UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMATICA

(F.A.F.I)

ESCUELA DE ADMINISTRACIÓN DE EMPRESAS Y GESTIÓN EMPRESARIAL

TESIS DE GRADO

PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO COMERCIAL

TEMA:

"LA INFLUENCIA DE LA CULTURA ORGANIZACIONAL EN LA APLICACIÓN DE LA ESTRATEGIA DE SEGURIDAD DE LA INFORMACION EN LAS ORGANIZACIONES FINANCIERAS EN LA CIUDAD DE BABAHOYO"

DIRECTOR:

ING. FABIAN TOSCANO M.B.A

LECTOR:

EC. VERONICA MERCHAN

EGRESADOS:

LISBETH KATHERINE MARTINEZ BARZALLO
CRISTHIAM EDGAR CARPIO BAJAÑA

AÑO: 2011

DEDICATORIA

Dedico esta tesis de grado a Dios que me guio en todo momento por el buen camino para poder culminar con éxito.

A mis padres fortaleza y regocijo en cada día y de los cuales me siento muy orgulloso.

A mi familia toda que con sus consejos me hicieron una mujer de bien y a los cuales les deseo felicidad.

LISBETH KATHERINE MARTINEZ BARZALLO

AGRADECIMIENTO

Agradecemos a nuestra facultad, que nos ha brindado a lo largo de la carrera formación, personal y profesional.

A cada uno de los maestros que nos guiaron y fortalecieron con sus sabios consejos.

Y a todas las personas que directa o indirectamente hicieron posible la culminación de nuestra tesis.

LISBETH KATHERINE MARTINEZ BARZALLO

DEDICATORIA

Dedico esta tesis de grado a Dios que me guió en todo momento por el buen camino para poder culminar con éxito.

A mi familia fortaleza y regocijo en cada día y de los cuales me siento muy orgullosa.

A mis hermanos y mis familiares porque me han brindado su apoyo y confianza en el transcurso de mi carrera, y por estar juntos en los momentos más difíciles.

CRISTHIAM EDGAR CARPIO BAJAÑA

AGRADECIMIENTO

A Dios, mi Guía, porque nunca me faltaste, en ti confío. Sabes lo esencial que has sido en mi posición firme de alcanzar esta meta, Siempre me has ayudado a seguir adelante, sé que todos pueden decepcionarme menos tú y reconozco que sin ti no hubiese podido sobrevivir. ..Gracias Señor

A mi Mami, por ser fuente de alegría. Por tu valor y fortaleza para enfrentar de cara las adversidades de la vida. Por haberme inspirado y motivado eres la magnífica artesana de quien soy.

A mis hermanas, por enseñarme cuánto valgo. Por estar presente aun cuando no lo he notado. Por abrazarme en mis abismos. Por protegerme y darme valor. Junto a Uds. aprendí que vivir la realidad puede ser más satisfactorio que soñar despierta.

Agradezco a nuestra facultad, que nos ha brindado a lo largo de la carrera formación, personal y profesional. A cada uno de los maestros que nos guiaron y fortalecieron con sus sabios consejos.

A todos ellos GRACIAS…….

CRISTHIAM EDGAR CARPIO BAJAÑA

DECLARACIÓN DE AUTORÍA DE LA TESIS

La autora de esta investigación declara que no existe investigación alguna del tema: **"LA INFLUENCIA DE LA CULTURA ORGANIZACIONAL EN LA APLICACIÓN DE LA ESTRATEGIA DE SEGURIDAD DE LA INFORMACION EN LAS ORGANIZACIONES FINANCIERAS EN LA CIUDAD DE BABAHOYO",** en la Facultad de Administración, Finanzas e Informática de la Universidad Técnica de Babahoyo, ni en ninguna biblioteca de las otras universidades en el Ecuador.

AUTORES:

MARTINEZ LIZBETH
CARPIO CRISTHIAM

INDICE GENERAL

RESUMEN

Se analiza la necesidad de implementar modelos que sean validados con una aplicación práctica y se desarrollen bajo metodologías estadísticas, teniendo en cuenta que la gestión corporativa del riesgo se ha convertido en un elemento importante dentro de las políticas administrativas de las instituciones dedicadas al otorgamiento de créditos; se presenta la oportunidad de generar un método de medición de riesgo de crédito, el cual se abordará desde tres modelos que permitan estimar la probabilidad de incumplimiento, con los cuales se puedan efectuar comparaciones de las bondades y desventajas de cada uno de ellos

Se entiende por **seguridad de la información** a todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la *confidencialidad*, la *disponibilidad* e *Integridad* de la misma.

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pudiendo encontrar información en diferentes medios o formas.

Para el hombre como individuo, la seguridad de la información tiene un efecto significativo respecto a su privacidad, la que puede cobrar distintas dimensiones dependiendo de la cultura del mismo.

SUMMARY

This project analyzes the necessity of creating models that are validated with a practical application. They are developed under statistical methodologies, keeping in mind that the corporate management of the risk has become an important element for the administrative politics of the institutions dedicated to offer credits. It is presented the opportunity of generating a credit risk measurement method. This method will be undertaken since three models to reckon the probability of breach, with which comparisons of the kindnesses and disadvantages of each one of them can be performed. These models are.

He/she understands each other for security from the information to all those preventive measures and you reactivate of the man, of the organizations and of the technological systems that allow to preserve and to protect the information looking for to maintain the confidentiality, the readiness and Integrity of the same one.

The concept of security of the information should not be confused with that of computer security, since this last one only takes charge of the security in the computer means, being able to find information in different means or forms.

For the man like individual, the security of the information has a significant effect regarding his privacy, the one that can charge different dimensions depending on the culture of the same one.

The field of the security of the information has grown and evolved considerably starting from the Second World War, becoming a career credited at world level. This field offers many specialization areas, included the audit of systems of information, planning of the continuity of the business, digital forensic science and administration of systems of administration of security, among others.

INTRODUCCIÓN

El presente trabajo de investigación tiene el propósito de resaltar los aspectos de la cultura organizacional que deben considerarse en a la implantación de una estrategia que considera principalmente conceptos relacionados con seguridad de la información en una organización de tipo financiero.

La cultura organizacional ha sido estudiada durante mucho tiempo como uno de los medios que al analizarlo pueden dar algún tipo de directriz que sirve de referencia, para entender de qué manera las estrategias fluyen de manera efectiva en una organización.

Con una experiencia laboral de casi una década, enfocamos el trabajo de esta investigación a la relevancia de la cultura organizacional en el sector financiero y cómo influye en las estrategias del sistema.

Para poder hablar de cultura organizacional, será muy importante considerar el tema del capital intelectual y en lo que se ha dado a conocer como el siglo del conocimiento, ya que este forma parte de la cultura organizacional y su enfoque se ve reflejado en las estrategias corporativas.

Otro punto a considerar es, el tema de la seguridad de la información que ha tenido un fuerte crecimiento en los últimos años, debido a la gran apertura y la globalización a la cual se han enfrentado todos los sectores empresariales.

Dentro de las asignaciones que he tenido en el sector financiero, hemos estado enfocando a la implantación de estrategias e institucionalización de las mismas, las cuales se han enfrentado principalmente con el tipo de cultura organizacional que tiene el sector, el cual de manera general es de tipo tradicionalista.

Adicionalmente a lo anterior, se realizó esta investigación buscando un enfoque que pudiera dar amplios resultados sobre los efectos en las implantaciones de estrategias, por lo cual relacionamos el tema de la seguridad de la información con la cultura organizacional, relacionada también con el capital intelectual y la forma cómo influye.

Con base en todo lo anterior, es la forma como esta investigación a través de el conocimiento de la cultura organizacional y como ayuda o no en una implantación.

Actualmente se da énfasis a la globalización y la apertura; sin embargo, es de mayor relevancia conocer cómo han sido recibidos estos conceptos en la cultura organizacional de una institución donde se ha tenido que implantar una política de protección de la información, a través del concepto de seguridad de la información.

El objetivo principal de esta investigación radica en la identificación del impacto de la cultura organizacional en la implantación de una estrategia de seguridad de la información, su efectividad, enfocado a una organización del sector financiero y sus aspectos más relevantes.

El análisis del concepto de cultura organizacional se ha desarrollado en todas las economías de tipo capitalista, a través del cual se buscan estilos, definiciones y cómo afectan estos sobre la implantación de estrategias en la organización.

Adicional a esto también es importante analizar dentro del concepto de cultura organizacional el aspecto de cómo el capital intelectual es parte de la cultura organizacional y ambos afectan de manera directa a la implantación de la estrategia de seguridad de la información, la cual, en los últimos tiempos, como lo hemos descrito, ha ido en incremento el concepto de aseguramiento y protección de la información.

CAPITULO I

1. MARCO REFERENCIAL

1.1 PROBLEMA DE INVESTIGACION

En la actualidad, las organizaciones están influenciadas por constantes cambios que ocurre en su entorno, por lo que, constantemente tienen que revisarse y ajustar los objetivos existentes o establecer otros nuevos. Por ello, el Gerente de Recursos Humanos de hoy en día, va más allá del simple trabajo de oficina y de diversas tareas referentes a la conducta humana porque la tendencia actual en trazarse objetivos que se basen en la información financiera como estrategia para el control administrativo, para garantizar el resguardo financiero.

De ahí, que se ha visto obligado a revisar los procedimientos empíricos de administración para apelar a los nuevos métodos de eficiencia con el objeto de administrar así, humana y técnicamente, los recursos.

1.2 ANTECEDENTES DE LA INVESTIGACION

Es muy común que en las organizaciones financieras se tenga precaución con la información que se maneja interna y externamente, pues puede afectar sus operaciones presentes y futuras, se habla constantemente de aplicar la cultura organizacional en los empleados para asegurar la responsabilidad del empleado ante su organización, muchas de estas organizaciones de tipo financiera en la ciudad de Babahoyo se han visto afectadas por la salida de información.

Poco o nada se ha hecho para remediar este problema que involucra a todos los ciudadanos que de una u otra manera ven afectados sus operaciones. No se encuentra investigaciones realizadas sobre este tema lo que nos impulso a desarrollar nuestro proyecto de tesis para remediar en algo esta situación conflictiva

1.3 DESCRIPCION DE LA SITUACION PROBLEMATICA

A través de la información, la gerencia puede determinar el tiempo real cuál ha sido el resultado de su gestión de tal manera que resulten valiosos para la toma de decisión de la administración.

