El fichaje	• La observación • La entrevista • La encuesta.

RECOLECCIÓN DE LA INFORMACIÓN

Tabla 3.5. Recolección de la información

PREGUNTAS	EXPLICACIÓN
1. ¿Para qué?	Recolectar información primaria para comprobar y contrastar con la hipótesis
2. ¿A qué personas o sujetos?	A los clientes internos de las instituciones financieras del cantón Pelileo
3. ¿Sobre qué aspectos?	Variable Independiente: Fraudes informáticos

	Variable Dependiente: Acceso a la información
4. ¿Quién?	Investigadora: Maribel Pico
5. ¿Cuándo?	De acuerdo al cronograma establecido
6. ¿Lugar de recolección de la información?	Instituciones financieras del Cantón Pelileo
7. ¿Cuántas veces?	1 sola vez
8. ¿Qué técnica de recolección?	Encuesta
9. ¿Con qué?	Cuestionario
10. ¿En qué situación?	Situación normal y cotidiana

3.7. Procesamiento y análisis de la información

- Revisión y codificación de la información
- Categorización y tabulación de la información
  1. Tabulación manual
  2. Tabulación computarizada (SPSS)
- Análisis de los datos
  1. La presentación de datos se lo hará a través de gráficos, cuadros para analizar e interpretarlos
- Interpretación de los resultados
  1. Describir los resultados
  2. Estudiar cada uno de los resultados por separado
  3. Redactar una síntesis general de los resultados

CAPITULO IV

ANALISIS E INTREPRETACION DE RESULTADOS

4.1. Encuesta a clientes

Según las respuestas obtenidas después de la aplicación de las encuestas realizadas a los clientes de la Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo, se muestra la valoración de frecuencia y porcentaje en los siguientes cuadros estadísticos.

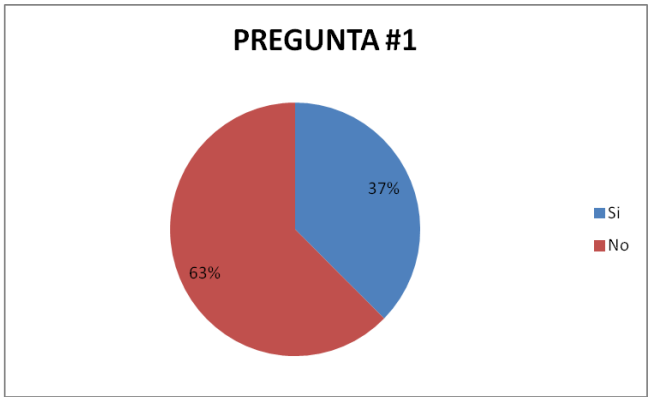
1. ¿Cree usted que ha sido víctima de algún tipo de fraude informático?

Tabla 4. 1 Víctima de fraude informático

N°	Indicador	Valores	%
1	Si	37	37%
2	No	62	63%
	Total	99	100%

Fuente: Estudio de campo
Autor: Maribel Pico

Gráfico 4. 1 Víctima de fraude informático



Fuente: Estudio de campo
Autor: Maribel Pico

Análisis e Interpretación

De las 99 personas encuestadas el 37% que representa 37 personas manifiestan creer que sí han sido víctimas de fraude informático, mientras el 63% que representa 62 personas indican estar seguro de no haber sido víctima de fraude informático

La minoría de los encuestados considera que han sido víctimas de algún tipo de fraude informático, hecho por el cual podrían tener grandes pérdidas económicas o a su vez pérdida de datos personales, lo cual con el tiempo podría ser catastrófico tanto para la institución financiera como para el cliente, por otro lado la mayoría de los encuestados manifiestan no haber sido víctimas de fraude informático, esto debido al alto grado de desconocimiento de las personas.

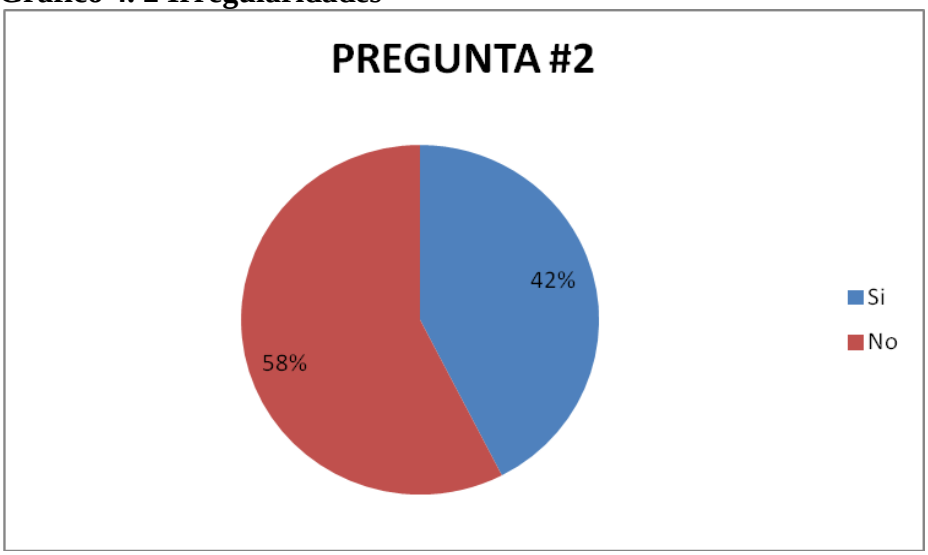
2. ¿En alguna ocasión ha notado irregularidades en el movimiento de transferencias de su cuenta personal?

Tabla 4. 2 Irregularidades

N°	Indicador	Valores	%
1	Si	42	42%
2	No	57	58%
	Total	99	100%

Fuente: Estudio de campo
Autor: Maribel Pico

Gráfico 4. 2 Irregularidades



Fuente: Estudio de campo
Autor: Maribel Pico

Análisis e Interpretación

De las 40 personas encuestadas el 42% que representa 42 personas manifiesta haber notado algún tipo de irregularidad en los movimientos de sus cuentas, mientras el otro 58% que representa 57 personas indica que sus cuentas no han tenido irregularidades.

La minoría de los encuestados mencionan haber notado irregularidades en el movimientos transaccional de su cuentas, es decir han notado desvíos mínimos casi imperceptibles de dinero sin saber el destino o uso del mismo, mientras la mayoría de los encuestados mencionan no haber notado ninguna irregularidad en sus cuentas, debido a la poca atención o desinterés de los clientes.

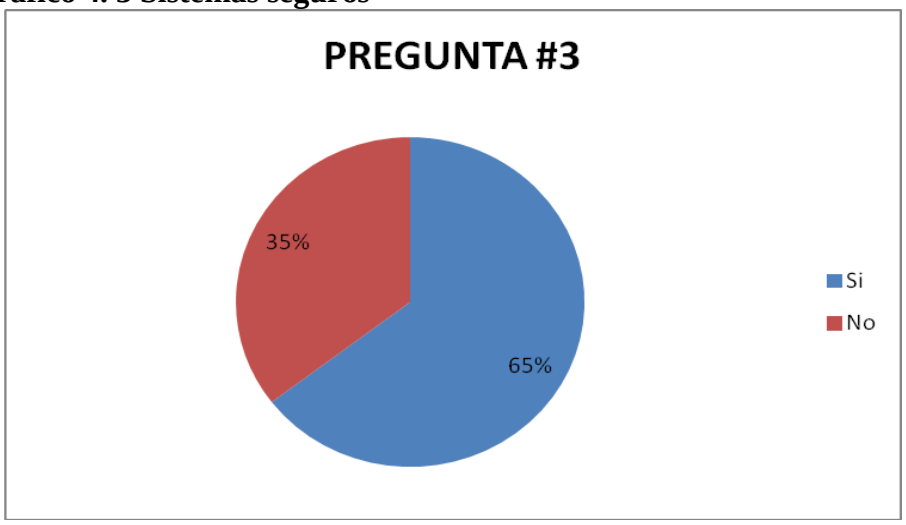
3. ¿Cree usted que los sistemas informáticos utilizados en la Cooperativa San Francisco son seguros?

Tabla 4. 3 Sistemas seguros

N°	Indicador	Valores	%
1	Si	64	65%
2	No	35	35%
	Total	99	100%

Fuente: Estudio de campo
Autor: Maribel Pico

Gráfico 4. 3 Sistemas seguros



Fuente: Estudio de campo
Autor: Maribel Pico

Análisis e Interpretación

De las 99 personas encuestadas el 65% que representa 64 personas indica tener plena confianza en los sistemas informáticos utilizados en la Cooperativa, y el otro 35% que representa 35 personas manifiesta no estar completamente seguro de los sistemas que utiliza la institución.

La mayoría de los encuestados manifiestan confiar en las seguridades de los sistemas utilizados en la institución financiera, por otro lado la minoría de los encuestados mencionan que en la actualidad ningún sistema informático es 100% seguro por lo cual es mejor tomar las medidas necesarias para prevenir cualquier ataque informático y evitar perjuicios.

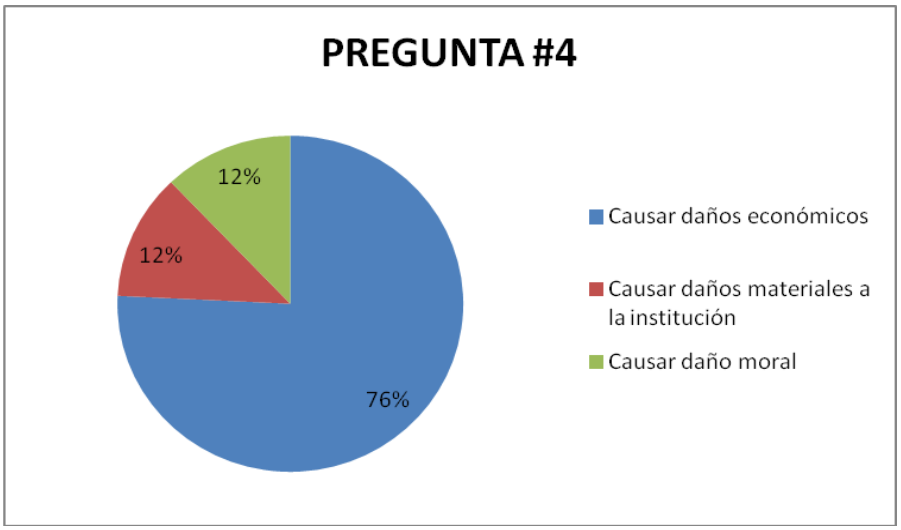
4. ¿Cuál cree usted sea la finalidad de los delincuentes al cometer fraudes informáticos?

Tabla 4. 4 Finalidad del fraude

N°	Indicador	Valores	%
1	Causar daños económicos	75	76%
2	Causar daños materiales a la institución	12	12%
3	Causar daño moral	12	12%
	Total	99	100%

Fuente: Estudio de campo
Autor: Maribel Pico

Gráfico 4. 4 Finalidad del fraude



Fuente: Estudio de campo
Autor: Maribel Pico

Análisis e Interpretación

De las 99 personas encuestadas el 76% que representa 75 personas manifiestan que el principal objetivo de los delincuentes al cometer fraudes es obtener beneficios económicos, mientras el 12% que representan 12 personas indican que la finalidad de este delito es causar daños materiales a la institución y finalmente el otro 12% indica que los delincuentes buscan causar daño moral.

La mayoría de los encuestados mencionan estar seguros que los delincuentes tienen como principal finalidad el obtener beneficios económicos propios sin

importar el perjuicio causado a la institución financiera como a sus respectivos clientes, por otro lado la primera décima parte de los encuestados dicen creer que el objetivo de los delincuentes es provocar daños materiales a la institución aprovechando las debilidades de los recursos tecnológicos y buscando el colapso total o parcial de los mismos, finalmente la décima parte restante de los encuestados manifiestan creer que el objetivo al cometer fraude es causar daño moral a la institución financiera por lo cual en un momento determinado dicha entidad podría llegar a perder credibilidad y con ello clientes.

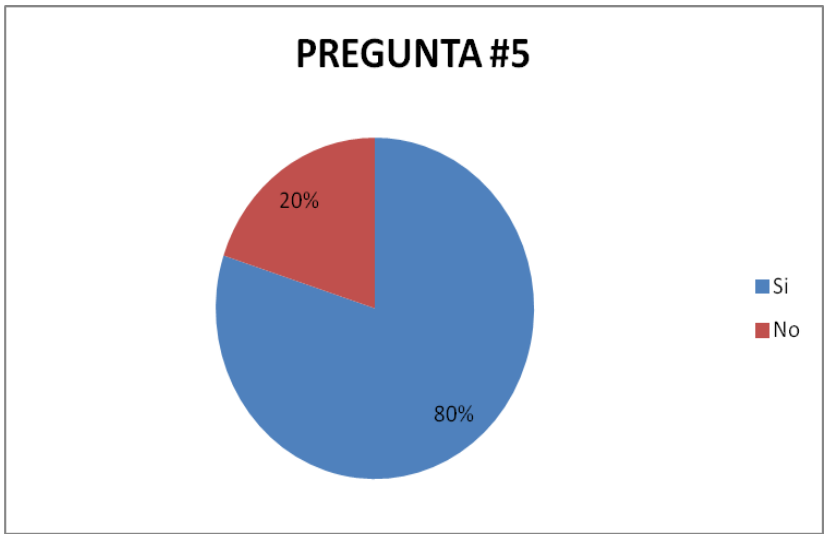
5. ¿Según su criterio el personal de la institución está preparado para dar soluciones a los diferentes problemas que se presenten?

Tabla 4. 5 Soluciones técnicas

N°	Indicador	Valores	%
1	Si	79	80%
2	No	20	20%
	Total	99	100%

Fuente: Estudio de campo
Autor: Maribel Pico

Gráfico 4. 5 Soluciones técnicas



Fuente: Estudio de campo
Autor: Maribel Pico

Análisis e interpretación

De las 99 personas encuestadas el 80% que representa 79 personas mencionan estar convencidos que el personal de la institución financiera está preparado para dar solución a las diferentes problemáticas que se presente, mientras el 20% que representa 20 personas indican no estar seguros que el personal esté suficientemente preparados.