La complejidad de los sistemas contables, depende de varios factores, entre los cuales destacan el tamaño de la empresa, así como de la necesidad de información que requiere la gerencia. Cuando las pequeñas empresas comienzas a expandir sus operaciones, se hace necesario dar mayor formalidad al sistema contable, a fin de poder mantener el dominio de todas las actividades. De lo contrario, escaparía de las manos de la gerencia, el control del negocio. Esto con el propósito de disponer eficientemente, de forma oportuna y confiable, de la información financiera que requieren las organizaciones para su normal funcionamiento.

También los constantes cambios las obligan a ser cada vez más ágiles para que puedan adaptarse con mayor facilidad a estos cambios. Por esta razón las compañías dependen en su totalidad de poseer la información exacta en el momento preciso, para la toma de decisiones; es aquí, donde radica la prioridad de contar con un sistema de información financiera que permita hacer un buen control

administrativo. Y a su vez, es necesario mantener un adecuado control de los procedimientos, para reducir las causas que puedan poner en riesgo el logro de los objetivos propuestos por la organización.

Las empresas tienen riesgo de perder información, esto podría detener su operación, deteniendo procesos de producción o administrativos, para ello es necesario proteger el funcionamiento de la información, existen diferentes maneras o métodos de proteger un sistema de información, todas estas partes del sistema de seguridad deben trabajar en conjunto para asegurar la información de la organización.

La seguridad de la información en las organizaciones existe solo si se juntan todos los elementos y métodos que la hacen posible ya que cualquier método utilizado por sí solo no puede abarcar todos los puntos vulnerables de los sistemas de información, así lo da a entender, [1]Hallberg (2003, p.97). “La seguridad de la información solo brinda áreas de oportunidad, en los sistemas avanzados por si sola seguridad en la información de la organización, la seguridad de la información en las organizaciones, no puede por sí mismo proporcionar la protección para su desarrollo”. De acuerdo con el autor, es por que pretendemos mostrar los puntos de protección en una empresa que usa una red de datos local para compartir y automatizar su información.

Hallber (2003, p.97) Editorial Life

1.4. Formulación del Problema de Investigación

¿Cuál es la causa de que las entidades financieras pequeñas medianas y grandes no aplican un control más eficiente de la información general que se maneja internamente para asegurar el desarrollo de sus actividades operativas y de administración?

A través de la información, la gerencia puede determinar el tiempo real cuál ha sido el resultado de su gestión de tal manera que resulten valiosos para la toma de decisión de la administración.

La complejidad de los sistemas contables, depende de varios factores, entre los cuales destacan el tamaño de la empresa, así como de la necesidad de información que requiere la gerencia. Cuando las pequeñas empresas comienzas a expandir sus operaciones, se hace necesario dar mayor formalidad al sistema contable, a fin de poder mantener el dominio de todas las actividades. De lo contrario, escaparía de las manos de la gerencia, el control del negocio. Esto con el propósito de disponer eficientemente, de forma oportuna y confiable, de la información financiera que requieren las organizaciones para su normal funcionamiento.

También los constantes cambios las obligan a ser cada vez más ágiles para que puedan adaptarse con mayor facilidad a estos cambios. Por esta razón las compañías dependen en su totalidad de poseer la información exacta en el momento preciso, para la toma de decisiones; es aquí, donde radica la prioridad de contar con un sistema de información financiera que permita hacer un buen control

administrativo. Y a su vez, es necesario mantener un adecuado control de los procedimientos, para reducir las causas que puedan poner en riesgo el logro de los objetivos propuestos por la organización.

1.4.1 Sub preguntas

- La desconfianza que hay en los clientes de las entidades financieras no ha permitido establecer un liderazgo organizacional, en comparación con otras organizaciones de tipo crediticio.
- Este sistema de información gerencial resulta complejo para determinadas áreas de la organización, que están presentado problemas.
- La información real deberá circular por todo el sistema financiero de la organización para su correcta aplicación en la toma de decisiones
- El desconocimiento de un buen manejo de la información provoca retrasos y errores que puedan generar serios inconvenientes a la institución financiera

1.5 Problema Central

Deficiencia en la seguridad de la información organizacional en las instituciones financieras que causan pérdidas no solo económicas sino de competitividad.

1.5.1 Problemas Derivados

- Deficiente servicio al presentar información retrasada o equivocada por consecuencia de una incorrecta utilización del sistema de información gerencial.
- Riesgo de tomar decisiones sin tener una certeza por parte de la información

proveniente de las distintas áreas de la organización.

- Efectos negativos al entorno interno y externo que puede resultar en una mala imagen para la organización.

1.5.2 Delimitación del Problema

- **Campo:** Instituciones financieras
- **Área:** financiera
- **Aspecto:** Control de la seguridad Financiera

1.6 OBJETIVOS DE LA INVESTIGACION

1.6.1 OBJETIVO GENERAL

Minimizar la perdida y desvió de la información en las instituciones financieras de la ciudad de Babahoyo a través de la implantación del Sistema de Gestión de Seguridad de la Información (SGSI) como estrategia para el control y seguridad administrativa en las empresas del sector financiero en general.

1.6.2 OBJETIVOS ESPECÍFICOS

- ❖ Realizar un análisis situacional a través del SGSI para conocer aspectos relevantes en la información de seguridad en las empresas financieras.
- ❖ Examinar los procedimientos que deben seguirse para garantizar la confiabilidad de la información financiera.
- ❖ Detectar la necesidad de correctivos de los procedimientos administrativos para alcanzar la efectividad en el control administrativo.

1.7 JUSTIFICACIÓN

La importancia en el estudio radica en la necesidad que han tenido las organizaciones financieras, de tener en cuenta con mayor énfasis, los elementos del comportamiento organizacional dentro de la cultura, para mantener una estrategia efectiva de protección de la información, con un enfoque de negocio, en una situación de globalización y restricción.

Para la organización financiera, es muy importante y necesario que cada una de sus áreas que la componen y sus filiales, puedan adecuar su comportamiento y cultura organizacional, con la finalidad de poner en marcha planes estratégicos de protección de la información, con la finalidad de lograr un elemento adicional a la cadena de valor de sus productos y servicios y poder diferenciarse, para lograr abarcar nichos de mercado y mantener la confianza de sus clientes

Con una cultura organizacional orientada a la efectividad y hacia el mantener la confianza del cliente, con el enfoque de que en la actualidad la apertura genera riesgos para la organización y deben ser cubiertos o mitigados para ofrecer la mayor transparencia posible en un mundo globalizado.

Lo anterior se puede lograr con un enfoque adecuado de los objetivos y metas que se persiguen en cada una de las estrategias de protección de la información, con la finalidad de mantener la confidencialidad, integridad y disponibilidad de la misma, explicando a cada individuo la importancia de esto y

sobre todo apoyados por la alta dirección y las estrategias siempre orientadas con enfoque de negocio.

Mediante un adecuado entendimiento de negocio y con una cultura organizacional adaptativa y flexible, se podrán tener estrategias de protección efectivas con orientación al cliente.

Esta investigación requerirá de la evaluación de un modelo que ayude a la integración del tipo de cultura organizacional con la estrategia de protección en la búsqueda de un programa efectivo.

Es importante tomar en cuenta los aspectos futuros de la globalización y la tendencia de las organizaciones, sus cambios culturales, así como el incremento de riesgos internos y externos de la información en un ambiente abierto.

CAPITULO II

2. MARCO TEORICO

2.1. ANTECEDENTES INVESTIGATIVOS.

No existen registros de investigaciones anteriores sobre la ejecución de un modelo para la medición del riesgo en el incumplimiento de créditos para una entidad financiera ya que debido a las constantes políticas ejercidas por los entes financieros no han permitido aplicar o ejecutar un modelo de medición de este tipo para evaluar el riesgo crediticio en las entidades financieras en la ciudad de Babahoyo.

La ejecución de un modelo así, surge de la necesidad de que en las instituciones financieras que operan en la ciudad de Babahoyo exista un ente regulador del riesgo que puede surgir en la aplicación de créditos por parte de cualquier organización financiera.

Los estudios relacionados con la factibilidad o no de establecer un modelo que permita a las instituciones financiera poder medir el riesgo que originan los créditos tanto de consumo como de inversión

2.2 FUNDAMENTACIÓN TEÓRICA

DEFINICIÓN DE INFORMACIÓN FINANCIERA.

El mundo de los negocio es cada vez mas complejo, exige mas profesionalismo en la administración de las empresas, si es que las organizaciones han de alcanzar un lugar destacado dentro del desarrollo económico del país y del mundo laboral. Para lograr esta meta se requiere, entre otros elementos, contar con un sistema de

información relevante, oportuno y confiable, generado mediante un buen sistema de contabilidad.

[1]Según Miyauchi (2000) "La información financiera se presenta en los documentos denominados estados financieros básico los cuales son: balance general, estado de resultados, estado de cambios en la situación financiera. Dichos estados son esenciales para lograr una administración eficiente de la organización"

2.2.1. IMPORTANCIA DE INFORMACIÓN FINANCIERA.

La información financiera es importante porque representa el medio indispensable para evaluar los resultados; es decir, para juzgar la efectividad con que la administración logra mantener intacta la inversión de los accionistas y obtener adicionalmente un rendimiento justo, por ser esto el mejor apoyo para facilitar el proceso administrativo y poder lograr llevar a cabo las funciones de planeación, control y toma de decisiones.

Al respecto Ramírez 1994 dice que “A mejor calidad en la información, corresponderá mejor probabilidad de éxito”… Por lo tanto para lograr la calidad en la información, ésta deberá incorporar a su contenido datos que satisfagan las necesidades de los diferentes usuarios.

---

[1]Según Miyauchi (2000) pag.8 Editorial Halcón

2.2.2. DEFINICIÓN DE CONTROL.

El control es un elemento del proceso administrativo que incluye todas las actividades que se emprenden para garantizar que las operaciones reales coincidan con las operaciones planificadas. Todos los gerentes de una organización tienen que realizar evaluaciones de los resultados y tomar las medidas necesarias para minimizar las ineficiencias. De tal manera, el control es un elemento clave en la administración. MOCKLER (1999), conceptualiza el control tomando sus elementos esenciales como: El esfuerzo sistemático para fijar niveles de desempeño con objetivos de planeación, para diseñar los sistemas de retroalimentación de la información, para comparar el desempeño real con esos niveles determinados de antemano, para tomar las medidas tendientes a garantizar que todos los recursos de la empresa se utilicen en la forma más eficaz u eficiente posible en la obtención de los objetivos organizacionales. (p.657).

2.2.3. IMPORTANCIA DEL CONTROL.

La importancia que tiene el control es que a través de esta función lograremos precisar si lo realizado se ajusta a lo planeado y en caso de existir desviaciones, identificar los responsables y corregir dichos errores. Sin embargo es conveniente recordar que no debe existir solo el control a posteriori, sino que, al igual que el planteamiento, debe ser, por lo menos en parte, una labor de previsión. En este caso se puede estudiar el pasado para determinar lo que ha ocurrido y porque los estándares no han sido alcanzados; de esta manera se puede adoptar las medidas

necesarias para que en el futuro no se cometan los errores del pasado. Además, siendo el control la última de las funciones del proceso administrativo, ésta cierra el ciclo del sistema al proveer retroalimentacion respecto a desviaciones significativas contra el desempeño planeado. La retroalimentación de información pertinente a partir de la función de control puede afectar el proceso de planeación.

2.2.4. PASOS EN EL PROCESO DEL CONTROL.

La definición de MOCKLER divide el control en cuatro etapas:

1) **Establecimiento de objetivos y métodos para medir el desempeño**: en este paso del proceso de control se establecen previamente los objetivos y éstos sirven como puntos de referencias para el desempeño o resultados de una organización, unidad organizacional o actividad individual. Para que este paso sea eficaz, los objetivos deben especificarse en términos significativos y deben ser aceptados por los interesados. Los métodos de medición también deberán aceptarse como exactos.

2) **Medición del desempeño:** proceso constante y repetitivo, dependiendo su frecuencia del tipo de actividad que se mida. Así los niveles de seguridad se ven reafirmados a medida que avance en los objetivos a largo plazo de la organización. El propósito de este paso es verificar sí se obtienen los resultados o cuáles son las correcciones necesarias que deben introducir en el proceso.

3) Comparación del desempeño con el objetivo: en este paso se trata de comparar los resultados con las metas y los objetivos determinados con anterioridad. Si el desempeño corresponde con los estándares establecidos, los administradores supondrán que todo está bajo control.

4) Tomar medidas correctivas: este paso se da cuando el desempeño no cumple con los niveles establecidos y en consecuencia se deben corregir las variaciones, errores o desvíos para que las operaciones sean normales. Esto se hace para mantener el desempeño dentro del nivel de los estándares establecidos para garantizar que todo se haga exactamente de acuerdo con lo planeado.

2.2.4. FACTORES ORGANIZACIONALES QUE CREAN LA NECESIDAD DEL CONTROL.

Hay muchos factores que hacen indispensable el control en las organizaciones modernas entre ellos figuran el ambiente cambiante de la empresa. Su creciente complejidad, la falibilidad de sus miembros y la necesidad que tienen los gerentes de delegar su autoridad, entre esos tenemos:

Cambios. El cambio constituye una parte inevitable de cualquier ambiente organizacional: el mercado cambia; aparecen nuevos productos; se descubren nuevos materiales; se aprueban nuevas normas. Gracias a la función de control, los gerentes detectan que están afectando a los productos o servicios de su

organización, y entonces pueden tratar de sortear los riesgos y aprovechar las oportunidades que brindan esos cambios.

Complejidad. Esta viene dada ya que debe de existir una vigilancia estrecha de las líneas de productos diversificados para asegurarse de que se conserven la calidad y rentabilidad; es preciso registrar con cuidado y analizar las ventas en los establecimientos que venden al menudeo; los mercados de la empresa, tanto los del extranjero como los del país, exigen una vigilancia estrecha.

Error. Si los gerentes y subordinados no cometieran errores nunca simplemente se establecerían criterios del desempeño y señalarían los cambios importantes e inesperados del ambiente. Pero los miembros de las organizaciones a veces se equivocan; se ordenan las piezas equivocadas, se toman decisiones erróneas en la fijación de precios, los problemas se diagnostican de modo incorrecto. Un sistema de control permite a los gerentes detectar esos errores antes que sean graves.

Delegación. La única manera en que los gerentes pueden determinar si sus subordinados están ejecutando las tareas que les han sido delegadas consiste en implementar un sistema de control. Si no se implantan, no podrán vigilar el avance de sus subordinados.

2.2.6 DEFINICIÓN DE ESTRATEGIAS.

[1]Mintzberg (citado por Viloria) ve a la estrategias desde una perspectiva; en tal sentido; "habla de las cinco P´s de la estrategia a los fines de indicar que la misma puede ser entendidita como: plan, pauta de acción, patrón, posición o perspectivo" (pag 49).

Las estrategias tienen que ver con todas las actividades críticas de la empresa, proveyendo un sentido de unidad, dirección y propósito, a la vez que facilite la puesta en práctica de los cambios exigidos por el entorno.

Según Viloria (2001) señala que lo que se refiere a los tipos de estrategia, podemos diferenciar las siguientes, de acuerdo con el tipo de asunto y con el nivel responsable de formularla y ejecutarla:

- **Estrategia corporativa:** Se refiere a aquel tipo de decisiones que por su alcance y naturaleza tiene que ver con el conjunto de la empresa; es desarrollada por los máximos niveles de la empresa y usualmente persigue identificar las fortalezas y debilidades de la organización, las amenazas y oportunidades que ofrece el entorno con la finalidad de establecer los objetivos corporativos que permitan la asignación de recursos humanos, financieros y físicos para cumplirlos.

---

[1] **Mintzberg 2008 pag. 49 Campos de Aplicación de las Estrategias**

- **Estrategias de negocios:** Se relacionan con la obtención de un mejor rendimiento financiero de los diferentes negocios de la empresa con la finalidad de mejorar el posicionamiento de la misma en relación con los competidores. De esta forma, los gerentes de las unidades de negocios o responsables de los negocios de la compañía, formulan e implementan acciones estratégicas coherentes con los objetivos corporativos, permitiendo, en consecuencia, la definición de estrategias de negocios, programas y presupuestos de inversión y operación.

- **Estrategias funcionales:** Se refieren al conjunto de requerimientos de las diferentes funciones de la empresa (recursos humanos, finanzas, producción, etc.) necesarios para darle efectivo cumplimiento a las estrategias de negocios y a la corporativa. De esta forma, los gerentes funcionales realizan, a su nivel, el correspondiente análisis de oportunidades y amenazas, de fortalezas y debilidades a objeto de formular un conjunto de programas y de asignar recursos que permitan darle cabal cumplimiento a los respectivos objetivos funcionales.

2.2.7 MATRIZ DOFA PARA LA FORMULACIÓN DE ESTRATEGIA.

La Matriz DOFA es una herramienta analítica que le permitirá trabajar con toda la información que posea sobre la organización, útil para examinar sus debilidades, oportunidades, fortaleza y amenazas.

Este tipo de análisis representa un esfuerzo para examinar la interacción entre las características particulares de la organización y el entorno en el cuales este compite.

Esta herramienta puede ser de gran utilidad ya que le va a permitir obtener un análisis de mercado permitiendo que se establezcan estrategias de mercadeo que califiquen para ser incorporadas en el plan de negocio.

Las organizaciones se ven influenciadas por factores internos y externos que afectan el desarrollo de sus actividades. Por esta razón los gerentes deben involucrarse con su entorno para formular estrategias efectivas que le permitan alcanzar de la mejor manera sus objetivos.

A raíz de esto ellos deben utilizar herramientas; que le ayuden ha formular las estrategias más idóneas, como la matriz DOFA definida por **Goodstein (2001) como: "Un marco conceptual para un análisis sistemático que facilite el aparcamiento entre las amenazas y oportunidades externas con las debilidades y fortalezas internas de la organización" (Pag. 270): así mismo añade... "Le permiten a las empresas un diagnóstico de su propia situación y su ubicación en el entorno y la elección de estrategias de acuerdo a este diagnóstico..." (pa g. 271).**

---

[1] **Goodstein (2001) pag. 270**

Partiendo de esta apreciación en la matriz DOFA se enfoca en los factores claves para el éxito de una organización. En los factores o componentes internos están las debilidades y fortaleza; aspectos sobre los cuales la empresa tiene cierto grado de control, que representan los aspectos negativos y positivos con que cuenta la organización.

- Fortaleza y debilidad
- Considera áreas como las siguientes
- Análisis de recursos
- Capital, recursos humanos, sistemas de información, activos fijos, activos no tangibles.
- Análisis de riesgo.
- Con relación a los recursos y a las actividades de la empresa.
- Análisis de portafolio
- La contribución consolida de las diferentes actividades de la organización.

En cuanto al aspecto externo se identifican las oportunidades y las amenazas que engloban aquellos factores que puedan representarse; en
determinado momento, un beneficio o peligro para la organización, aquí se tiene que desarrollar toda la capacidad y habilidad para aprovechar las oportunidades y para minimizar o anular las amenazas, circunstancia sobre las cuales se tiene poco o ningún control directo.

2.2.8 OPORTUNIDADES Y AMENAZAS

Las oportunidades organizacionales se encuentran en aquellas áreas que podrían generar muy altos desempeños. Las amenazas organizacionales están en aquellas áreas donde la empresa encuentra dificultad para alcanzar altos niveles de desempeño.

CONSIDERE:

- Análisis del Entorno
- Estructura de su industria (Proveedores, canales de distribución, clientes, mercados, competidores). -Grupos de interés
- Gobierno, instituciones públicas, sindicatos, gremios, accionistas, comunidad.
- El entorno visto en forma más amplia
- Aspectos demográficos, políticos, legislativos, etc.

2.2.9 OBJETIVOS DE CONTROL ADMINISTRATIVO.

Ramírez (2004), señala que "El control administrativo en las organizaciones contribuye al logro de los siguientes objetivos:

1. DIAGNOSTICAR.

En este objetivo el control administrativo busca descubrir en su actuación áreas problemas o áreas de aciertos para determinar las acciones que Se deben realizar a fin de corregir una situación o capitalizar un acierto. El control administrativo está orientado a la prevención de situaciones críticas, "Pretende diagnosticar a tiempo, para evitar quiebras de empresa".

2. COMUNICACIÓN.

Otro de los objetivos básicos del control es proporcionar un medio de comunicación entre las personas que integran la organización. Esto se logra informando los resultados de las diversas actividades que se llevan a cabo dentro de la empresa. También es un medio para que el subordinado conozca las pautas que servirán de guía y base para que el jefe evalúe periódicamente su actuación

3. MOTIVACIÓN.

Normalmente, todos los sistemas de control administrativos son rechazados a priori por el personal afectado. Por excelente que sea la herramienta que se va a implantar, se debe motivar a todos los afectados a identificar dicha herramienta como un medio de superarse y desarrollarse.

Se considera que lo más importante, al implantar cualquier sistema de control, es el convencimiento del personal de la bondad de la herramienta puesta, en servicio; ya que una vez aceptado el nuevo sistema; su implantación es sencilla y se logra el éxito.