La mayoría de los encuestados mencionan estar completamente convencidos de la preparación del personal de la institución financiera, por otro lado la minoría de los encuestados consideran que no existe el suficiente conocimiento por lo cual no existiría seguridad en las decisiones que deben tomarse.

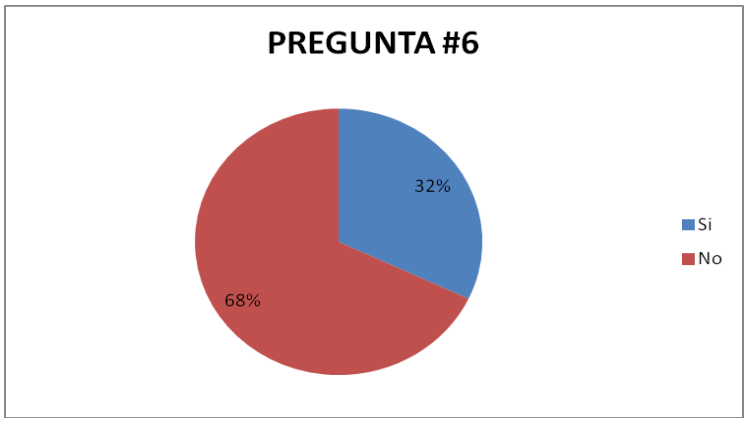
6. ¿Tiene usted conocimiento que la Cooperativa de Ahorro y Crédito San Francisco cuenta con un sitio web a disposición de sus clientes?

Tabla 4. 6 Sitio Web

N°	Indicador	Valores	%
1	Si	32	32%
2	No	67	68%
	Total	99	100%

Fuente: Estudio de campo
Autor: Maribel Pico

Gráfico 4. 6 Sitio Web



Fuente: Estudio de campo
Autor: Maribel Pico

Análisis e Interpretación

De las 99 personas encuestadas el 32% que representa 32 personas manifiestan tener conocimiento de la existencia del sitio web oficial de la Cooperativa de Ahorro y Crédito, mientras el 68 % que representa 67 personas indican no tener conocimiento de la existencia del uso de este tipo de tecnología.

La minoría de los encuestados mencionan tener conocimiento de la existencia del sitio web de la institución financiera, situación que la ven provechosa debido a que hacen uso de la tecnología para mejorar los servicios que ofrecen a la sociedad, por otro lado la mayoría de los encuestados manifiestan no tener conocimiento de la existencia del sitio web oficial de la institución, situación que es preocupante debido a que no se estaría explotando al máximo sus utilidades, ni aprovechando sus beneficios.

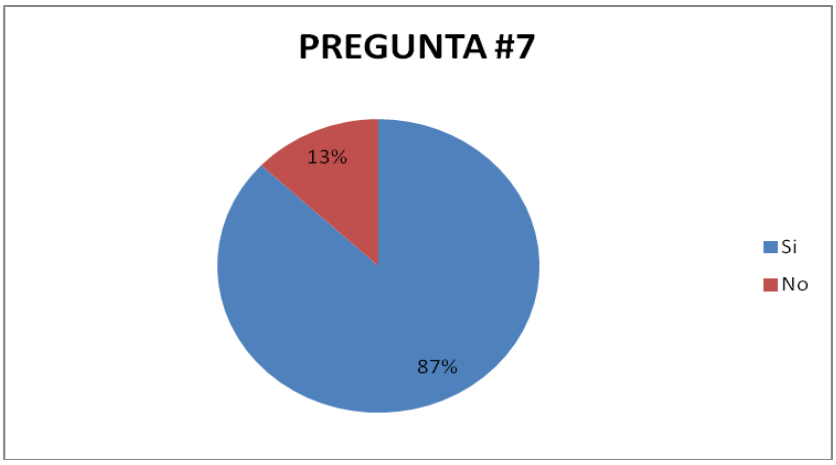
7. ¿Tendría usted la confianza de realizar transacciones electrónicas en el sitio oficial de la institución?

Tabla 4. 7 Transacciones electrónicas

N°	Indicador	Valores	%
1	Si	86	87%
2	No	13	13%
	Total	99	100%

Fuente: Estudio de campo
Autor: Maribel Pico

Gráfico 4. 7 Transacciones electrónicas



Fuente: Estudio de campo
Autor: Maribel Pico

Análisis e Interpretación

De las 99 personas encuestadas el 87% que representa 86 personas manifiestan que no tendrían la suficiente confianza de realizar transacciones mediante la web debido al peligro que esto representa, mientras únicamente el 13% que representa 13 personas estarían dispuestos a realizar transacciones vía web.

La mayoría de los encuestados mencionan que estrían dispuestos a realizar transacciones vía web a través del sitio oficial de la institución, esto debido al gran ahorro de tiempo y el normal desarrollo de sus actividades, mientras la minoría de los encuestados manifiestan no tener confianza al realizar transacciones electrónicas debido al desconocimiento respecto a las amenazas informáticas que aparecen día a día.

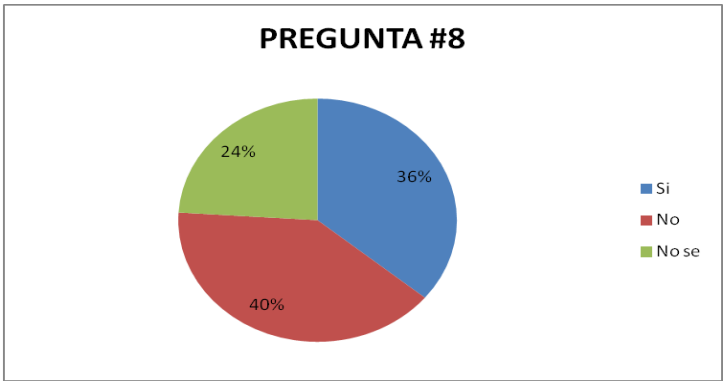
8. ¿En caso de ser víctima de fraude informático estaría dispuesto a realizar la respectiva denuncia ante las autoridades correspondientes?

Tabla 4. 8 Víctimas de fraude

N°	Indicador	Valores	%
1	Si	36	36%
2	No	39	40%
3	No se	24	24%
	Total	99	100%

Fuente: Estudio de campo
Autor: Maribel Pico

Gráfico 4. 8 Víctimas de fraude



Fuente: Estudio de campo
Autor: Maribel Pico

Análisis e Interpretación

De las 99 personas encuestadas el 36% que representa 36 personas manifiestan que estarían dispuestas a denunciar el fraude informático, por otro lado 40% que representa 39 personas no realizarían la denuncia correspondiente y el 24% que representa 24 personas no sabrían que acciones tomar frente esta situación.

La primera décima parte de los encuestados manifiestan estar dispuestos a denunciar los fraudes informáticos, por otro lado la mayoría de los encuestados mencionan no tener la intención de denunciar los delitos informáticos debido al desconocimiento de la existencia de una ley que sanciona estos delitos, finalmente décima parte restante de los encuestados manifiestan no saber las acciones que tomarían ante esta situación por lo cual es de suma importancia educarse frente a este fenómeno en pleno auge.

4.2. Encuesta al Administrador de Sistemas

Según las respuestas obtenidas después de la aplicación de la encuesta realizadas al Administrador de Sistemas de la Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo, se muestra la valoración de frecuencia y porcentaje en los siguientes cuadros estadísticos.

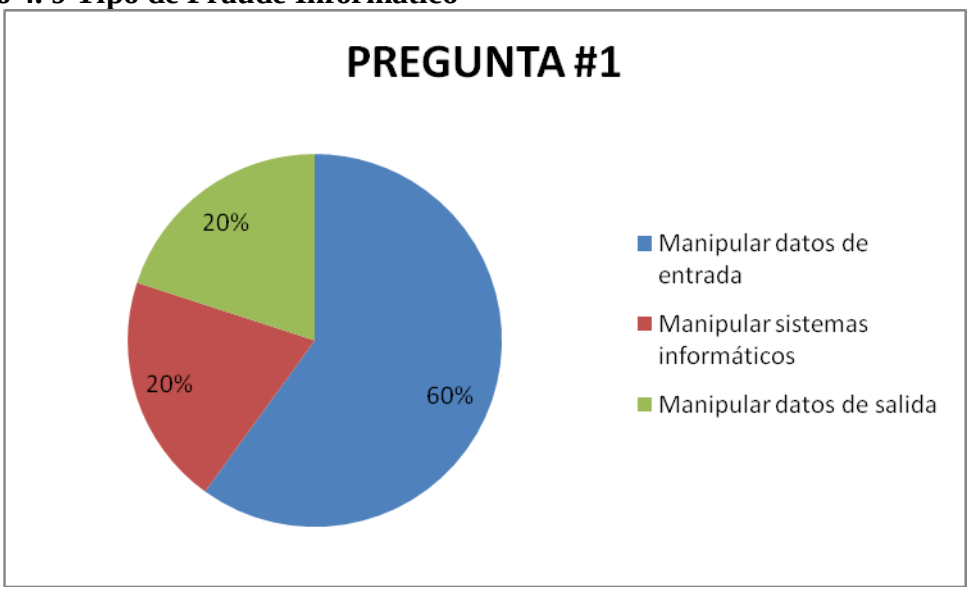
1. ¿Qué tipo de fraude informático es el más común en las instituciones financieras?

Tabla 4. 9 Tipo de Fraude Informático

N°	Indicador	Valores	%
1	Manipular datos de entrada	3	60%
2	Manipular sistemas informáticos	1	20%
3	Manipular datos de salida	1	20%
	Total	5	100%

Fuente: Estudio de campo
Autor: Maribel Pico

Gráfico 4. 9 Tipo de Fraude Informático



Fuente: Estudio de campo
Autor: Maribel Pico

Análisis e Interpretación

De las 5 personas encuestadas el 60% que representa 3 personas manifiestan que los fraudes más comunes en la actualidad son los cometidos mediante la manipulación de datos de entrada, mientras el 20 % que representa 1 persona manifiesta que en su mayoría los fraudes son cometidos mediante la alteración en los sistemas informáticos y el ultimo 20 % que representa 1 persona piensan la los fraudes más comunes son cometidos mediante la manipulación de datos de salida.

La minoría de los encuestados mencionan que un alto porcentaje de fraudes informáticos son cometidos valiéndose de la manipulación de datos de entrada, es decir ingreso de información falsa o errónea con la finalidad de beneficiar a terceros, la otra la décima parte manifiesta que los fraudes más comunes son cometidos mediante la manipulación de los sistemas informáticos, es decir la alteración del código fuente del mismo, la décima parte restante piensa que los fraudes más frecuentes son los realizados por la manipulación de datos de salida, aprovechando el descuido e ingenuidad de los usuarios.

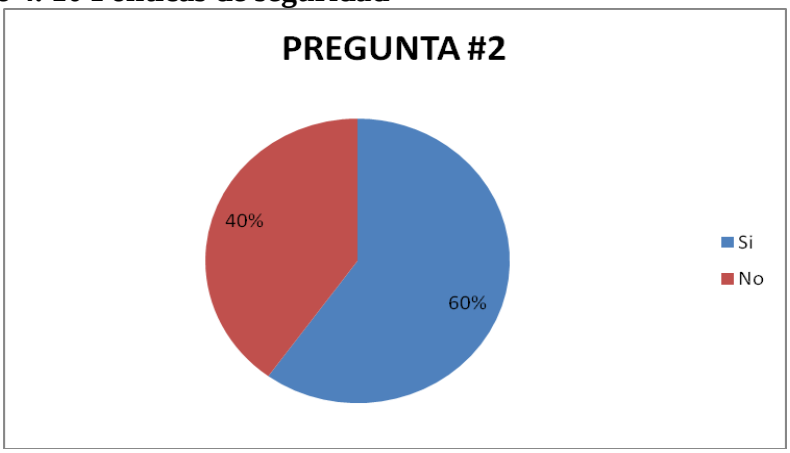
2. ¿Piensa usted que en la institución existen las suficientes políticas de seguridad?

Tabla 4. 10 Políticas de seguridad

N°	Indicador	Valores	%
1	Si	3	60%
2	No	2	40%
	Total	5	100%

Fuente: Estudio de campo
Autor: Maribel Pico

Gráfico 4. 10 Políticas de seguridad



Fuente: Estudio de campo
Autor: Maribel Pico

Análisis e Interpretación

De las 5 personas encuestadas el 60% que representa 3 personas manifiestan que en la institución financiera si existen las suficientes políticas de seguridad, mientras el 40 % que representa 2 personas creen que en la institución no existen las suficientes medidas de seguridad para salvaguardar la información.

La mayoría de los encuestados mencionan que en la institución financiera en la actualidad cuenta con las suficientes políticas de seguridad para salvaguardar toda la información que se requiera, por otro lado minoría de los encuestados dicen en la actualidad la institución si cuenta con buenas políticas de seguridad, pero que no son las suficientes dado que a diario aparecen nuevas amenazas informáticas.

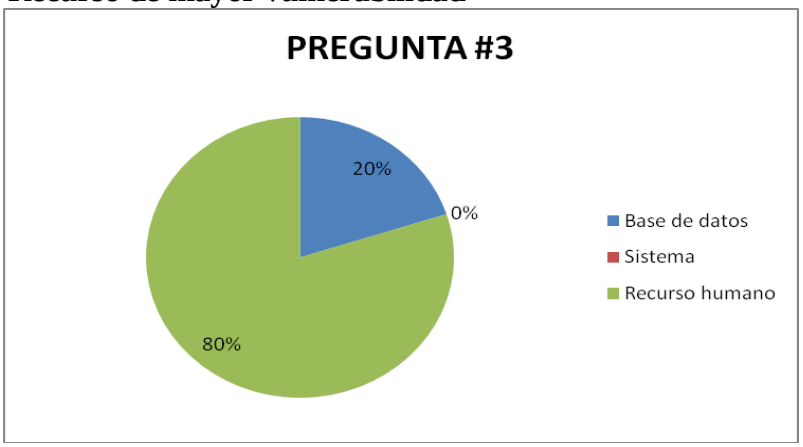
3. ¿Según su criterio cuál es el recurso de mayor vulnerabilidad en los sistemas informáticos dentro de la institución?