2.2.10 PROCEDIMIENTOS BÁSICOS PARA EL CONTROL ADMINISTRATIVO.

Según Mockler (2007) existen cuatro procedimientos básicos que se deben llevar a cabo para realizar un buen control administrativo.

Estos se explican a continuación:

2.2.10.1CONTROLES ANTERIORES A LA ACCIÓN.

Llamados también Precontroles, garantizan que antes de emprender una acción se haya hecho el presupuesto de los recursos humanos, materiales y financieros que se necesitaran. Cuando llega el momento de la acción, los presupuestos, aseguran que los recursos requeridos estén disponibles en los tipos, calidad, cantidad y ubicaciones necesarios. Los presupuestos pueden exigir contratar y adiestrar a nuevos empleados, adquirir equipo y suministros, diseñar y programar los nuevos materiales o productos.

---

[1] **Según Mockler (2007 pag.245 Editorial La Campana**

2.2.10.2 CONTROLES DIRECTIVOS O CONTROLES DE ALIMENTACIÓN HACIA ADELANTE.

Su objetivo es descubrir las desviaciones respecto a alguna norma o meta y permitir que se hagan correcciones antes de culminar una determinada serie de acciones. Los controles directivos dan como resultado sólo si el gerente es capaz de obtener información precisa y oportuna sobre los cambios del ambiente o el avance hacia la meta deseada.

2.2.10.3 CONTROLES DE SELECCIÓN PRELIMINAR.

Este tipo de control ofrece un proceso de selección en el cual, para que en una operación continué, antes hay que aprobar un procedimiento o satisfacer determinadas condiciones.

2.2.10.4 CONTROLES DESPUÉS DE LA ACCIÓN.

Se investigan las causas de las desviaciones respecto al plan o norma, y luego los hallazgos se aplican a actividades futuras parecidas. Es decir miden los resultados de una acción terminada.

2.2.11 CORRECTIVOS EN LOS PROCEDIMIENTOS ADMINISTRATIVOS PARA ALCANZAR LA EFECTIVIDAD EN LAS EMPRESAS.

Los procedimientos son elementos que permiten organizar cualquier actividad de forma lógica y clara, pero a su vez deben ser analizados constantemente a fin de

establecer correctivos que puedan permitir el desarrollo sostenido de las organizaciones.

Según Internet (2005) estas son las actividades que se llevan a cabo en el proceso administrativo.

1. PLANEACIÓN.

Para un gerente y para un grupo de empleados es importante estar identificado con los objetivos que van a alcanzar, se formulan un plan o un patrón predeterminando las futuras actividades, esto requiere la facultad de prever, de visualizar, el propósito de ver hacia delante para alcanzar el éxito establecido en las metas identificadas realistas y retadoras.

2.2.12 ACTIVIDADES DE LA PLANEACIÓN.

a. Aclarar, amplificar y determinar los objetivos.

b. Pronosticar.

c. Establecer las condiciones y suposiciones bajo las cuales se hará el trabajo.

d. Seleccionar y declarar las tareas para lograr los objetivos.

e. Establecer un plan general de logros enfatizando la creatividad para encontrar nuevos y mejores de desempeñar el trabajo.

f. Establecer políticas, procedimiento y métodos de desempeño.

g. Anticipar los posibles problemas futuros.

h. Modificar los planes a la luz de los resultados del control (Ibid).

2.2.12.1 ORGANIZACIÓN.

Después que la planeación haya sido determinada, el paso siguiente para cumplir con el trabajo es distribuir las actividades planeadas entre los miembros del grupo e indicar la participación de cada miembro para establecer y reconocer las relaciones necesarias.

Este tipo de actuación es una actividad de control muy importante para la consecución de objetivos puesto que la información oportuna y apropiada constituye en la mayoría de los casos la primera base para la correcta toma de decisiones. La dirección identifica los riesgos existente a todos los niveles en la empresa, ésta realiza un análisis de los factores que generan riesgos de manera que deben estimar la importancia de los mismo.

2.2.12.1.1ACTIVIDADES IMPORTANTES DE LA ORGANIZACIÓN.

a. Subdividir el trabajo en unidades operativas (dptos).

b. Agrupar las obligaciones operativas en puestos.(puesto x puesto).

c. Seleccionar y colocar a los individuos en el puesto adecuado.

d. Utilizar y acordar la autoridad adecuada para cada miembro de la

e. administración.

f. Proporcionar facilidades personales y otros recursos.

g. Ajustar la organización a la luz de los resultados del control.

2.2.12.2LA EJECUCION

Para llevar a cabo físicamente las actividades que resulten de los pasos de planeación y organización es necesario que el gerente tome medidas que inicien y continúen las acciones requeridas para los miembros del grupo ejecuten las tareas. Entre las medidas comunes utilizadas por el gerente para poner el grupo en acción, están, dirigir, desarrollar, instruir, ayudar a los miembros a mejorarse en el trabajo mediante su propia creatividad y la composición de esto conlleva a la ejecución de los planes establecidos.

2.2.12.2.1 ACTIVIDADES IMPORTANTES DE LA EJECUCIÓN.

a. Poner en práctica todo lo afectado por la decisión.

b. Conducir y retar a otros para que hagan su mejor esfuerzo.

c. Comunicar con efectividad.

d. Motivar a los miembros.

e. Desarrollar a los miembros para que realicen todo su potencial.

f. Recompensar con reconocimiento y buena paga por un trabajo bien hecho.

g. Satisfacer las necesidades de los empleados a través del esfuerzo de trabajo.

h. Revisar los esfuerzos de la ejecución a la luz de los resultados del control.

4. EL CONTROL

Los gerentes siempre han encontrado conveniente comprobar o vigilar lo que se está haciendo para asegurar que el trabajo de otros está progresando en forma satisfactoria hacia el objetivo predeterminado. Establecer un buen plan, distribuir las actividades componentes requeridas para ese plan y la ejecución exitosa de cada miembro no asegura que la empresa será un éxito, pueden presentarse discrepancias, malas interpretaciones y obstáculos inesperados y habrán de ser comunicados con rapidez al gerente para que se emprenda una acción correctiva.

ACTIVIDADES IMPORTANTES PARA EL CONTROL.

a. Evaluar los resultados contra los estándares de desempeños.

b. Idear los medios efectivos para medir las operaciones.

c. Comunicar cuáles son los medios de medición.

d. Transferir datos detallados de manera que muestren la comparación y las variaciones.

e. Informar a los miembros responsables de las Interpretaciones.

f. Comparar los resultados con los planes generales.

g. Seguir las acciones correctivas cuando sean necesarios.

h. Ajustar el control a la luz de los resultados del control (Ibid).

En la realidad, la planificación está involucrada en el trabajo de organizar, ejecutar y controlar. De igual manera, los elementos de ejecutarse utilizan en planear y controlar con efectividad, cada función es fundamental de la administración afecta a las otras y todas están relacionadas para formar el proceso administrativo.

Toma de decisiones: Es el medio de elegir y manejar las operaciones de la forma correcta a fin de que actúe con rapidez para alcanzar los objetivos trazados logrando la efectividad y eficiencia de la organización sustentado en la información real.

2.2.13 PROCEDIMIENTOS QUE DEBEN SEGUIRSE PARA GARANTIZAR LA CONFIABILIDAD DE LA INFORMACIÓN FINANCIERA.

Los procedimientos que a continuación se especifican, tienen por objeto garantizar la integridad de la información que ha de ser contabilizada, la cual se produce como resultado de las operaciones.

• Efectivo: Es necesario determinar cuál debe ser la cantidad que se mantenga en efectivo y realizar periódicamente una evaluación del manejo del mismo.

• Transacciones: Todas las transacciones y acontecimiento ocurridos durante un periodo determinado han sido efectivamente reflejadas en los registros contables.

• Imprevistos: En algunas ocasiones se presentan situaciones imprevistas, lo que obliga a realizar determinados desembolsos, como la indemnización de un ejecutivo que se separa de la empresa, fondo de contingencias.

• Presentación: La información financiera presentada en los estados financieros es suficiente, adecuada y está correctamente clasificada.

• Los principios de la contabilidad generalmente aceptados (PCGA).

PCGA: Tiene como finalistas lograr que los estados financieros sean apropiados y se rijan bajo un mismo estándar. Su efectividad en el desarrollo de la práctica contable ha proporcionado el respaldo y soporte autorizado para que se constituyan en generalmente aceptados. Proporciona información útil y plenamente confiable para el usuario dentro del proceso de cuantificación pero se debe cumplir una serie de requisitos que permita vigilar la vida económica empresarial. La importancia de esta información radica en la cualidad de poder amoldarse al propósito de cada usuario, pero relacionada a su vez, a los intereses comunes que reúne toda la organización.

Criterios por los que están orientados los principios de contabilidad generalmente aceptados:

1. Utilidad (contenido informativo).
2. Confiabilidad (objetividad, verificación, estabilidad).
3. Provisionalidad.

1. **Utilidad**: Establece que la información contable que se presenta debe ser importante y pertinente al usuario; la misma obtiene su apoyo en el contenido informativo y la oportunidad.

Contenido informativo: Se refiere al valor de la información, o sea, el emitir palabras y cantidades en forma simbólica que relate el estado financiero de la empresa en sus distintas etapas, su evolución y resultados de las operaciones realizadas.

Oportunidad: La información debe llegar de manera oportuna al interesado, de forma tal, que el mismo pueda tomar decisiones adecuadas. De no proporcionarse a tiempo, puede resultar obsoleta a sus interesados, pudiéndole producir así perdida a la empresa.

2. **Confiabilidad:** Brinda la seguridad al usuario que la información se encuentre libre de errores, que es fidedigna y que no está parcializada, es decir, confiabilidad es el grado de fe que el usuario posee sobre la información que adquiere para luego utilizarla en la toma de decisiones.

Objetividad: La información contable es concisa y veraz, obteniendo su equidad sin perturbar los intereses de los usuarios.

Verificabilidad: La información contable es expuesta a pruebas que permiten comprobar su verdad para que aun, siendo personas distintas, puedan llegar a un consenso utilizando un método en sus reglas de operación.

Estabilidad: Indica que se continua bajo un mismo patrón en el proceso contable obtenido de los resultados semejantes en los diversos periodos.

3. **Provisionalidad**: La información generada requiere que los estados financieros presentados tengas un contenido actualizado que muestre claramente la condición de la empresa cada vez esta así lo requiera, aún no habiendo terminado el periodo contable y por medio de ello ejecutar nuevas operaciones que apelen en bien su desarrollo.

2.12.14 APORTES DE LA INVESTIGACIÓN

El control es una proceso mediante el cual se puede obtener información y retroalimentación que permitan asegurar mantener las funciones de planeación, organización y dirección sean exitosas. Es decir, la finalidad del control es garantizar que los resultados de lo planeado, organizado y ejecutado se ajusten tanto como sea posible a los objetivos previamente establecidos. De ahí lo importante es que se establezcan estrategias o tácticas bien definidas para que luego se conviertan en pilares sólidos y fundamentales para la optimización de los costos y la consecución de las metas establecidas.

A raíz de esto se debe valorar la necesidad de contar con un sistema de información que permita elaborar objetivos que puedan responder estas necesidades, por lo tanto se debe tomar en cuenta lo siguiente:

- Contenido: La información debe ser necesaria y relevante.

- Tiempo: La información debe transmitirse en tiempo oportuno adecuado.

- Actualidad: La información debe ser la más reciente.

- Acceso: Los miembros de la organización que necesiten utilizar información deben acceder a la misma con facilidad.

Entonces, para el logro de los objetivos organizacionales depende de la capacidad qué tenga la información-financiera ya que ésta transforma datos en información relevante para conocer la verdadera situación financiera y económica de la empresa. Está se utiliza para hacer pronósticos de condiciones y resultados financieros futuros o sea como indicador de gestión ya que sirve para indicar las áreas débiles y con problemas, y en cualquier instancia, conocer el impacto de la inflación, las acciones de los competidores, el desarrollo tecnológico, entre otros, pero para lograr la consistencia, comparabilidad y coherencia en la información financiera debe minimizarse la utilización de juicios subjetivos.

El propósito de la información es brindar una base para que se pueda administrar, controlar y analizar eficientemente los resultados obtenidos en ciertas actividades económicas de ésta manera, el sistema de control depende de la información inmediata del desempeño; para realizar las evaluación de desempeño es verificar si se obtienen los resultados, de no ser así proceder a realizar las correcciones necesarias que se deben introducir en el proceso.

En generarlas organizaciones se orientan hacia la medición, evaluación y control de tres aspectos principales:

- Resultados: resultados concretos y finales que se pretenden alcanzar dentro de cierto periodo.
- Desempeño: comportamiento o medios instrumentales que se pretenden poner en práctica.
- Factores críticos de éxito: es decir, aspectos fundamentales para que la organización sea exitosa en su resultado y en su desempeño.

  Los aspectos más focalizados del desempeño organizacional son:

- Rentabilidad: volumen de dinero generado después de deducir los gastos.
- Competitividad: éxito de la empresa frente a sus competidores.
- Eficiencia: consecución de los resultados con el mínimo de recursos.

Una vez que determinada actividad ha concluido, se miden los resultados y se comparan con los establecidos y así poder llevar a cabo las acciones correctivas que requiera el caso. Esta acción busca mantener el desempeño del nivel y los estándares establecidos para garantizar que todo se haga exactamente de acuerdo con lo planteado.

Todo lo anteriormente expuesto, ayuda para que las organizaciones lleven a cabo una toma de decisiones inteligente ya que las mismas van a estar basadas en la información financiera. En la organización se toman decisiones diariamente, unas

son rutinarias y otras no son repetitivas, pero eso si ambas requieren una información adecuada. Por eso que la importancia de contar con un sistema de información financiera es proveer información sólida y sistemática acerca del negocio y sus operaciones.

Es allí donde el Gerente es muy cuidadoso a la hora de revisar y detectar los errores al momento de la revisión y verificación de las actividades establecida diariamente durante dicha revisión es velar por el cumplimiento de los mecanismos de control interno.

Finalmente, los resultados obtenidos son evaluados eficientemente. Esto muestra que los controles ejecutados son efectivos por cuanto los errores son detectados al momento de las observaciones por parte de la administración. Es obvio que la calidad en la información asegura la mejor alternativa y estrategia que permita elegir correctamente la toma de decisiones.

2. 3. MARCO CONCEPTUAL

2.3.1Definiciones:

Acción Correctiva: Cuarta etapa del proceso de control que busca mantener el desempeño dentro de los patrones establecidos (Chiavenato 2001, p.675)

Administración: Proceso de planear, organizar, dirigir y controlar el uso de los recursos organizacionales, para alcanzar determinados objetivos de manera eficiente y eficaz (Chiavenato 2001, p.30).

Control: Consiste en la verificación que si la actividad controlada está alcanzando o no los resultados deseados (Chiavenato 2001, p.346-347).

Control Administrativo: Es el proceso mediante el cual la administración se asegura de que los recursos son obtenidos y usados eficiente y efectivamente, en función de los objetivos planeados para la organización. (Ramírez 1994, p.11).

Disponibilidad Financiera: Es el fondo monetario con que cuenta la empresa para cualquier eventualidad (Def. op).

Disponibilidad Presupuestaria: Es el fondo monetario con que cuenta cada partida según su presupuesto (Def. op.).

Estado Financiero: Es una herramienta que pronostico de condiciones y resultados financieros, es decir, es el principal medio para reportar información financiera de propósito general a las personas externas a la organización. Miyauchi (2000 p.2).

Estrategia: Es el patrón de los objetivos, propósitos o metas, establecidas de tal modo que definan la forma de conseguirlos (Def. op).

Matriz DOFA: Es una herramienta que le permite a las empresas hacer un diagnóstico, de su propia situación y su ubicación en el entorno, útil para examinar sus debilidades, oportunidades, fortaleza y amenazas. Goodstein (2001, p.271).

Organización: Unidad o entidad social en que las personas interactúan para alcanzar objetivos comunes (Chiavenato 2001 p.394).

P.C.A.G: Los principios de contabilidad de aceptación general, son las convenciones, reglas y procedimientos particulares aceptados en la práctica contable que tengan suficiente soporte, otorgado en una oportunidad determinada, por parte de una institución profesional autorizada. (Miyauchi 2001 p.3)

Procedimientos Administrativos: Es un sistema abierto y cíclico de planeación, organización, dirección y control, todas estas funciones administrativas están íntimamente relacionada entre sí son interdependientes e interactivos. (Chiavenato 2001 p.345).

2.4 FORMULACION DE LA HIPOTESIS Y VARIABLES

2.4.1 HIPÓTESIS GENERAL

Podrá la implantación de este sistema de gestión de seguridad de la información (SGSI), resolver el constante desvió y perdida de la datos que manejan las instituciones financieras en la ciudad de Babahoyo y que causan tremendas perdidas y un perjuicio a los clientes.

2.4.2 HIPOTESIS ESPECÍFICAS

- Se Comprobara si al aplicar y analizar el sistema de gestión de seguridad de la información (SGSI), se podrá formular estrategias que brinden un mejor control y resguardo de la información en las entidades financieras

- Se establecera si los procedimientos a seguir garantizaran la confiabilidad de la información financiera

- Verificar que los correctivos detectados generen una mejor información financiera a los usuarios y a la propia empresa

2.5 VARIABLES

2.5.1 INDEPENDIENTE

Implantación de un Sistema de Gestión de la Seguridad de la información (SGSI) para las entidades financieras de la ciudad de Babahoyo-

2.5.2DEPENDIENTE

Perdida y desvió constante de la información en las instituciones financiereras de la ciudad de Babahoyo

CAPITULO III

3. Tipo y Diseño de Investigación

Los tipos de investigación que utilizaremos en el desarrollo de nuestro trabajo investigativo son:

- ✓ Según su finalidad.

La investigación será aplicada, porque, va a la confrontación de la teoría en utilizar la información para el mejor manejo de las organizaciones financieras. Estudiando los problemas concretos bajo circunstancias y características concretas. Utilizando los resultados obtenidos para mejorar el estándar de competitividad y satisfacción de los organismos de control.

- ✓ Según su objetivo gnoseológico.

Será explicativa, en cuanto la situación problemática a ser analizada y descrita, debe develarse la explicación del por qué existe actualmente el desconocimiento en la utilización correcta de la información financiera.

- ✓ Según su contexto.

Es una investigación de campo dado que la investigación se realiza en el medio donde se suscita la situación problemática actual, en las instituciones financieras de la ciudad de Babahoyo.

- ✓ Según el control de las variables.

Es no experimental fundamentada en que el fenómeno observado y analizado forma parte del ciclo operativo diario del manejo de la información financiera en los bancos y cooperativas financieras de la ciudad de Babahoyo.

- ✓ Según la orientación temporal.

  La investigación será longitudinal.

- ✓ Según su perspectiva general.

  La investigación se desarrollará desde una perspectiva cuantitativa

3.1 Métodos de Investigación

Para el desarrollo de nuestra investigación emplearemos los siguientes métodos:

3.1.1 Métodos Teóricos:

- Método histórico-lógico. Se analizará la insatisfacción del consumidor en lo que respecta a los servicios e información financiera que se brindan en la ciudad de Babahoyo.

- **Método Analítico- Sintético**. Se analizarán los eventos antes mencionados, de manera que separaremos el todo en sus partes para efectuar relaciones entre los factores y después hacer una síntesis.

- Método Inductivo-Deductivo. Se realizará un análisis desde una situación particular a una situación general.

3.1.2 Método Empírico.

- Se utilizará la observación para visualizar cuidadosamente la problemática en cuanto al desarrollo empresarial, y poder obtener la

información de la realidad actual de las ramas de casa y sus problemas en las instituciones financieras de la ciudad de Babahoyo.

3.2 POBLACION Y MUESTRA

La población estará constituida de la siguiente manera:

3.2.1POBLACION

La población estará constituida de la siguiente manera:

DENOMINACIÓN	CANTIDAD
Número de empleados en las instituciones financieras de la ciudad de Babahoyo	357
TOTAL	**357**

Fuente: Superintendencia de Bancos

3.2.2 Muestra

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

En donde,

N = Población

n = Muestra

E = Porcentaje de error $(0.05)^2$

DESARROLLO:

$$n = \frac{357}{(0.05)^2\ (357-1) + 1}$$

$$\frac{357}{0.0025(356)+1}$$

$$\frac{357}{1.89}$$

n = 188

3.3 TECNICAS E INSTRUMENTOS PARA LA RECOLECCION DE DATOS

3.3.1 Fuentes de información

Se utilizarán dos tipos de fuentes de información:

a) Fuente primaria.

Entrevistas a los empleados bancarios de la ciudad de Babahoyo.

b) Fuente secundaria (bibliográfica-linkografía):

Para obtener la información que sustenta este trabajo de investigación, se asistió a bibliotecas y otros centros de documentación como la Biblioteca General de la Universidad Técnica de Babahoyo, Cámara de Comercio e Babahoyo, SRI, Internet (recopilación de teoría en general y temas relacionados con el presente trabajo).