Tabla 4. 11 Recurso de mayor vulnerabilidad

N°	Indicador	Valores	%
1	Base de datos	1	20%
2	Sistema	0	0%
3	Recurso humano	4	80%
	Total	5	100%

Fuente: Estudio de campo
Autor: Maribel Pico

Gráfico 4. 11 Recurso de mayor vulnerabilidad



Fuente: Estudio de campo
Autor: Maribel Pico

Análisis e Interpretación

De las 5 personas encuestadas el 20% que representa 1 personas manifiestan que la base de datos es la mayor vulnerabilidad de los sistemas informáticos, por otro lado el 80 % que representa 4 personas mencionan que la mayor vulnerabilidad existente es el recurso humano.

La minoría de los encuestados mencionan que el recurso con más vulnerabilidad es la base de datos, debido a las pocas medidas de seguridad, por otro lado ninguno de los encuestados creen que el sistema informático en sí sea vulnerable, finalmente la mayoría de los encuestados manifiestan que el recurso humano es el más vulnerable, debido al desconocimiento, ingenuidad o ambición de las personas.

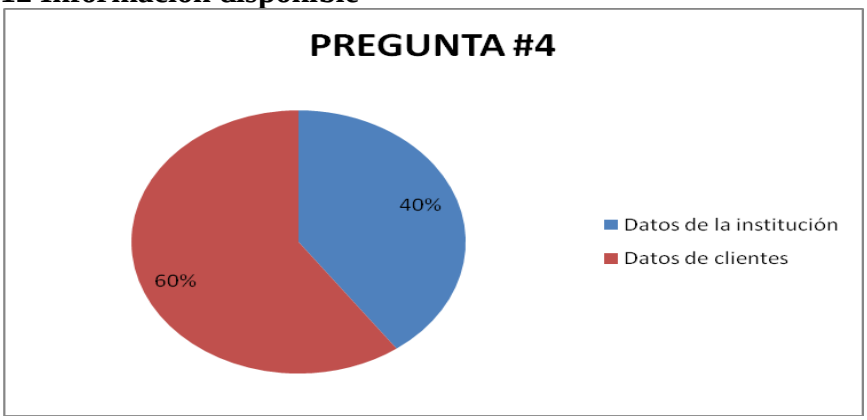
4. ¿Qué tipo de información está disponible para los clientes internos de la institución?

Tabla 4. 12 Información disponible

N°	Indicador	Valores	%
1	Datos de la institución	2	40%
2	Datos de clientes	3	60%
	Total	5	100%

Fuente: Estudio de campo
Autor: Maribel Pico

Gráfico 4. 12 Información disponible



Fuente: Estudio de campo
Autor: Maribel Pico

Análisis e Interpretación

De las 5 personas encuestadas el 40% que representa 2 personas mencionan que la única información disponible para los clientes son los datos de la institución, mientras el 60 % que representa 3 personas manifiestan que la única información disponible para los clientes son los datos correspondientes a los mismos.

La minoría de los encuestados manifiesta que la información que se encuentra a disposición para los clientes de la entidad financiera son datos generales de la institución, mientras la mayoría de los encuestados mencionan que la información disponible para los clientes es la referente a datos propios de los mismos, buscando con ello evitar la divulgación de información confidencial.

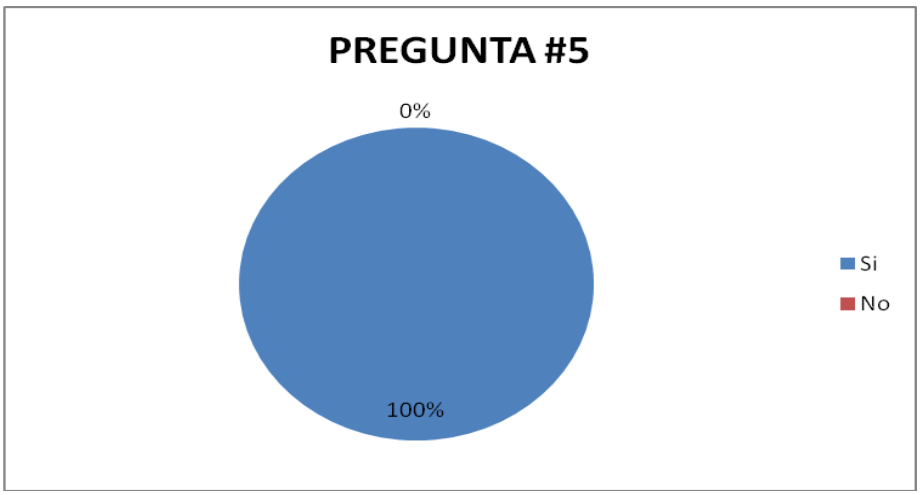
5. ¿Cree usted que las decisiones técnicas tomadas por las autoridades de la institución son las adecuadas?

Tabla 4. 13 Decisiones técnicas

N°	Indicador	Valores	%
1	Si	5	100%
2	No	0	0%
	Total	5	100%

Fuente: Estudio de campo
Autor: Maribel Pico

Gráfico 4. 13 Decisiones técnicas



Fuente: Estudio de campo
Autor: Maribel Pico

Análisis e Interpretación

De las 5 personas encuestadas el 100 % que representa 5 personas mencionan que las decisiones de carácter técnico tomadas por las autoridades de la institución financiera son las adecuadas, mientras el 0 % es decir ninguna persona cree lo contrario.

La totalidad de los encuestados manifiestan que cada una de las decisiones técnicas tomadas por parte de las autoridades son las adecuadas, gracias a lo cual se busca dar solución a los diversos problemas que pueden darse en la institución financiera.

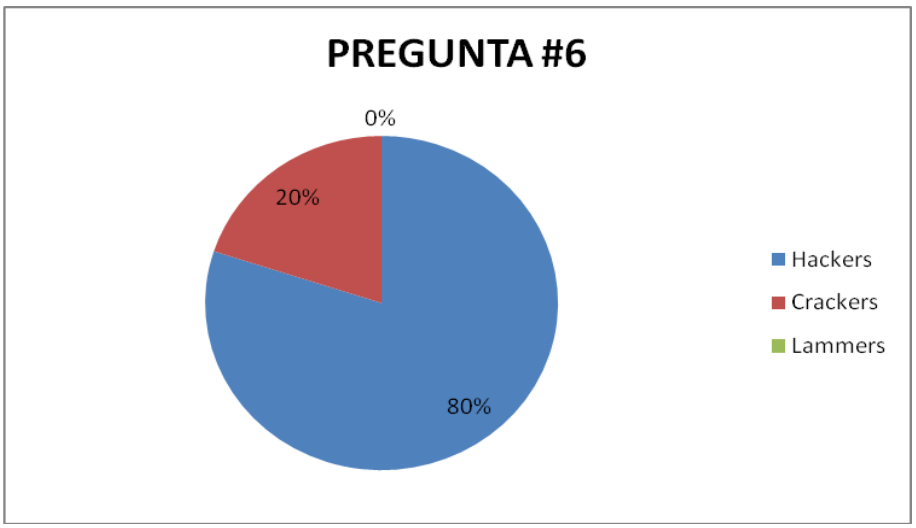
6. ¿Cuál sería la denominación que usted le daría a las personas que cometen fraude informático?

Tabla 4. 14 Denominación de delincuentes

N°	Indicador	Valores	%
1	Hackers	4	80%
2	Crackers	1	20%
3	Lammers	0	0%
	Total	5	100%

Fuente: Estudio de campo
Autor: Maribel Pico

Gráfico 4. 14 Denominación de delincuentes



Fuente: Estudio de campo
Autor: Maribel Pico

Análisis e Interpretación

De las 5 personas encuestadas el 80% que representa 4 personas mencionan que la denominación conocida por ellos para los delincuentes informáticos es la de Hackers, por otro lado el 20 % que representa 1 persona manifiesta conocer a los delincuentes como Crackers.

La mayoría de los encuestados mencionan conocer a las personas que cometen fraude informático como Hackers, quienes usan sus conocimientos para beneficio propio, por otro lado la minoría de los encuestados los denomina Crackers, finalmente ninguna persona relaciona a los delincuentes con el término Lammers.

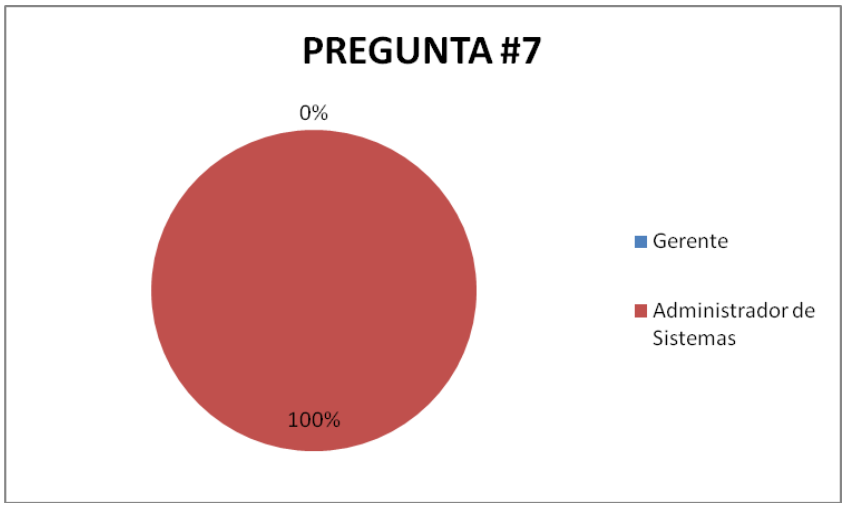
7. ¿Quién es el encargado de la toma de decisiones ante los diferentes problemas técnicos que se dan en la institución financiera?

Tabla 4. 15 Problemas técnicos

N°	Indicador	Valores	%
1	Gerente	0	0%
2	Administrador de Sistemas	5	100%
	Total	5	100%

Fuente: Estudio de campo
Autor: Maribel Pico

Gráfico 4. 15 Problemas técnicos



Fuente: Estudio de campo
Autor: Maribel Pico

Análisis e Interpretación

De las 5 personas encuestadas el 1000 % que representa 5 personas manifiestan que la persona encargada de la toma de decisiones ante los problemas técnicos de la institución es el Administrador de Sistemas.

La totalidad de los encuestados mencionan que la única persona encargada de la toma de decisiones técnicas en la institución financiera es el Administrador de Sistemas, debido a los conocimientos que posee y las soluciones viables que pueden proporcionar a los diferentes problemas de la institución financiera, por otro lado ninguna persona manifiesta que el Gerente tome decisiones técnicas.

4.3. Interpretación de datos

Se ha tomado en cuenta las 3 preguntas discriminantes, la número 2, la número 4 y la número 8 de la encuesta aplicada a los clientes de la Cooperativa de Ahorro y Crédito San Francisco, ya que los resultados arrojados , señalan que un alto porcentaje de clientes de la institución financiera no toman las medidas apropiadas al momento de revisar el movimiento de sus cuentas personales por lo cual podían ser fácilmente víctimas de fraude informático, siendo el principal objetivo de los delincuentes el obtener beneficios económicos y sin que las victimas estén dispuestas a denunciar el delito, ante las instancias correspondientes debido al alto grado de desconfianza en las leyes actuales que rigen nuestra constitución.

Además se ha tomado en cuenta las 2 preguntas discriminantes, la número 1 y la número 3 de la encuesta aplicada a los Administradores de Sistemas de la Cooperativa de Ahorro y Crédito San Francisco, ya que los resultados arrojados en la misma, señalan que con mayor frecuencia los fraudes son cometidos mediante la manipulación de datos de entrada, es decir el ingreso de datos falsos, lo cual está estrechamente ligado a que el recurso con mayor vulnerabilidad es el humano dado al alto grado de desconocimiento, la falta de moral o a su vez la falta de ética profesional en el personal de la institución financiera.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- La institución financiera en la actualidad no cuenta con una guía preventiva de usuario, herramienta que ayude a combatir el desconocimiento de los usuarios respecto a los fraudes informáticos.
- No se cuenta con las políticas de seguridad suficientes para crear en los clientes y personal de la institución conciencia de prevención, buscando con ello tomar más en cuenta lo que sucede con nuestras cuentas de ahorro personal.
- Actualmente en la institución financiera no se lleva a cabo una campaña de conocimiento de la existencia del sitio web oficial de la cooperativa y de las medidas de prevención que deben considerarse al hacer uso de esta herramienta tecnológica.
- Existe un alto grado de desconocimiento respecto al fenómeno denominado fraudes informáticos, hecho que afecta directamente a los clientes como a la institución financiera. Debido a las pérdidas económicas que éstos representan, trae consigo el deslinde de clientes por la falta de confianza en la entidad.
- Los clientes de la Cooperativa de Ahorro y Crédito San francisco Ltda. Agencia Pelileo muestran muy poco interés con relación a los trámites legales que deberían realizarse contra los fraudes informáticos, situación que se viene dando por la falta de confianza en las autoridades correspondientes y el desconocimiento de la existencia de una ley que castiga este tipo de delitos.

- Cada empleado tiene su zona de trabajo y sus funciones asignadas lo cual permite una distribución equilibrada de trabajo, a pesar de ello el personal no considera dentro de sus responsabilidades el cierre de sesión de usuario, acción que por insignificante que parezca pueda traer consigo graves consecuencias.

5.2. Recomendaciones

- Desarrollar de manera urgente una guía preventiva de usuario con la finalidad que esta sirva como herramienta para prevenir el ser víctimas de un posible fraude informático. Puesto que la mejor manera de contrarrestar este delito es manteniendo un alto nivel de conocimiento, para de esta manera saber cómo reaccionar ante esta situación.
- Establecer nuevas política de seguridad para la institución financiera, como políticas de acceso a los sistemas informáticos, asignando permisos necesarios y restringiendo acciones innecesarias para los empleados.
- Impulsar campañas promocionales del sitio web oficial de la institución, así como de las medidas de seguridad que los clientes deben tomar para prevenir el ser víctimas de fraudes informáticos.
- Proporcionar el material necesario para los clientes, de manera que se logre un crecimiento respecto a los conocimientos de los fraudes informáticos. Acción que ayudara a disminuir la incidencia de este delito.
- Dar a conocer a los clientes la existencia y vigencia de la ley encargada de castigar los delitos informáticos, tratando con ello que este acto ilícito no quede en la impunidad.
- Dar a conocer a los empleados que dentro de sus funciones primordiales está el cierre de sesión de usuario, tratando con ello de evitar acciones no autorizadas por personal desconocido y ajeno a la institución.

CAPITULO VI

PROPUESTA

6.1. Datos Informativos

- Titulo

  Análisis de los fraudes informáticos y su incidencia en el acceso a la información en la Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo.

- Institución ejecutora

  Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo.

- Director de tesis

  Ing. Pilar Urrutia

- Beneficiario

  Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo.

- Ubicación

  Quis Quis 412 y Av. Padre Chacón

- Tiempo estimado para la ejecución

  - Fecha de inicio: Febrero de 2012
  - Fecha de finalización: Agosto de 2012

- Equipo técnico responsable

    - Investigadora: Maribel Pico
    - Gerente: Ing. Freddy Zurita
    - Coordinador: Ing. Pilar Urrutia

- Costos

  El costo de la propuesta asciende a $ 847,10.

6.2. Antecedentes de la propuesta

Debido a la problemática existente en la institución financiera se puede mencionar que al momento no existe los sistemas de seguridad apropiados para el normal y correcto almacenamiento de la información que en esta dependencia se desarrollan, por lo cual se torna urgente el desarrollo de una guía preventiva de seguridad que logre disminuir el impacto en el acceso a los datos de la Cooperativa. Tratando así a los clientes para que estos no sean una nueva víctima de fraude informático.

Por ello se recomienda el inmediato desarrollo de una guía preventiva de seguridad el cliente y personal de la Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo puedan encontrar una herramienta apropiada que ayude a combatir y por ende disminuir el impacto de los fraudes informáticos, consiguiendo con ello evitar daños para la institución ya sean estos económicos, físicos o morales.

6.3. Justificación

El realizar el análisis de los fraudes informáticos se torna en un aspecto primordial para la Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo, debido a la importancia de la información que en esta dependencia se genera, por ello la necesidad de disminuir su impacto y ayudar a satisfacer diversas necesidades, como:

- Protección la información de la institución

En la actualidad es bien sabido que existe la necesidad de crear un ámbito de seguridad informática en la institución financiera, dado que la parte más valiosa de ésta es la información y debido al gran número de casos de fraudes informáticos presentados en la actualidad.

Por ello es imprescindible que en la institución financiera se tome las medidas de seguridad necesarias para proteger y salvaguardar los datos resultantes de los diferentes procesos que en esta dependencia se desarrollan.

- Mejora de las estrategias de seguridad

Las medidas seguridad establecidas dentro de la institución en muchas ocasiones no son las adecuadas, por lo cual es menester mejorar o replantear las medidas ya existentes, tratando con ello de buscar que todos los usuarios de la institución así como sus empleados pongan en práctica lo establecido con la finalidad de evitar el ser víctimas de fraudes informáticos.

6.4. Objetivos

6.4.1. Objetivo General

Analizar los fraudes informáticos y su incidencia en el acceso a la información de la Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo.

6.4.2. Objetivos Específicas

- Realizar un estudio de campo que permita la determinación de la realidad existente en la institución financiera.
- Determinar las políticas de seguridad necesarias para salvaguardar la integridad de la información de la institución.
- Diseñar una guía preventiva de seguridad que permita disminuir los fraudes informáticos en la Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo.

6.5. Análisis de factibilidad

Para la gerencia máxima de la Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo se torna como una política imprescindible el desarrollo de una guía preventiva de seguridad para su entidad, acción viable en la actualidad gracias al alto grado de preparación del personal institucional.

La ejecución de dicho proyecto servirá de gran ayuda a la institución, como para el entorno en el que se desenvuelve dada la problemática que se presenta en la actualidad, puesto que la guía preventiva de seguridad buscará cambiar la mentalidad en el personal y clientes respecto a la protección de su información.

Para ello se cuenta con los elementos lógicos y físicos necesarios para el normal y correcto desarrollo de la guía de prevención, puesto que contamos con la información necesaria que facilite la toma adecuada de decisiones.

El proyecto puesto en ejecución está orientado personas de ambos sexos, es decir tanto hombres como mujeres, puesto que los dos cuentan con capacidades necesarias para hacer uso de este manual.

El proyecto mencionado está basado y de acuerdo a la economía de la Cooperativa de Ahorro y Crédito San francisco Ltda. Agencia Pelileo, es decir la institución financiera está en la capacidad de financiar la ejecución del proyecto, de la misma manera éste no atentará contra el medio ambiente en el que nos desenvolvemos.

A sí mismo no existen impedimentos legales que eviten o pongan algún tipo de traba para la ejecución del proyecto, más bien este se torna en un aporta para combatir a los cyberdelincuentes tratando con ello de una u otra manera disminuir el impacto en el acceso a la información que en estas se generan.

6.6 Informe Técnico

6.6.1 Datos informativos

- Titulo

  Análisis de los fraudes informáticos y su incidencia en el acceso a la información en la Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo.

- Institución ejecutora

  Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo.

- Director de tesis

  Ing. Pilar Urrutia

- Beneficiario

  Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo.

- Ubicación

  Quis Quis 412 y Av. Padre Chacón

- Tiempo estimado para la ejecución

  - Fecha de inicio: Febrero de 2012
  - Fecha de finalización: Agosto de 2012

- Equipo técnico responsable

  - Investigadora: Maribel Pico
  - Gerente: Ing. Freddy Zurita
  - Coordinador: Ing. Pilar Urrutia

- Costos

  El costo de la propuesta asciende a $ 847,10.

6.6.2. Tema

Análisis de los fraudes informáticos y su incidencia en el acceso a la información en la Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo.

6.6.3. Objetivos

6.6.3.1. Objetivo General

Analizar los fraudes informáticos y su incidencia en el acceso a la información de la Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo.

6.6.3.2. Objetivos Específicas

- Realizar un estudio de campo que permita la determinación de la realidad existente en la institución financiera.
- Determinar las políticas de seguridad necesarias para salvaguardar la integridad de la información de la institución.
- Diseñar de una guía preventiva de seguridad que permita disminuir los fraudes informáticos en la Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo.

6.6.4. Fundamentación teórica

6.6.4.1. Fraudes informáticos

Fraudes informáticos es toda acción consciente y voluntaria que provoca perjuicio a una persona natural o jurídica sin que necesariamente conlleve a un beneficio material para su autor, o que por el contrario produce un beneficio ilícito para su autor, y en cuya ejecución interviene indispensablemente dispositivos utilizados en las actividades informáticas.

En el desarrollo de un fraude informático se identifica varios elementos:

- Incidente
- Evento
- Riesgo

Incidente

Es cualquier evento relacionado con la seguridad de la información en el cual alguna política de seguridad ha sido violada. Es decir cualquier ocurrencia que es clasificada como un ataque en el sistema, la red o una estación de trabajo debe ser considerada un incidente. Se puede considerar como un incidente:

- Accesos no autorizados o a su vez intento de acceder a los sistemas de información.
- Interrupción o negación de servicio.
- Alteración o destrucción de los procesos de entrada, almacenamiento o salida de información.
- Cambios o intentos de cambio en hardware, software o firmware sin conocimiento del usuario.

Para lograr entender un ataque es necesario conocer la siguiente información:

1. **La naturaleza del ataque:** Es decir se debe saber con claridad porque el atacante escogió ese objetivo, al igual que se debe tener conocimiento de los riesgos que implican la ejecución del respectivo ataque y los daños que estos podrían causar.
2. **Alcance del ataque:** Una vez entendida la naturaleza del ataque, es necesario determinar que afecta o cual es el elemento que sufre los daños. Estos elementos pueden ser:
   - Hardware
   - Software
   - Datos
   - Personas
   - Documentación física
   - Comunicaciones
3. **Motivo del ataque:** Es decir las razones que impulsan el cometer el atraque, estas pueden ser:
   - Venganza
   - Codicia
   - Curiosidad
   - Necesidad de poder y control
   - Conducta compulsiva o adictiva
   - Beneficio personal monetario
   - Actuar en nombre de alguien más
   - Accidente o falta de conocimiento

Evento

El personal involucrado en la administración de un sistema de información puede determinar la presencia de un evento basado en un hecho evidente en el sistema, regularmente este hecho es solo un atributo o una característica del evento.

Se puede considerar como un evento:

- Colapso del sistema
- Despliegue inusual de graficas
- Algo que no esté "correcto"

Sin embargo un constante monitoreo por parte de los administradores de sistemas pueden determinar la ocurrencia de un evento dado que estos están basados en la violación de alguna política, un acto malicioso o una infracción externa.

Riesgo

La vulnerabilidad es una debilidad que expone un activo a una pérdida o daño físico o lógico. Se puede considerar como una vulnerabilidad:

- Fallas en las aplicaciones
- Redes no redundantes
- Seguridad física débil
- Fallas de los sistemas contra incendios

Un ataque es una persona o alguna condición que tiene alguna probabilidad de aprovechar algún tipo de vulnerabilidad. Se puede tomar como ejemplos de ataques a los siguientes, un servicio de inteligencia externo, el clima, entre otros.

El riesgo es descrito como la relación entre la vulnerabilidad y el evento.

Riesgo = Vulnerabilidad * Evento.

Vulnerabilidad= Determinada por el valor del bien afectado.

Riesgo= Probabilidad que un evento explote la vulnerabilidad dando como resultado el daño a un bien en particular. Para calcular el riesgo de un bien debe considerarse todas las vulnerabilidades y eventos relevantes.

6.6.4.2. Tipos de Fraudes Informáticos

Existen tres maneras de cometer fraudes informáticos:

1. **Fraudes cometidos mediante la manipulación de computadoras**

En los fraudes cometidos mediante la manipulación de computadoras se identifica los siguientes:

- **Manipulación de los datos de entrada:** Es el delito informático más común debido a que es fácil de cometer y difícil de descubrir.
- **Manipulación de programas:** Este delito consiste en modificar programas informáticos existentes o insertar nuevos programas o nuevas rutinas.
- **Manipulación de los datos de salida:** Se efectúa fijando un objetivo al funcionamiento del sistema informático. El claro ejemplo de éste delito es el fraude que se comete en los cajeros automáticos.
- **Fraude que aprovecha las repeticiones automáticas de los procesos de cómputo:** Es una técnica especializada que se denomina técnica del salchichón o salami en la que rodajas apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

2. Daños o modificaciones de programas

Este tipo de fraudes pueden ser ocasionados por:

- **Sabotaje informático:** Su intención es obstaculizar el normal funcionamiento del sistema de la institución.
- **Virus:** Se adhieren a los programas legítimos y se propagan otros programas informáticos.
- **Gusanos:** Se infiltra en programas legítimos de procesamiento de datos, pero éste no puede regenerarse.
- **Bomba lógica:** Requiere de conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro.

3. Acceso no autorizado a servicios y sistemas informáticos

- **Piratas informáticos:** El delincuente aprovecha la falta de medidas de seguridad para obtener acceso o descubrir deficiencias en las medidas de seguridad vigentes.

- **Reproducción no autorizada de programas informáticos:** Esto representa pérdidas económicas sustanciales para los propietarios legítimos.

6.6.4.3. Tipos de atacantes

Debido al avance tecnológico que se viene dando día a día y con ello la adquisición indiscriminada de la misma surge la grave problemática del mal uso de estas herramientas, actos realizados por los denominados cyberdelincuentes. Por tal motivo es sumamente importante saber quién es cada uno de ellos.

1. **Hackers**

Son individuos que dominan la programación y la electrónica para lograr comprender sistemas complejos y su respectivo funcionamiento. Las principales características de un hacker son:

- Adquieren conocimientos que luego son difundidos por él, para que otros sepan cómo funciona realmente la tecnología.
- Aprenden y trabajan solos y nunca se forman a partir de las ideas de otros, aunque es cierto que las comparten, si estas son interesantes.
- Tienen conocimiento de la creación de Virus o Crack de un software o sistema informático.
- Tiene el conocimiento, habilidad y deseo de explorar completamente un sistema informático.

2. **Crackers**

Su principal actividad es llevar a cabo el proceso para legalizar un software sin límites de tiempo y sin pagar por ello la respectiva licencia. Hecho por el cual es considerado el grupo más peligroso por los fabricantes de sistemas y los medios de comunicación.

Las principales características de un crackers son:

- Sus conocimientos son difundidos a otras personas.
- Tiene conocimientos de la parte de programación y la parte física de la electrónica.

- Diseña y fabrica programas y hardware para reventar software y comunicaciones como el teléfono, el correo electrónico o el control de otros computadores remotos.

3. Lammers

Son individuos con ganas de hacer hacking, pero que carecen de cualquier conocimiento. Las principales características de un lammer son:

- Ponen en práctica todo el software de hacheo que encuentran en Internet.
- Este tipo de personajes es quien emplea las terminales de trabajo, conocidas también como Back Office, Netbus o virus con el fin de generar miedo.

4. Copyhackers

Se desenvuelven sólo en el terreno del crackeo de Hardware, mayoritariamente del sector de tarjetas inteligentes empleadas en sistemas de telefonía celular. La principal motivación de estos nuevos personajes, es el dinero.

5. Bucaneros

Son individuos que no poseen conocimientos de la tecnología, ni tienen intención de adquirirlos, éstos sólo buscan el comercio negro de los productos entregados por los Copyhackers. El bucanero es simplemente un comerciante, el cual no tienen escrúpulos a la hora de explotar un producto de Cracking a un nivel masivo.