3.3.2 Técnicas para la recolección de la información

Se utilizaran dos tipos de técnicas:

a) Estudio documental, que consistirá en el análisis de la bibliografía relacionada con nuestro tema de investigación.

b) Entrevista personal utilizado un cuestionario estructurado.

3.4 Procedimiento

Los resultados de la investigación se presentaran en tablas y cuadros estadísticos, los que se realizaran por medio de un programa especialmente diseñado en Microsoft Excel y la redacción del texto se realizará en Microsoft Word.

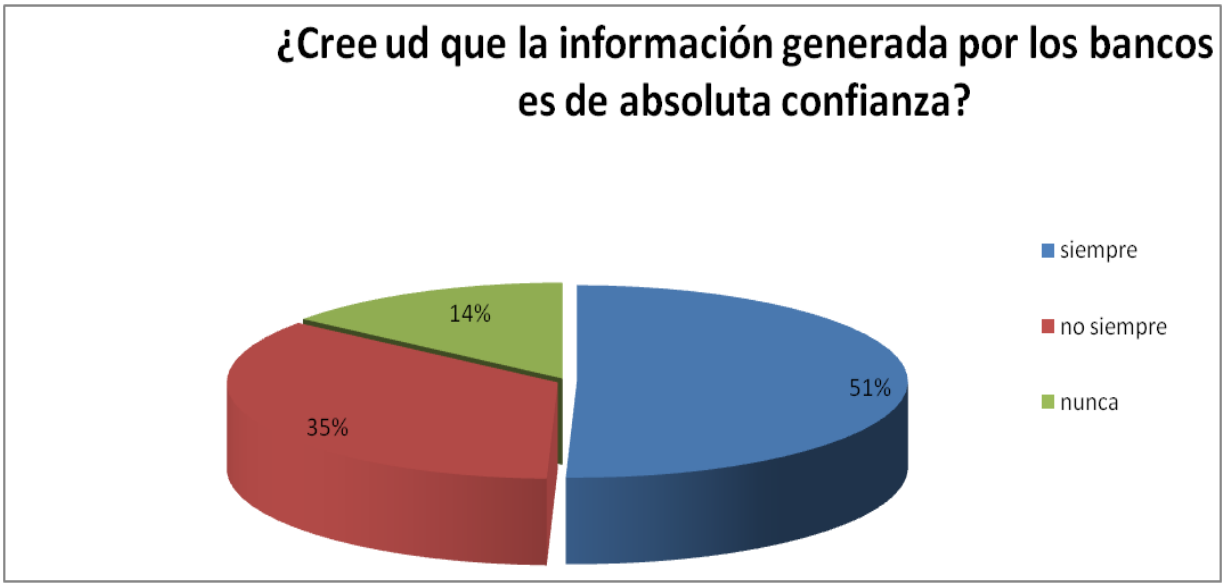
3.5 TRATAMIENTO DE LA INFORMACION

La tabulación de los datos y obtención de los resultados se realizará por medio de un programa informático en Microsoft Excel, utilizaremos pruebas no paramétricas

3.6 INTERPRETACIÓN DE DATOS

PREGUNTAS PARA EMPLEADOS INTERNOS DE LAS INSTITUCIONES FINANCIERAS DE LA CIUDAD DE BABAHOYO

1. ¿Cree ud que la información generada por los bancos es de absoluta confianza?	Datos	%
siempre	95	51%
no siempre	66	35%
nunca	27	14%
Total	**188**	**100**

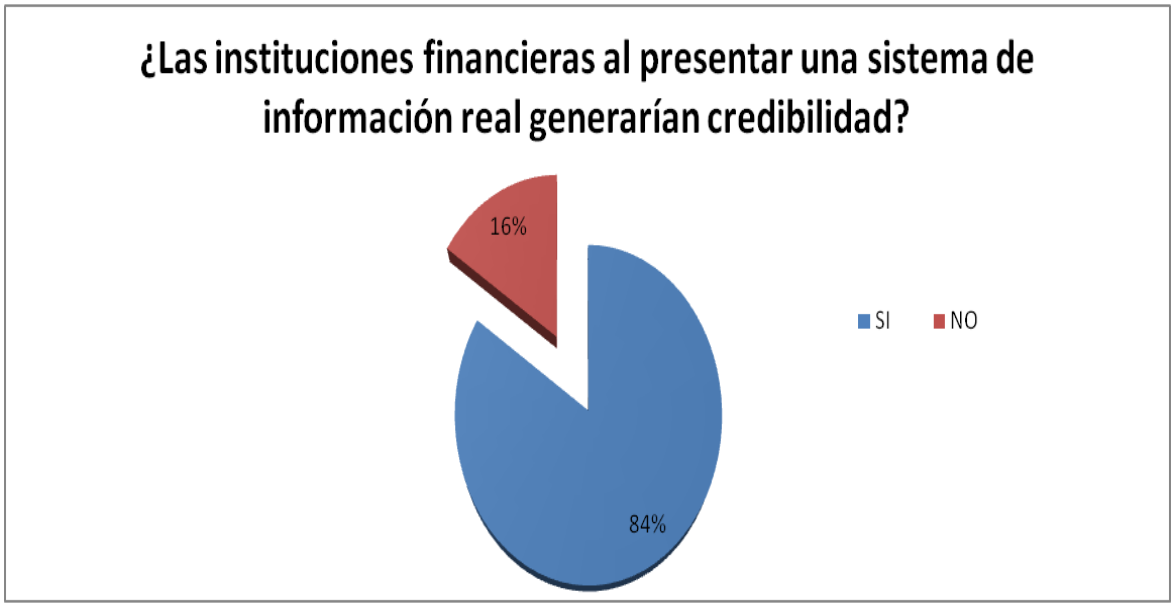


Elaborado por: Los Autores

Análisis de Datos

El 51% de los encuestados opina que la información proporcionada por los bancos es absolutamente confiable, el 35% opina que no siempre es de confianza mientras que el 14% de las personas opinaron que en ningun momento son garantía de confianza

2. ¿Las instituciones financieras al presentar una sistema de información real generarían credibilidad?	Datos	%
SI	158	84%
NO	30	16%
Total	**188**	100

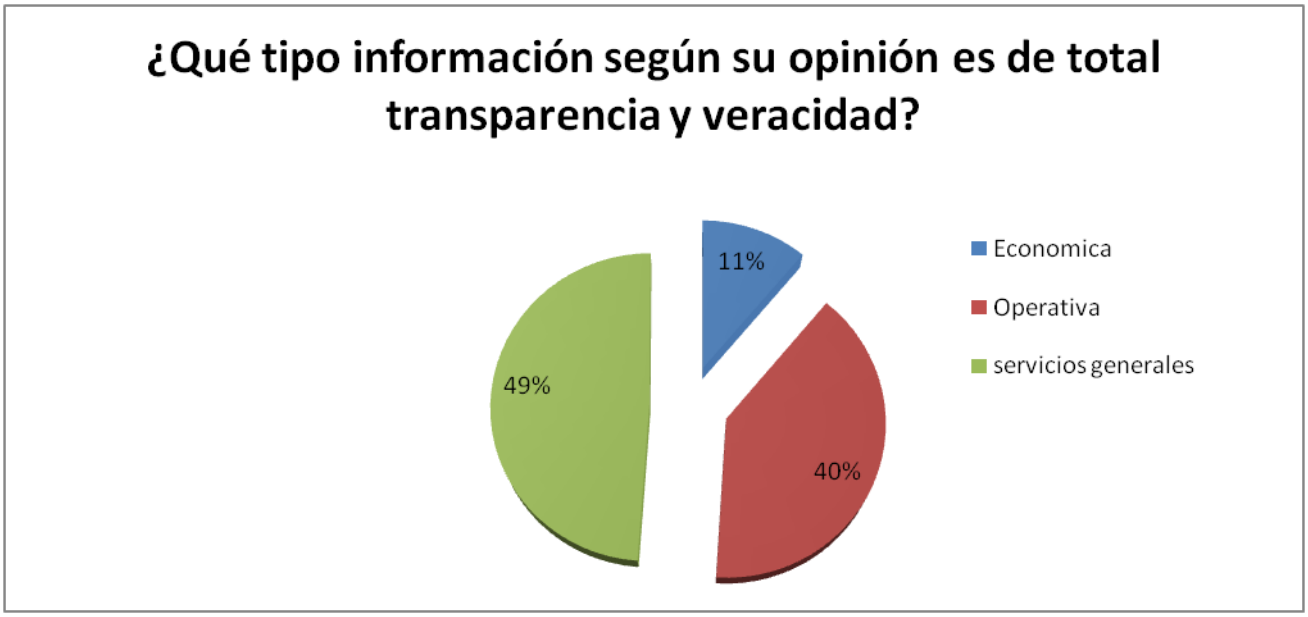


Elaborado por: Los Autores

Análisis de Datos

El 84% de los encuestados dicen que si generarían credibilidad al presentar los estados financieros, el 16% opina que no generaría confianza al presentar la información financiera

3 ¿Qué tipo información según su opinión es de total transparencia y veracidad?	Datos	%
Economica	21	11%
Operativa	75	40%
servicios generales	92	49%
Total	**188**	100

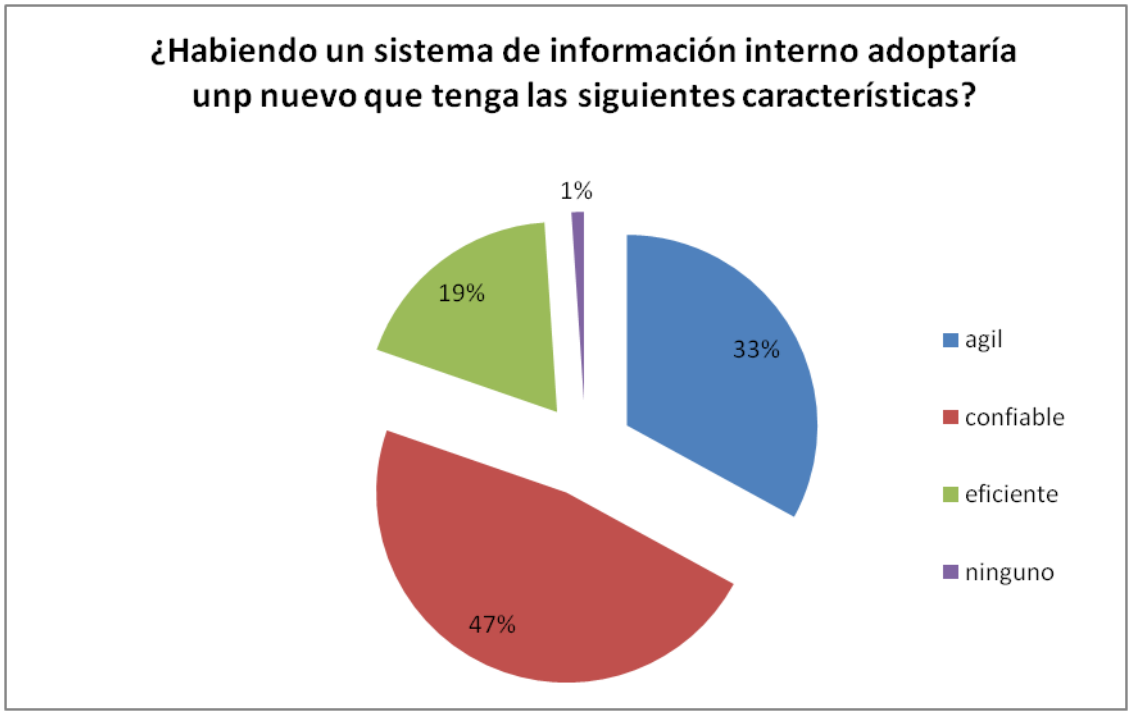


Elaborado por: Los Autores

Análisis de Datos

El 11% de los encuestados nos dice que la información económica es la de mayor transparencia y veracidad, el 40% opino que la información operativa tiene mayor transparencia, mientras que el 49% opino que la información de servicios generales es la de mayor veracidad.