6. Phreaker

Son individuos con conocimientos profundos en telefonía. Buscan evitar los mecanismos de facturación de las compañías telefónicas, con lo cual se consigue llamar de cualquier parte del mundo sin costo prácticamente.

Las principales características de un Phreaker son:

- Tiene conocimientos en sistemas de telefonía, tanto terrestres como móviles.
- También poseen conocimientos de tarjetas prepago.

- Debe tener amplios conocimientos sobre informática

7. Newbie

Es un individuo novato que navega por Internet, que tropieza con una página de hacking y descubre la existencia de un lugar de descargas de buenos programas de hackeo. Lugar de donde decide bajar todo lo que puede para empezar a trabajar con los programas. Estos aprenden el Hacking de manera muy cauta.

8. Cript Kiddie

Se trata de simples usuarios de Internet, sin conocimientos sobre Hack o Crack. Estos de dedican a buscar programas de Hacking y después los ejecutan, sin tener idea de sus consecuencias y muchas veces sus mismas computadoras se ven afectadas.

6.6.4.4. Tipos de Ataques

En la actualidad existen diferentes técnicas y procedimientos al realizar un ataque, entre ellos podemos identificar los siguientes:

- Ingeniería social
- Shoulder surfing
- Negación de servicio
- Phishing
- Malware
- Conexiones inseguras
- Dominio falso
- Clickjacking
- Cross Site Scripting

1. Ingeniería Social

Es la manipulación del recurso humano de las instituciones para convencerlas de que ejecuten acciones o actos que normalmente no realizan para que revele toda la información necesaria para superar las barreras de seguridad.

Esta técnica es una de las más usadas y efectivas a la hora de averiguar nombres de usuarios y claves. Usualmente éste delito es realizado mediante llamadas telefónicas, haciéndose pasar por personal de la institución y requiriendo información personal con alguna excusa convincente.

2. **Shoulder Surfing**

Esta técnica consiste en espiar físicamente a los usuarios, para obtener generalmente claves de acceso al sistema. El Surfing explota el error de los usuarios de dejar su login y password anotadas cerca de la computadora, por lo cual cualquier intruso puede pasar por ahí, verlos y memorizarlos para su posterior uso. Otra técnica relacionada al surfing es aquella mediante la cual se ve, por encima del hombro, al usuario cuando teclea su nombre y password.

3. **Phishing**

Es una modalidad de estafa con el objetivo de intentar obtener de un usuario todos sus datos personales posibles, como claves, cuentas bancarias, números de tarjeta de crédito, entre otros para luego ser usados de forma fraudulenta. Este delito puede producirse de varias formas, desde un simple mensaje a su teléfono móvil, una llamada telefónica, una web que simula una entidad, y la más conocida a recepción de un correo electrónico.

4. **Malware**

Éste término engloba a todo tipo de programa o código de computadora cuya función es dañar un sistema o causar un mal funcionamiento. Dentro de este grupo podemos encontrar términos como: Virus, Troyanos, Gusanos, etc.

5. **Dominio falso**

También denominada Pharming, consiste en suplantar al Sistema de Resolución de Nombres de Dominio o DNS, con la finalidad de conducirle al usuario a una página Web falsa. El delincuente realiza el redireccionamiento a las páginas Web

falsas a través de un código malicioso, para esto se requiere que el atacante logre instalar en su sistema alguna aplicación o programa malicioso.

6. **Conexiones inseguras**

Una conexión insegura se origina cuando intercambiamos datos o nos conectamos con sitios sin certificados de seguridad al día.

7. **Clickjacking**

Es una técnica maliciosa muy parecida al phishing ya que se engaña al usuario para obtener el control de su equipo e importantes beneficios de ello. Su fin es que el internauta haga clic en lugares específicos de algún sitio que, por lo regular, es descarga de archivos maliciosos para después obtener acceso a sus sistemas.
Es decir éste tipo de ataque informáticos necesitan antes una acción de confirmación u otra acción del usuario que les abra las puertas a la vulnerabilidad.

8. **Cross Site Scripting**

Es un tipo de vulnerabilidad que puede darse en cualquier aplicación web en la que se muestre en pantalla cualquier tipo de datos sobre los que el usuario tenga influencia directa. Como es de suponer, esto abarca a gran porcentaje de sitios web.

6.6.4.5. Seguridad mediante cortafuegos

El principal mecanismos de seguridad del sistema financiero de la Cooperativa San Francisco Ltda. Agencia Pelileo es el de mantener a los intrusos fuera de su red, permitiéndole a ésta realizar su trabajo de manera normal.

Para ello la tecnología fundamental utilizada en estos casos es la instalación de un **firewall.** Un cortafuegos es un sistema o grupo de sistemas informáticos situados en el perímetro de una red para proteger todas sus vías de acceso estableciendo un control del tráfico de entrada y salida. Se encarga sólo de la protección contra la

diseminación de los ataques derivados de accesos públicos, es decir, sólo puede controlar el tráfico que pasa a través de él.

El cortafuegos tiene una doble misión:

- Bloquear el tráfico proveniente de direcciones no autorizadas o que acceden aplicaciones restringidas.
- Permitir el flujo de tráfico de las operaciones legales.

Los principales aspectos críticos que deberá resolver la configuración del cortafuegos en el sistema financiero se centra en las siguientes problemáticas:

- Usurpación de la identidad e integridad de la información.
- Permitir el acceso a las direcciones de origen validadas y autorizadas.
- Permitir el acceso a las aplicaciones en función de la identidad validada.
- Filtrado de solicitudes de conexión desde nuestra red a Internet.
- Protección de los datos de identidad de nuestros usuarios en los accesos autorizados a Internet.
- Realizar todas las funciones anteriores sin afectar a las prestaciones y funcionalidades de Internet que los usuarios internos demandan.

6.6.4.6. Seguridad Global en la Organización

Al mencionar seguridad global, nos referimos a brindar la protección necesaria a todos los recursos informáticos de la institución, aún cuando estén o no interconectados. Dada esta situación es de vital importancia siempre tener en cuenta que la seguridad comienza y termina con personas, por lo cual es de suma importancia capacitar al recurso humano de la institución.

La mejor manera de proporcionar seguridad informática a la Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo, es creando conciencia a cada uno de los miembros de institución sobre la importancia y la sensibilidad de la información y servicios que favorecen el desarrollo de la organización y su buen funcionamiento.

6.6.4.7. Valor de los datos

Establecer el valor de los datos es algo totalmente relativo, pues la información constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, la documentación o las aplicaciones.

Situación que puede traer consigo grandes problemas para la institución, puesto que los datos generados dentro de la misma constituyen el motor principal para el normal y correcto funcionamiento de la organización.

6.6.4.8. Impacto en la organización

La implementación de medidas de seguridad en la institución financiera puede traer consigo varios tipos de problemas que afectan el funcionamiento de la organización. Entre los principales problemas tenemos:

Incrementar la complejidad en la operatoria de la organización, tanto técnica como administrativa.

- Nuevas tareas para la parte técnica, como por ejemplo cambio de privilegios y restricciones a algunos usuarios.
- Administrativamente se les deberá comunicar por medio de una nota de los cambios realizados y en qué les afectará.

6.6.4.9. Visibilidad de la falta de seguridad

Basándonos en un reciente estudio de Datapro Research Corp. se puede resumir que los problemas de seguridad en los sistemas informáticos responden a la siguiente distribución:

- Errores de los empleados 50%
- Empleados deshonestos 15%
- Empleados descuidados 15%
- Intrusos ajenos a la Empresa 10%
- Integridad física de instalaciones 10%)

Dada esta información se puede notar que el 80% de los problemas, son generados por los empleados de la organización, y, éstos se podrían tipificar en tres grandes grupos:

- Problemas por ignorancia

- Problemas por haraganería
- Problemas por malicia

6.6.4.10. Implementación

La implementación de medidas de seguridad, es un proceso técnico administrativo. Este proceso debe estar fuertemente apoyado por el sector gerencial, ya que sin ese apoyo, las medidas que se tomen no tendrán la fuerza necesaria.

Hay que tener muy en cuenta la complejidad que suma a la operatoria de la organización la implementación de estas medidas.

Resulta claro que proponer o identificar una política de seguridad requiere de un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

6.6.4.11. Nivel de seguridad

La seguridad debe contemplar no sólo que no accedan intrusos, sino que los sistemas y las aplicaciones funcionan y son utilizados correctamente. Los niveles de seguridad no pueden, ni deben, ser iguales para todos los elementos, ya sean éstos usuarios, aplicaciones, entre otros quienes gestionan la información.

Las medidas de seguridad deben contemplar algunos de los siguientes aspectos:

- Identificación biunívoca de los usuarios (Users ID)
- Claves de acceso de al menos 6 caracteres y ficheros de claves protegidos y encriptados.
- Modificación periódica de las claves de acceso, como mínimo cada tres meses
- Registros de control del uso correcto, intentos incorrectos
- Acceso remoto seguro
- Cifrado y firma digital en las comunicaciones
- Salvaguardas y copias de seguridad.
- Planificación de desastres.

- Formación de los usuarios en los aspectos de seguridad.

6.6.4.12. Análisis de los fraudes informáticos

Antes de dar solución a la problemática existente de los fraudes informáticos en la Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo mediante la creación de una guía preventiva de seguridad, analizaremos detenidamente cada uno de ellos para poder determinar como afectan el normal funcionamiento de la institución financiera.

- **Analizando la Ingeniería Social y Shoulder Surfing**

Al momento de recopilar la información necesaria para el desarrollo del presente trabajo investigativo, fue necesario realizar investigaciones de campo en las cuales se percató que el personal de la institución financiera, así como sus respectivos clientes no toman las medidas de seguridad necesarias para salvaguardar su información.

Es así que en las visitas realizadas a la Cooperativa San Francisco sobresalen los siguientes errores:

- Anotar información de suma importancia en hojas volantes, para luego arrojarlas a la basura.
- Dejar su login y password anotas cerca a la computadora o a su vez colgada de la pantalla de la computadora.
- Facilitar información sensible de usuarios de la institución vía telefónica.
- No verificar la procedencia de las llamadas telefónicas, antes de facilitar información.
- Revisión de los enlaces sugeridos en los correos electrónicos de destinatarios desconocidos.
- Excesivo uso de sistemas de mensajería, redes sociales y otras aplicaciones no relacionadas con los sistemas de la cooperativa.

Tomando en cuenta los descuidos de seguridad realizados con respecto a la ingeniería social, fácilmente se puede concluir que el obtener información personal de los usuarios como claves de acceso, login, saldos disponibles, entre otros, se torna en una tarea fácil.

Para citar un claro ejemplo de éste tipo de fraude seguimos los siguientes pasos:

Paso 1: Se realiza una llamada telefónica a un agente de crédito desde el teléfono móvil de una persona ajena a la institución financiera.

Paso 2: Solicitar información de un determinado cliente de la cooperativa.

Paso 3: Se recibe la información requerida, sin antes haberse indagado la procedencia de la llamada.

- **Analizando el Phishing**

Debido a que el principal objetivo de éste tipo de delito informático, es obtener información personal de los usuarios de la institución financiera, a través de la suplantación de la identidad de la empresa o a su vez de su personal, se ha podido determinar que los errores más comunes cometidos por el recurso humano de la Cooperativa son:

- Responder a mensajes del teléfono móvil solicitando datos personales.
- Responder a llamadas que solicitan actualización de datos sin comprobar su origen.
- Ingreso a sitios sugeridos por ventanas emergentes, sin introducir la URL en la barra de búsqueda como sería lo indicado.
- Responder correos electrónicos sin verificar si éstos provienen de las instituciones financieras.

Para citar un ejemplo de éste delito, seguimos los siguientes pasos:

Paso 1: Creación de una nueva cuenta de correo por ejemplo: **coac-sanfra@hotmail.com.**

Paso 2: Envío de un mensaje de correo electrónico cuyo contenido sea la solicitud de información personal, como por ejemplo:

SAN FRANCISCO
INSTITUCIÓN FINANCIERA COOPERATIVA

ESTIMADO CLIENTE

Estamos trabajando para proteger a nuestros usuarios contra fraude. Le informamos que su cuenta ha sido seleccionada para comprobar que la seguridad de su cuenta no está comprometida, necesitamos confirmar su identidad para lo cual solicitamos se nos facilite su número de cuenta, nombres y apellidos completos, dirección, teléfono, móvil, e-mail.

Por favor tenga en cuenta que si en 24 horas no confirma su información, nos veremos obligados a bloquear su cuenta para su protección.

SERVICIO DE ATENCION AL CLIENTE

Paso 3: Recibir la respuesta al mensaje enviado, como por ejemplo:

GRACIAS POR SELECCIONAR MI CUENTA

Nombres y Apellidos: Diego XXXX Sánchez XXXX

Número de Cuenta: 541XXX

Dirección: Pelileo-XXX

Convencional: 032831-XXX

Móvil: 099360XXXX

e-mail: **diego_xxxxxxx_x@hotmail.com.**

Entonces podemos darnos cuenta que la información personal solicitada, es obtenida fácilmente, situación preocupante para la institución financiera.

- **Analizando los Malware**

Los códigos maliciosos tienen como fin dañar los sistemas de la institución, ya sean éstos, daños en aplicaciones o a su vez la inhabilitación total del equipo. Se destaca que los principales errores cometidos en las instituciones financieras son:

- Pasar por alto la solicitud de actualizaciones ya sea en el sistema o en aplicaciones.
- Descargas y ejecución de software encontrado en la web por simple curiosidad, sin tener idea de las verdaderas consecuencias que éstas acciones traerían.
- Ingreso a links de procedencia sospechosa, colgados en las redes sociales Messenger, Twitter, Facebook, etc.
- Abrir archivos adjuntos o seguir un enlace de correos no solicitados, también denominados Spam.

Para comprobar ésta situación seguimos los siguientes pasos:
Paso 1: Solicitar a un Agente de Crédito se proporcione información enviada por el Gerente hacia su correo personal.
Paso 2: Se comprueba que al ingresar al buzón de entrada de su cuenta de correo, no verifica si los mensajes existentes provienen de contactos autorizados, sino más bien, los abre y sigue los links proporcionados en ellos de manera indiscriminada.

- **Analizando varios fraudes**

En el desarrollo de las actividades cotidianas del personal de la Cooperativa de Ahorro y Crédito san Francisco Ltda. Agencia Pelileo, se ha podido determinar observar que el recurso humano de dicha institución fácilmente podría ser víctimas de ataques informáticos, debido a que frecuentemente cometen las siguientes imprudencias:

- Poco interés por determinar si el sitio web que está usando es seguro.
- Poca atención en la URL del sitio al cual desean conectarse (https).

- Uso frecuente y en ocasiones indiscriminado de portales de descargas, los cuales son utilizados para infectar con algún tipo de malware.
- Descuido al revisar si el sitio web visitado posee certificados de seguridad.
- Confirmar la ejecución de aplicaciones, de las cuales no se sabe su origen.

Para comprobar ésta situación se realizaron los siguientes pasos:

Paso 1: Solicitar a un miembro del personal de la Cooperativa se nos facilite una información descargada desde la web.

Paso 2: Percatarse y evaluar los descuidos de seguridad cometidos por el personal.

6.6.4.13. Guía Preventiva de Seguridad

Una guía preventiva es una herramienta que proporciona la ayuda necesaria al usuario, para que éste tenga la paute para proteger alguna manera un sistema informático o medio de comunicación, debido a la importancia de la información que en ellos reposa o a su vez transmite. De allí surge la importancia de la mencionada herramienta pues ésta se encarga de brindar tips o recomendaciones que el usuario de manera cauta deberá poner en práctica para tratar de salvaguardar sus intereses.

La guía preventiva de usuario contará con características importantes que logren cubrir con las expectativas de los usuarios, quienes serán los encargados de explotar toda la información que ésta contendrá. Entre las características y contenido de la guía preventiva de usuario podemos mencionar:

- Uso de términos de fácil comprensión para el usuario.
- Interfaz clara y comprensible.
- Descripción de fraude informático.
- Mención de los fraudes informáticos más frecuentes.
- Descripción de cada uno de los fraudes informáticos.
- Recomendaciones para prevenir cada uno de los fraudes informáticos.
- Tips generales de cómo defenderse de los ataques informáticos.

La guía preventiva de usuario busca anticiparse al hecho que la Cooperativa de Ahorro y Crédito "San Francisco" Ltda. Agencia Pelileo sea víctima de algún tipo de fraude informático, tratando con ello que los usuarios tengan por lo menos conocimientos básicos para defenderse ante un ataque informático. Además de ello se busca cambiar la mentalidad de los usuarios y personal de la institución acerca de esperar a que las cosas sucedan para tomar las medidas necesarias, por qué no anticiparnos a los hechos y tomar cartas en el asunto, para con ello evitar de una u otra manera el ser víctimas de fraude informático.

La guía preventiva de usuario desarrollada para la Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo tendrá la siguiente información:

6.6.4.14. Diseño de la guía preventiva de seguridad

GUÍA DE USUARIO

FRAUDES INFORMÁTICOS

Gráfico 6. 1. San Francisco

Resumen

Este documento describe el proceso de asegurar y fortalecer el nivel de seguridad de los sistemas informáticos de la institución financiera, con la finalidad de prevenir el ser víctima de fraudes informáticos. Cubre los fraudes tecnológicos más comunes, así como las respectivas medidas que deben tomarse para combatirlos, de igual manera proporcionan información adicional con recomendaciones para contrarrestar los diferentes delitos tecnológicos.

Presentación

En la actualidad el internet, es una herramienta que además proporcionarnos información útil en ocasiones se torna en una repositorio lleno de peligros para la institución.

Dado que en el mundo existen individuos dispuestos a cometer actos ilícitos y fraudulentos, cada individuo está en la obligación de mitigar los riesgos, para lo cual la mejor herramienta es el mantenerse constantemente informados.

Es así que la Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo, siempre en constante preocupación por su seguridad, tiene a bien presentarles de manera clara, breve y precisa las diferentes modalidades de fraudes informáticos que hacen mal uso de la tecnología.

FRAUDES MAS FRECUENTES

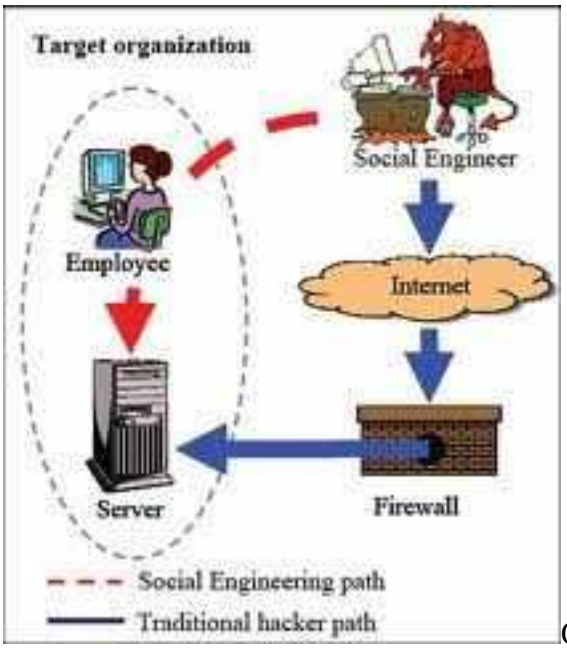
1. INGENIERÍA SOCIAL

Consiste en la manipulación de las personas bajo su propia voluntad realicen actos que normalmente no harían; el atacante puede aprovechar el desconocimiento de unas mínimas medidas de seguridad por parte de personas relacionadas de una u otra forma con el sistema para poder engañarlas en beneficio propio.

Reglas de seguridad:

- Instruir a los usuarios y personal de la institución financiera para que no divulguen información sensible con desconocidos o en lugares públicos.
- Tener servicio técnico propio o de confianza.
- Asegurarse que las personas que llaman por teléfono son quien dicen ser.
  Por ejemplo: Realizar preguntas que únicamente el verdadero usuario podría responder, o devolver la llamada de manera de verificar la misma.

- Llevar a cabo programas de concientización sobre la seguridad de la información.



C

Gráfico 6. 2. Ingeniería social

2. PHISHING

Esta es una modalidad de estafa diseñada con la finalidad de robarle la identidad. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños. Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes. Los mensajes falsos parecen provenir de sitios Web reconocidos o de su confianza, como el de su institución financiera.

Reglas de seguridad:

- Nunca responda a solicitudes de información personal a través de correo electrónico.
- En caso de alguna duda póngase en contacto con la entidad que supuestamente le ha enviado el mensaje.
- Para visitar sitios Web, introduzca la dirección URL en la barra de direcciones.
- Asegúrese de que el sitio Web utilizado sea cifrado.
- Consulte frecuentemente sus saldos financieros, es decir las cuentas de ahorro, tarjetas de Créditos.
- Comunique los posibles delitos relacionados con su información personal a las autoridades competentes.

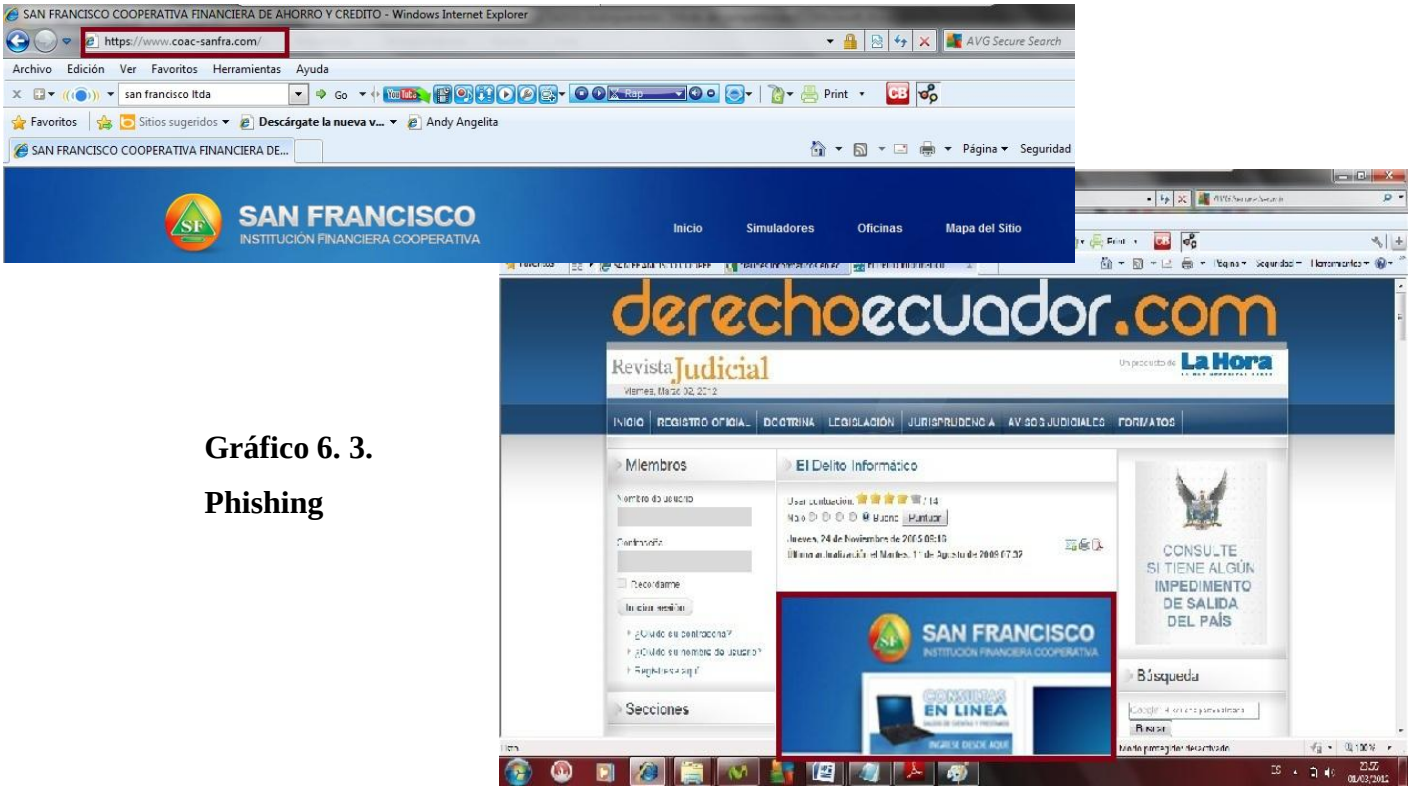


Gráfico 6. 3.

Phishing

3. MALWARE

Son todos los programas o códigos de computadora cuya función es dañar un sistema y dañar la computadora sin el conocimiento de su dueño, con finalidades muy diversas.

Reglas de seguridad:

- Si recibe un e-mail y este le lleva a una página de Internet desconocida, no acceda al sitio Web, porque es seguro que el contenido será malicioso.
- Cuando reciba la alerta de que el programa está por expirar, no ignore la actualización, no tendrá que comprar otro producto, sólo deberá autentificarlo para continuar teniendo actualizaciones.
- Asegúrese de tener un programa de antivirus en su computadora.
- Realice las actualizaciones automáticas que le pida el programa, porque contienen cientos de archivos de protección contra los nuevos virus que aparecen cada día.
- Nunca abra un archivo adjunto de un e-mail de un remitente desconocido.

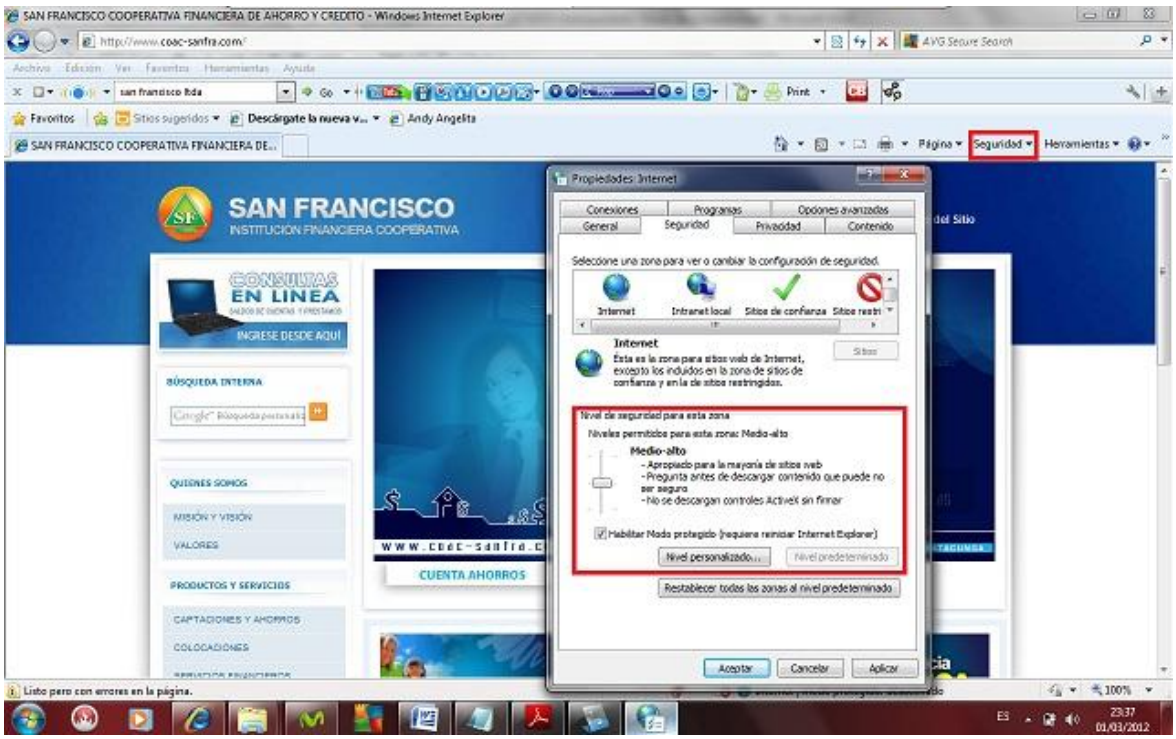


Gráfico 6. 4 Malware

4. CONEXIONES INSEGURAS

Se produce cuando intercambiamos datos o nos conectamos con sitios sin certificados de seguridad al día, sin validaciones de seguridad de terceras partes. Las conexiones a sitios sensibles deben estar certificadas por entidades terceras, ya que toda transmisión de información puede ser vulnerada y necesita estar constantemente auditada en las medidas de seguridad que ofrece.