4 ¿Habiendo un sistema de información interno adoptaría uno nuevo que tenga las siguientes características?	Datos	%
Agil	62	33%
Confiable	89	47%
Eficiente	35	19%
Ninguno	2	1%
Total	**188**	100

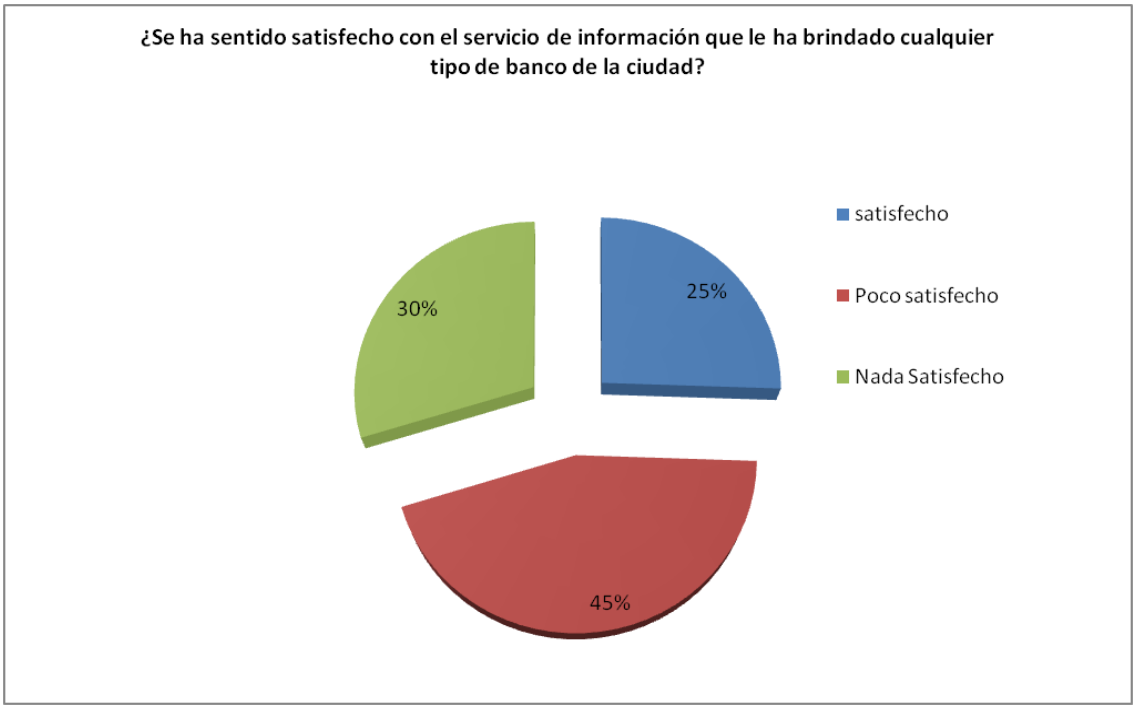


Elaborado por: Los Autores

Análisis de Datos

El 33% de los encuestados opina que adoptaría un sistema de información agil, el 47% un sistema confiable, el 19% un sistema eficiente, el 1% ninguno.

5¿Se ha sentido satisfecho con el servicio de información que le ha brindado cualquier tipo de banco de la ciudad?	Datos	%
satisfecho	48	25%
Poco satisfecho	84	45%
Nada Satisfecho	56	30%
Total	**188**	100



Elaborado por: Los Autores

Análisis de Datos

El 25% de los encuestados opina que si se han sentido satisfecho con el servicio de información proporcionado, el 45% opina que se ha sentido poco satisfecho, mientras que el 30% opino que se ha sentido nada satisfecho.

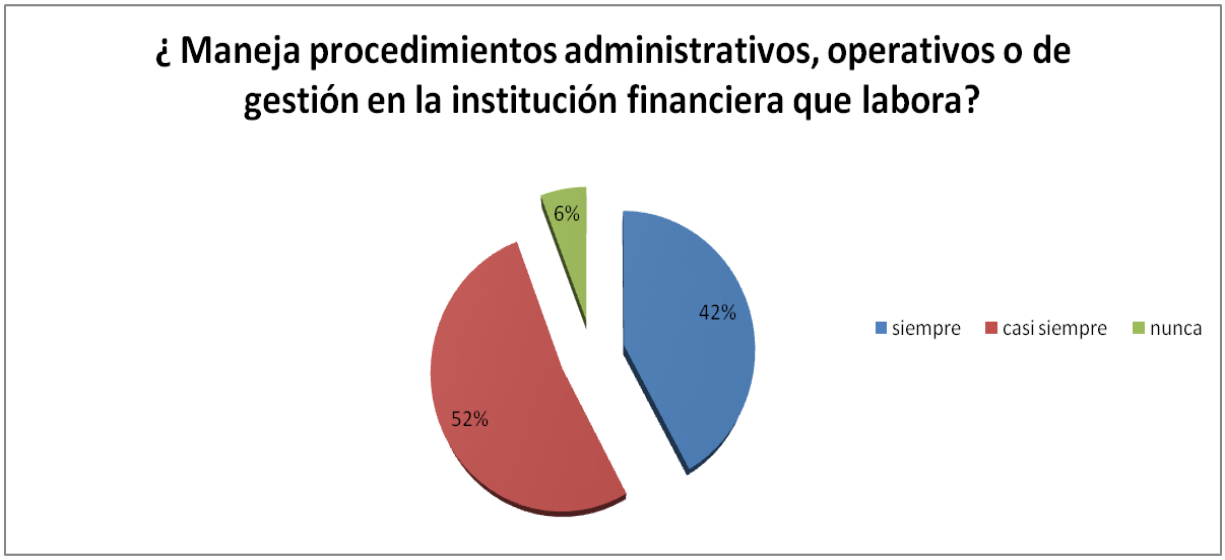
6 ¿En su opinión falta más cultura organizacional para aplicar un mejor sistema de información financiera?	Datos	%
si	126	67%
no	62	33%
Total	**188**	100

Elaborado por: Los Autores

Análisis de Datos

El 67% de los encuestados considero que si hace falta mas cultura organizacional para aplicar mejor un sistema de información financiera, el 33% opino que no hace falta cultura organizacional en lo que respecta a al sistema de información financiera.

7. ¿ Maneja procedimientos administrativos, operativos o de gestión en la institución financiera que labora	Datos	%
siempre	79	42%
casi siempre	98	52%
nunca	11	6%
Total	**188**	100

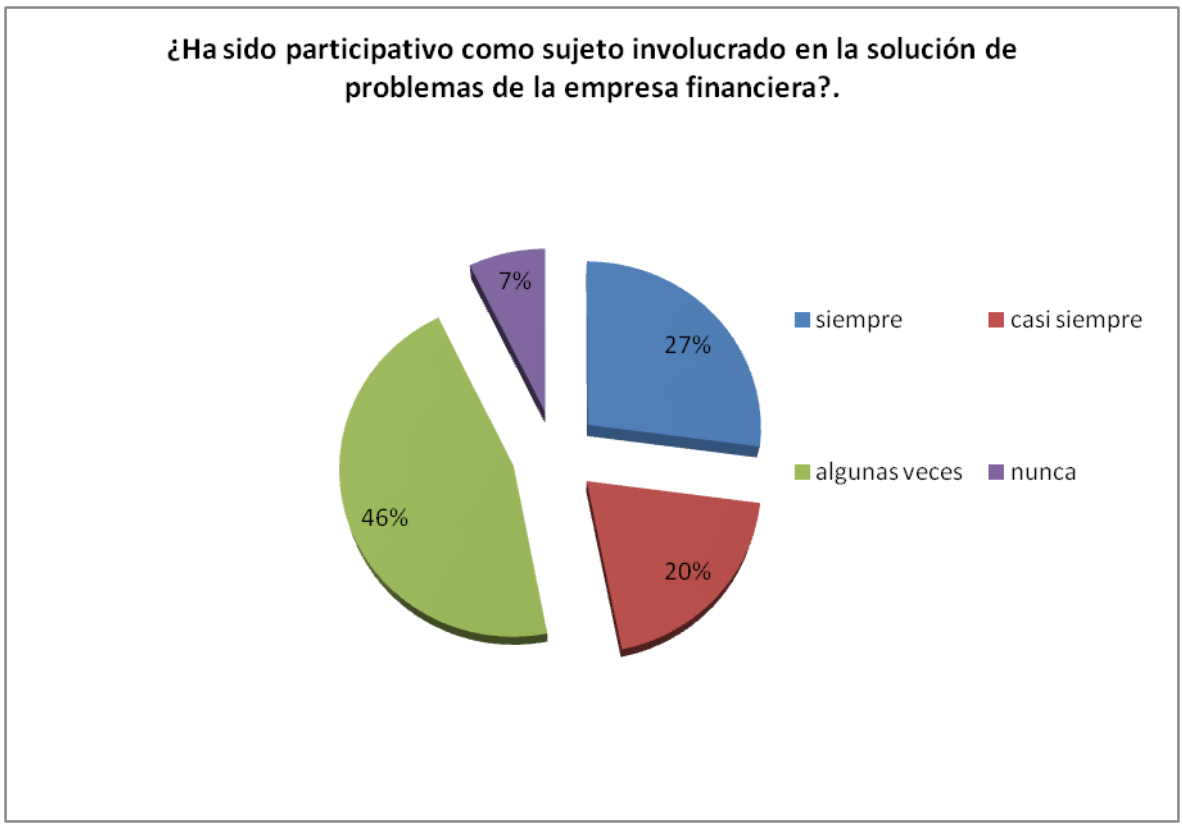


Elaborado por: Los Autores

Análisis de Datos

El 42% de los encuestados nos dijo que si maneja procedimientos administrativos, operativos o de gestión siempre, el 52% opino que casi siempre, el 6% nos dijo que nunca había manejado ese tipo de procedimientos.