Reglas de seguridad

- Verificar que exista siempre una conexión segura del tipo **https://**...
- No ingresar si el certificado del sitio reporta errores como:
    - Certificado emitido por una entidad desconocida
    - Certificado emitido para otro sitio
    - Certificado vencido

Gráfico 6. 5. Conexión insegura

5. DOMINIO FALSO

Un dominio falso es un nombre falsificado de un sitio web.

Por ejemplo: El dominio seguro es www.coac-sanfra.com y el dominio falso podría ser www.co@c-sanfra.com.

Por ello se debe tener mucho cuidado con los dominios falsos, ya que el sitio al que le llevan es exactamente igual al original. Generalmente, estos dominios falsos llegan a través de e-mails fraudulentos que solicitan la actualización de datos en un sitio Web de dominio falso.

Reglas de seguridad:

- Se debe permanecer alerta a la URL https://www.coac-sanfra.com del sitio al cual nos conecta el link. Si este no coincide exactamente con la URL de sitio oficial de la institución financiera, es mejor que no siga navegando en él.
- Tenga siempre activas las alertas de su navegador, como también, reportar sitios no confiables cada vez que se encuentre con uno de ellos.

Dar clic en la opción Seguridad del navegador.

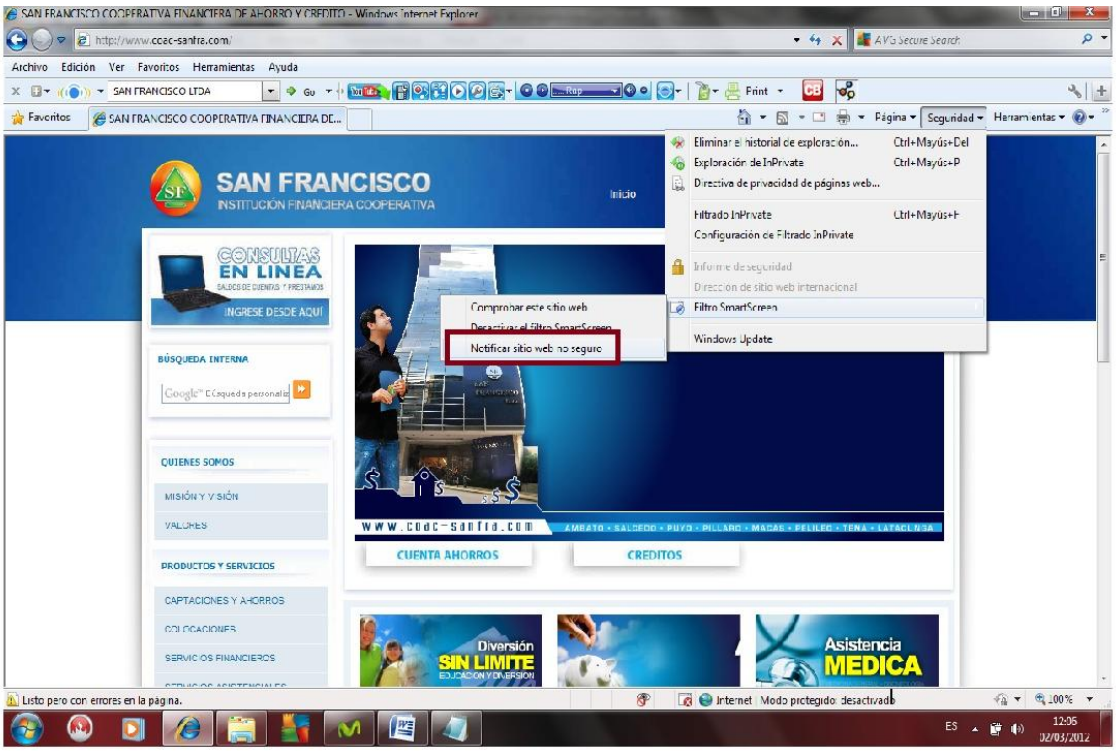


Gráfico 6. 6. Dominio falso 1

Luego de ello siga el Menú de Smart Screen Filter hasta la opción Report Unsafe Website o reportar sitio inseguro

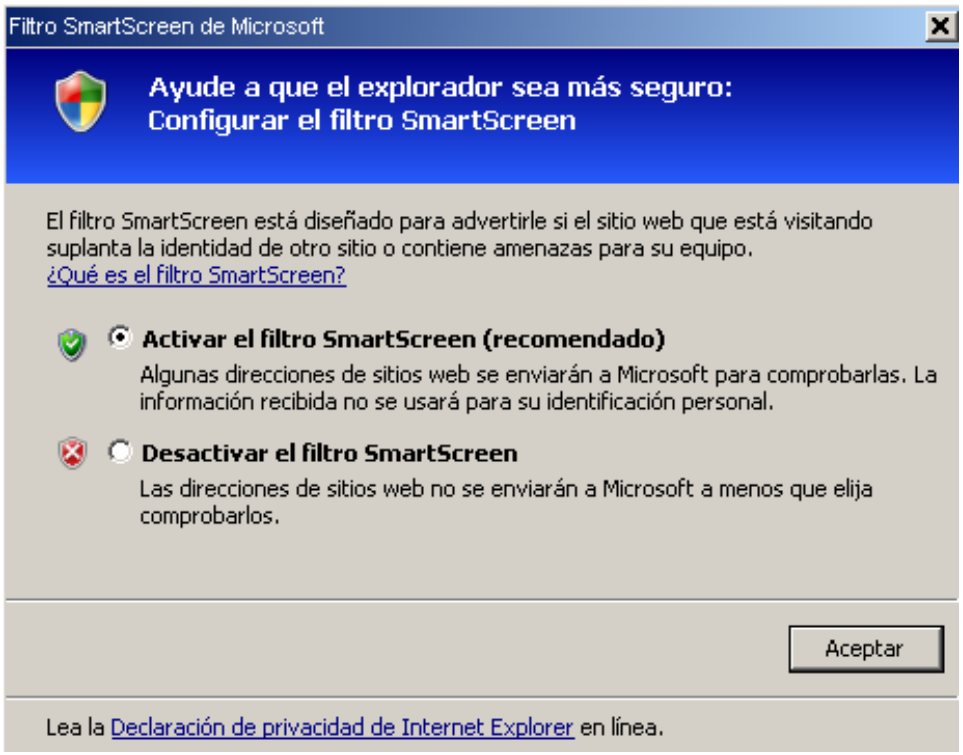


Gráfico 6. 7. Dominio falso 2

6. CLICKJACKING

Son los sitios que escondiendo o camuflando botones y diálogos, hacen que los navegantes acepten enviar información o instalar programas.

Reglas seguridad

- Nunca acceda a su sitio de confianza desde links publicados en sitios desconocidos, pues dichos links pueden estar montados sobre botones falsos que le llevarán al sitio o archivo malicioso.
- Recuerde tener activas las alertas del navegador.
- Comprobar el tipo de páginas hacia las que nos dirige nuestro navegador de Internet.
- Tener actualizado el sistema operativo y los navegadores web en sus últimas versiones.
- Para protegerse usted del Clickjacking puede instalar una herramienta denominada ClearClick, la misma que chequea que no esté usando un botón pensando que es otro y si es así, le avisaría

Uso del ClearClick

Gráfico 6. 8. Clearclick 1

Gráfico 6. 9. Clearclick 2

7. CROSS SITE SCRIPTING

Es una vulnerabilidad que aprovecha la falta de mecanismos de filtrado en los campos de entrada que permiten el ingreso y envió de datos sin validación alguna, aceptando el envió de scripts completos, pudiendo generar secuencias de comandos maliciosos que impacten directamente en el sitio o en el equipo de un usuario.

Reglas de seguridad:

- Se debe evitar el acceso a sitios potencialmente no seguros a través de links sospechosos. .
- Tener activada la protección del navegador de Internet para evitar estos fraudes.

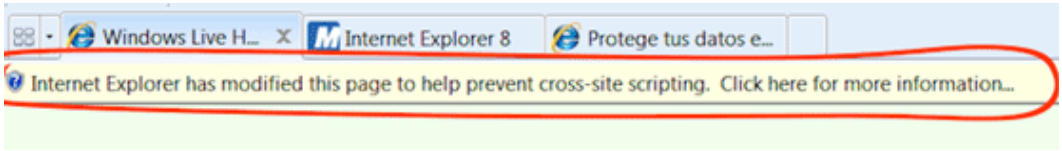


Gráfico 6. 10. Cross site

REGLAS GENERALES PARA PROTEGERNOS DE CYBER ATAQUES

- Nunca hacer clic en enlaces que le lleguen por e-mail queriendo que visite el sitio de su institución financiera y le solicite identificarse.
- Asegurémonos estar visitando el sitio web oficial de la Cooperativa, revisando que la dirección sea la correcta.
- No olvide cerrar su sesión antes que otra persona utilice su ordenador de manera que éstas no puedan acceder a su información.
- No descargue archivos de procedencia dudosa.
- Mantenga siempre al día su navegador de Internet.
- Mantener las máquinas actualizadas y seguras físicamente
- Contar con auditorias de seguridad y sistemas de detección.
- Mantenerse informado constantemente sobre cada unas de las vulnerabilidades encontradas y parches lanzados.
- Contar con personal especializado en cuestiones de seguridad.
- Capacitar al usuario de manera constante.
- No realice operaciones bancarias a través de redes abiertas disponibles en sitios públicos.
- Realizar transacción bancaria vía web únicamente desde su casa u oficina,
- Al realizar transacciones bancarias cierra todas las ventanas que no tengan que ver con el proceso que está realizando, especialmente facebook o correos electrónicos.
- Mientras realiza operaciones transaccionales no descuide su atención del proceso.
- Solicite información a su institución financiera acerca de los productos, servicios y medidas de seguridad implementadas y que se encuentran a su disposición.
- Instalar programas antivirus en su ordenador y mantenerlos actualizados.
- Revise con frecuencia sus estados de cuenta para detectar consumos no reconocidos.
- No anote ni comparta sus contraseñas con nadie.
- Elija contraseñas fáciles de recordar, pero difíciles de adivinar.

6.6.4.15. Validando la guía preventiva de seguridad

Con la finalidad de cubrir las expectativas del trabajo realizado en la institución financiera se realizó algunas pruebas, las cuales ayudaron a determinar la ayuda proporcionada por la guía preventiva, por lo cual se puede citar los resultados obtenidos:

- No se divulga información sensible de la cooperativa y de sus respectivos clientes.
- Se evidencia que no existen hojas volantes con las cuentas de usuario y contraseñas colgadas en los monitores del computador de la institución.
- Se informa al personal técnico sobre cualquier sospecha de malware.
- No se ingresa a links que aparecen en ofertas publicitarias.
- Las URL son digitadas asegurándose de que el sitio web al que se desea acceder sea seguro.
- No se ingresa a redes sociales mientras está utilizando los sistemas de la cooperativa.
- Cierran su sesión de usuario antes de abandonar su puesto de trabajo.
- Verifica el origen de las llamadas recibidas a su teléfono móvil o a la extensión asignada para su uso dentro de la cooperativa.
- No ingresa información personal, a pesar de ser solicitada mientras se navega en la web en sitios desconocidos.

6.7. Conclusiones y Recomendaciones

6.7.1. Conclusiones

- La guía preventiva de seguridad ofrecerá información útil y de fácil comprensión para todos los usuarios de los sistemas informáticos de la institución financiera, logrando con ello que éstos tengan las pautas necesarias para combatir los fraudes tecnológicos.

- La mayor debilidad encontrada en los sistemas informáticos dentro de Cooperativa de Ahorro y Crédito San Francisco Ltda., es el desconocimiento existente en el recurso humano de la institución.

- En la actualidad existe una gran cantidad de fraudes informáticos, por lo cual se hace difícil el seleccionar los más comunes, puesto que día a día aparecen nuevas amenazas para nuestros los sistemas informáticos.
- La principal finalidad de la guía preventiva de seguridad es crear una conciencia de prevención en el personal de la institución, como en sus respectivos clientes.

6.7.2. Recomendaciones

- Se sugiere al personal de la institución financiera como a los clientes de la misma mantenerse constantemente informados sobre las amenazas existentes para los sistemas informáticos, con la finalidad de combatirlos o a su vez evitarlos.
- Se considera necesario realizar una capacitación a todo el personal de la institución, inicializando desde las funciones básicas de un computador para poder proseguir con las amenazas existentes para nuestro sistema.
- El personal de la institución deberá ser más cuidadoso con el manejo de la información, debido a la importancia que representa.
- Se sugiere que exista un stand de trabajo individual para cada miembro del personal, para evitar el compartir contraseñas y cuentas de usuario, y al mismo tiempo mantener confidencialidad en los datos.

6.8. Bibliografía

Información en documentos impresos

- PAZMAY, Galo (2004). "Guía práctica para la elaboración de tesis y trabajos de investigación", Editorial Freire, Riobamba.
- URBINA, Vanessa. (2005. Auditoria de fraudes en sector financiero privado en el periodo 2000-2003). Guayaquil-Ecuador.
- VEGA, Jessy. (2009. Diseño de un manual de control interno para el Departamento Financiero en la escuela superior politécnica de Chimborazo-Riobamba, aplicando la nueva normativa y herramientas informáticas que rigen para el sector público en el año 2009). Riobamba-Ecuador.

- VIZUETE, Deisy. (2005. Alcance y Metodología para el análisis de riesgos y para la seguridad de la información para la empresa Promix Ecuador C.A). Loja-ecuador.

Información en documentos electrónicos

- SALAZAR, Walter (2010). Tecnología. 22/10/2011. http://elazahar.blogspot.com/2007/07/conceptos-tecnologa.html. Tecnología a tu alcance.
- RESTREPO, Guillermo (2011). Tecnología. 22/10/2011. http://www.monografias.com/trabajos11/tecnol/tecnol.shtml. Tecnología actual.
- ORTIZ, Antonio (2004). Informática. 24/10/2011. http://www.error500.net/garbagecollector/archives/categorias/apuntes/concepto_de_informatica.php. Curso de informática básica.
- CHÁVEZ, Aníbal (2011). Informática. 24/10/2011. http://es.wikipedia.org/wiki/Inform%C3%A1tica. Informática.
- MERLAT, Máximo (2011). Seguridad informática. 24/10/2011. http://www.alegsa.com.ar/Dic/seguridad%20informatica.php. Definición de seguridad informática.
- CALDERÖN, José (2011). Seguridad informática. 25/10/2011. http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica. Seguridad Informática.
- SARZANA, Carlos (2009). Seguridad informática. 25/10/2011. http://www.monografias.com/trabajos/hackers/hackers.shtml.Seguridad informática-Hackers
- LIMA, María de Luz (2009). Delitos informáticos. 25/10/2011. http://www.derechoecuador.com/index.php?option=com_content&task=view&id=30. El delito informático.
- HUILCAPI, Arturo (2011). Delitos informáticos. 25/10/2011. http://es.wikipedia.org/wiki/Delito_inform%C3%A1tico. Delito informático.
- LORENZO, Patricia (2011). Delitos informáticos. 25/10/2011. http://www.delitosinformaticos.info/delitos_informaticos/definicion.html. Definición de delito informático.
- LOERINCS, Gabor (2001). Fraudes informáticos. 25/10/2011. http://www.monografias.com/trabajos12/conygen/conygen.shtml. Conceptualización y generalidades de fraude informático.

- CARRION, Hugo (2001). Fraudes informáticos. 25/10/2011. http://www2 .compendium.com.ar/juridico/depablo.html. Derecho Informático-Delito Informático.
- VILLASMIL, Jonathan (2009). Instituciones financieras. 26/10/2011. http://www.consumoteca.com/economia-familiar/economia-y-finanzas/entidades-financieras. Instituciones financieras.
- VILLASMIL, Jonathan **(**2009). Información financiera. 26/10/2011. http://www.mailxmail.com/curso-comunicacion-informatica-historia-computacion/concepto-160-informacion-160-informatica. Información
- MAYA, Jesús (2009). Información. 26/10/2011. http://es.wikipedia.org/wiki/Informaci%C3%B3n. Información financiera
- ANDRADE, Wilson (2010). Vulnerabilidad. 26/10/2011. http://www.alegsa.com.ar/Dic/vulnerabilidad.php. Vulnerabilidad.
- PËREZ, Carlos (2011). Acceso a la información. 26/10/2011. http://es.wikipedia.org/wiki/Acceso_a_la_informaci%C3%B3n. Acceso a la información.
- VILLANUEVA, Ernesto (2011). Acceso a la información. 27/10/2011. http://www.fpchiapas.gob.mx/transparencia/inicio/definicion_acceso.php. Acceso.
- LUQUE, José María (2010).¿Qué es el Phishing y cómo protegerse?. http://seguridad.internautas.org/html/451.html. Phishing.
- BAQUIA, Pablo (2010). Pharming, una nueva técnica de fraude. http://www.helpdesk-software.ws/es/it/11092005.htm. Dominio falso.
- CONDES, Santiago (2012).Conexiones Inseguras. http://www.bci.cl/seguridad/fraudes/conexiones_act.html. Conexión insegura.
- MEDINA, Mercedes (2012).Atentos al clickjacking.http://www.asersa.com/asersa/boletinPdf/ATENTOSALCLICKJACKING.pdf. Clickjacking

Anexos

ANEXO 1

Fórmula de cálculo de la muestra

$$n = \frac{PQN}{(N-1)E^2/K^2 + PQ}$$

PQ= Constante de varianza población (0,25)

N= Tamaño de la población

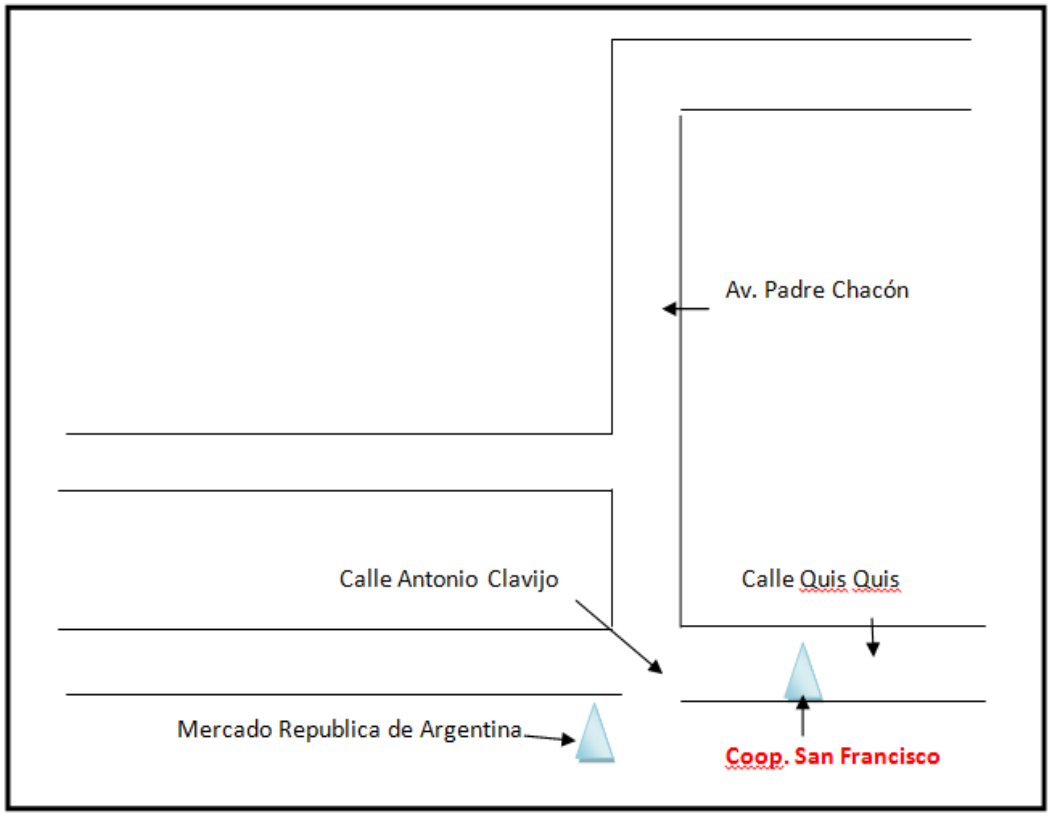
E= Error máxima posible va de 1% (0,01) al 10% (0,1)

K= Coeficiente de error 2

ANEXO 2

Croquis (donde está ubicado el problema)

CENTRO DEL CANTON PELILEO



ANEXO 3

Estructura de la Encuesta a Clientes

UNIVERSIDAD TÈCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

LUGAR A ENCUESTAR:

OBJETIVO DE LA ENCUESTA:

Señores, su veracidad en las respuestas permitirá al investigador desarrollar un trabajo real y efectivo.

Agradecemos su colaboración y garantizamos absoluta reserva con su información.

CUESTIONARIO DIRIGIDO A LOS CLIENTES DE LA COOPERATIVA "SAN FRANCISCO"

Gracias por su colaboración

Fecha de aplicación:

1. ¿Cree usted que ha sido víctima de algún tipo de fraude informático?
   ( ) Si
   ( ) No
2. ¿En alguna ocasión ha notado irregularidades en el movimiento de transferencias de su cuenta personal?
   ( ) Si
   ( ) No
3. ¿Cree usted que los sistemas informáticos utilizados en la Cooperativa San Francisco son seguros?
   ( ) Si
   ( ) No
4. ¿Cuál cree usted sea la finalidad de los delincuentes al cometer fraudes informáticos?
   ( ) Económicos
   ( ) Causar daños materiales institución
   ( ) Causar daño moral

5. ¿Según su criterio el personal de la institución está preparado para dar soluciones a los diferentes problemas que se presenten?

( ) Si

( ) No

6. ¿Tiene usted conocimiento que la Cooperativa de Ahorro y Crédito San Francisco cuenta con un sitio web a disposición de sus clientes?

( ) Si

( ) No

7. ¿Tendría usted la confianza de realizar transacciones electrónicas en el sitio oficial de la institución?

( ) Si

( ) No

8. ¿En caso de ser víctima de fraude informático estaría dispuesto a realizar la respectiva denuncia ante las autoridades correspondientes?

( ) Si

( ) No

( ) No se

ANEXO 4

Estructura de la Encuesta a Administradores de Sistemas

UNIVERSIDAD TÈCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

LUGAR A ENCUESTAR:

OBJETIVO DE LA ENCUESTA:

Señores, su veracidad en las respuestas permitirá al investigador desarrollar un trabajo real y efectivo.

Agradecemos su colaboración y garantizamos absoluta reserva con su información.

CUESTIONARIO DIRIGIDO AL ADMINISTRADOR DE SISTEMAS DE LA COOPERATIVA

Gracias por su colaboración

Fecha de aplicación:

1. ¿Qué tipo de fraude informático es el más común en las instituciones financieras?

   ( ) Manipular datos de entrada

   ( ) Manipular sistemas informáticos

   ( ) Manipular datos de salida

2. ¿Piensa usted que en la institución existen las suficientes políticas de seguridad?

   ( ) SI

   ( ) NO

3. ¿Según su criterio cuál es el recurso de mayor vulnerabilidad en los sistemas informáticos dentro de la institución?

   ( ) Base de datos

   ( ) Sistemas

( ) Recurso humano

4. ¿Qué tipo de información está disponible para los clientes internos de la institución?

( ) Datos de la institución

( ) Datos de clientes

5. ¿Cree usted que las decisiones técnicas tomadas por las autoridades de la institución son las adecuadas?

( ) SI)

( ) NO

6. ¿Cuál sería la denominación que usted le daría a las personas que cometen fraude informático?

( ) Hackers

( ) Crackers

( ) Lammers

7. ¿Quién es el encargado de la toma de decisiones ante los diferentes problemas técnicos que se dan en la institución financiera?

( ) Gerente

( ) Administrador de Sistemas

ANEXO 5

GLOSARIO DE TÉRMINOS

Ataques informáticos: Un **ataque informático** es un método por el cual un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático.

Bugs: Defecto en un software o un hardware que no ha sido descubierto por los creadores o diseñadores de los mismos.

Certificados de seguridad: Es un conjunto de documentos electrónicos emitidos por una entidad certificadora de confianza, que permiten encriptar la información transmitida e identificar a la fuente de dicha información.

Colapso del sistema: Paralización repentina o disminución importante de una actividad debidas a la excesiva actividad.

Consistencia de datos: Tus datos e información es consistente cuando son reales y lógicos.

Cyberdelincuencia: Se entiende por cyberdelincuencia aquellas acciones que han sido cometidas mediante la utilización de un bien o servicio informático.

Dispositivos electrónicos: Los Dispositivos o Aparatos Electrónicos consisten en la combinación de diversos elementos o componentes organizados en circuitos, destinados a controlar y aprovechar las señales eléctricas, a diferencia de un dispositivo eléctrico, el cual sirve para controlar y aprovechar el flujo de la corriente eléctrica.

Encriptar: La encriptación es el proceso para volver ilegible información considera importante. La información una vez encriptada sólo puede leerse aplicándole una clave.

Estación de trabajo: Es un microordenador de altas prestaciones destinado para trabajo técnico o científico. Es una computadora que facilita a los usuarios el acceso a los servidores y periféricos de la red.

Innovación tecnológica: Es la transformación de una idea en un producto o equipo vendible, nuevo o mejorado; en un proceso operativo en la industria o el comercio, o en una nueva metodología para la organización social.

Integridad de información: Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas.

Interfaz de usuario: Es el medio con que el usuario puede comunicarse con una máquina, un equipo o una computadora, y comprende todos los puntos de contacto entre el usuario y el equipo. Normalmente suelen ser fáciles de entender y fáciles de accionar.

Intruso informático: Son archivos cuyo propósito es invadir la privacidad de tu computadora, posiblemente dejando daños y alterando el software del equipo.

Licencia: Es un contrato entre el licenciante (autor/titular de los derechos de explotación/distribuidor) y el licenciatario del programa informático (usuario consumidor /usuario profesional o empresa), para utilizar el software cumpliendo una serie de términos y condiciones establecidas dentro de sus cláusulas.

Negación de servicios: Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

NetBus: Es un software malicioso para el control de una forma remota de sistemas informáticos Microsoft Windows a través de una red.

Políticas de seguridad: Es un conjunto de requisitos definidos por los responsables de un sistema, que indica en términos generales que está y que no está permitido en el área de seguridad durante la operación general del sistema.

Redireccionamiento: Acceder a una determinada dirección mediante otra.

Repositorio: Podría definirse como la base de datos fundamental para el diseño; no sólo guarda datos, sino también algoritmos de diseño y, en general, elementos software necesarios para el trabajo de programación.

Sistema informático: Es un conjunto de partes que funcionan relacionándose entre sí con un objetivo preciso. Sus partes son: Hardware, Software y las personas que los usan.

Tecnologías: La tecnología es un concepto amplio que abarca un conjunto de técnicas, conocimientos y procesos, que sirven para el diseño y construcción de objetos para satisfacer necesidades humanas.

Vulnerabilidad: La palabra vulnerabilidad hace referencia a una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.