8.¿Ha sido participativo como sujeto involucrado en la solución de problemas de la empresa financiera?.	Datos	%
siempre	52	27%
casi siempre	38	20%
algunas veces	88	46%
nunca	10	7%
Total	**188**	100



Elaborado por: Los Autores

Análisis de Datos

El 27% de los encuestados opino que siempre ha participado como sujeto involucrado en la solución de problemas, el 20% nos dijo que casi siempre se vio participando en los problemas financieros de la empresa, el 46 opino que algunas veces, mientras que el 7% nos informo que nunca ha participado

3.7 Análisis e Interpretación de Resultados

- El 51% de los encuestados opina que la información proporcionada por los bancos es absolutamente confiable, el 35% opina que no siempre es de confianza mientras que el 14% de las personas opinaron que en ningun momento son garantía de confianza

- El 84% de los encuestados dicen que si generarían credibilidad al presentar los estados financieros, el 16% opina que no generaría confianza al presentar la información financiera

- El 11% de los encuestados nos dice que la información económica es la de mayor transparencia y veracidad, el 40% opino que la información operativa tiene mayor transparencia, mientras que el 49% opino que la información de servicios generales es la de mayor veracidad.

- El 33% de los encuestados opina que adoptaría un sistema de información ágil, el 47% un sistema confiable, el 19% un sistema eficiente, el 1% ninguno.

- El 25% de los encuestados opina que si se han sentido satisfecho con el servicio de información proporcionado, el 45% opina que se ha sentido poco satisfecho, mientras que el 30% opino que se ha sentido nada satisfecho.

- El 67% de los encuestados considero que si hace falta mas cultura organizacional para aplicar mejor un sistema de información financiera, el 33% opino que no hace falta cultura organizacional en lo que respecta a al sistema de información financiera.

- El 42% de los encuestados nos dijo que si maneja procedimientos administrativos, operativos o de gestión siempre, el 52% opino que casi siempre, el 6% nos dijo que nunca había manejado ese tipo de procedimientos.

- El 27% de los encuestados opino que siempre ha participado como sujeto involucrado en la solución de problemas, el 20% nos dijo que casi siempre se vio participando en los problemas financieros de la empresa, el 46 opino que algunas veces, mientras que el 7% nos informo que nunca ha participado

CAPITULO IV

4. PROPUESTA DE TESIS

Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) para las entidades financieras de la ciudad de Babahoyo

4.1 Introducción

Diseñar e implementar un SGSI dependerá de los objetivos estratégicos del negocio y las necesidades de las instituciones financieras, siendo estos los parámetros básicos para la definición del alcance de su implementación. Promover la ejecución de este proyecto proviene de las áreas directivas responsables del buen funcionamiento de la entidad y se convierte en un requisito indispensable para garantizar el éxito del proyecto.

Un SGSI varía según el tipo de organización y el sector económico en el que se encuentre, sin embargo, el procedimiento para la implementación y mantenimiento independiente del tipo de organización, debe seguir un ciclo de mejora continua. Es el método más adecuado para la implementación de un SGSI ya que propone una estrategia de mejora continua en 4 pasos: Planear, hacer verificar y actuar. Las fases que a continuación se describen, definidas por el ciclo Deming, permiten entender todo el procedimiento de implementación del SGSI para las entidades bancarias.

4.2 Fundamentación Teórica de la Propuesta

4.2.1 Fase I – Definición del alcance del SGSI

El alcance de un SGSI dependerá de la identificación de aquellos procesos considerados críticos y sobre los cuales se implementará el SGSI, al momento de definir el alcance del SGSI, el responsable del proyecto debe tener claros los siguientes aspectos:

- Las características del negocio. Tipos de productos y/o servicios ofrecidos, y clientes objetivo.
- Modelo de organización de la entidad bancaria. Por procesos, por productos o por funciones.
- Ubicación y área de cubrimiento. Presencia nacional y/o internacional, grado de penetración frente a las demás entidades bancarias dentro del total de personas bancarizadas en el país.
- Clasificación de todos los activos de la entidad bancaria

De acuerdo con la Organización Internacional de Estándares dentro del estándar ISO/IEC 27001:2010, para definir el alcance se incluyen:

- Todas las interfaces que operan en la organización
- Todas las áreas involucradas en los procesos
- Todos aquellos proveedores que incidan en el SGSI

El método mas preciso para determinar el alcance de un SGSI, es la metodología de elipses. Este método establece que se han de tomar cada uno de los procesos de una organización y separarlos para su análisis de la siguiente manera:

- Identificar los procesos básicos y listar los subprocesos de cada uno de ellos. Estos se ubican en la elipse central o concéntrica
- Ubicar en la elipse intermedia las interacciones que el proceso analizado tiene con otros procesos dentro de la organización, ligándolos a través de flechas
- En la última elipse o capa mas externa, se identifican y se ligan las organizaciones externas a la entidad y que tienen alguna relación o con el proceso analizado.

Sin embargo existen otros métodos para su definición, señala que una herramienta práctica, sencilla y de fácil aplicación son los mapas mentales, estos mapas son herramienta fundamental en la gestión de cualquier proyecto, que permite la memorización, organización y representación de los procesos.

4.2.2 Fase II – Planeación de un SGSI

Gran parte de los proyectos que se llevan a cabo en las organizaciones fracasan antes de concluir por la falta de una planeación apropiada. La buena planeación, concentrada en el modelado del futuro, junto con la supervisión y el control de los procesos, son la clave para el éxito en un proyecto.

En la planeación entonces, se incluirán todas aquellas actividades que ayudarán a lograr la implementación exitosa del SGSI., en esta fase se deben tener identificados los siguientes aspectos:

- Definir un objetivo y el alcance del proyecto.
- Establecer el presupuesto necesario para ejecutar el proyecto.
- Nombrar un gerente del proyecto.
- Nombrar un equipo de trabajo quien asumirá diferentes responsabilidades referentes al proyecto.
- Conocer toda la documentación relativa a los procesos de negocio para los cuales se implementará el SGSI y las Políticas de Seguridad existentes en la Organización.
- Definir y documentar roles, responsabilidades y dedicación en tiempo de los integrantes del equipo de trabajo para garantizar una selección idónea.
- Estructurar el plan detallado de actividades para el alcance definido.
- Desarrollar un cronograma de actividades que contenga tiempos, responsables, presupuesto y fecha de entrega para la implementación del SGSI.

Aclarados estos aspectos del proyecto, se hace necesaria la definición de una metodología de trabajo, a la hora de seleccionar un estándar de trabajo en la gerencia del proyecto se debe tener en cuenta lo siguiente:

- Utilizar una terminología común. Revisar la terminología a usar al interior del equipo de trabajo para reducir riesgos de inconsistencias y simplificar la comunicación.
- Definir un ciclo de vida para el proyecto.
- Seguir estrictamente las directrices del estándar escogido para la gerencia del proyecto.
- Ejecutar rigurosamente el procedimiento de trabajo escogido, verificando los avances, el cumplimiento de los compromisos y el chequeo constante de todos los aspectos esenciales del mismo, lo cual garantiza el cumplimiento de los ítems anteriores.

4.2.3 Fase III – Estructuración del SGSI

Luego de determinar el alcance y todas aquellas actividades propias de la planeación, se da inicio al proceso de definición del SGSI a través de una serie de actividades de recolección de información y de análisis de la misma para la toma de decisiones. La definición del SGSI comprende la realización de las siguientes actividades:

4.2.4 Diagnóstico de Seguridad de la Información

El Diagnóstico de Seguridad persigue la identificación del estado de la Seguridad de una Organización, para ello existen básicamente dos aproximaciones. La primera,

implica la realización de un análisis de riesgos de los sistemas de información, mientras que la segunda se lleva a cabo mediante la determinación del estado de la seguridad de una entidad frente a un estándar. De acuerdo con el (Guía de implantación de un sistema de gestión de seguridad de la información basado en el estándar ISO/IEC27001:2009, 2010), el mejor diagnóstico al interior de las entidades bancarias parte de la evaluación comparativa frente al estándar ISO 27002:2010

El diagnóstico comprende entonces una serie de acciones definidas a continuación.

- **Análisis de Cumplimiento de la norma internacional (ISO/IEC 27002:2010):**

De acuerdo con el diagnóstico de seguridad, esta primera acción tiene por objeto analizar el grado de cumplimiento de los controles de seguridad que tiene actualmente la entidad bancaria con relación a los definidos por la norma ISO/IEC 27002:2005 mediante la revisión de la documentación existente en la organización, entrevista con personal clave en los diferentes procesos, evaluación de la reglamentación existente y revisión de la legislación aplicable a la organización. Los resultados de este análisis deberán ser documentados en un informe de nivel de cumplimiento de acuerdo con los estándares internacionales.

- **Estudio de Riesgos de Seguridad**

Otro elemento fundamental del diagnóstico de seguridad consiste en establecer el nivel de seguridad actual, determinar los riesgos y con base en estos resultados definir el modelo de seguridad más apropiado

Esta etapa es considerada como una de las más críticas dentro del proceso de definición del SGSI y es uno de los resultados en los que una futura auditoria de certificación enfocará su revisión para observar el nivel de riesgo obtenido y las opciones de tratamiento definidas.

El desarrollo del análisis de riesgos, estará basado en la metodología recomendada por el estándar BS7799-3:2006, obteniéndose como resultado el informe de análisis de riesgos, en el cual se mostrará el nivel de riesgo de cada activo de información, resultado de evaluar el impacto, vulnerabilidades, amenazas, y factor de ocurrencia de amenazas y vulnerabilidades.

En líneas generales, para actualizar y obtener la respectiva matriz de riesgos se seguirán una serie de tareas recomendadas que se describen a continuación:

- **Identificación de activos de información y valoración del riesgo.**

De acuerdo con los conceptos básicos de contabilidad, todos aquellos bienes tangibles e intangibles y los derechos que tienen valor o utilidad son considerados activos que posee cualquier empresa, ahora, un concepto más cercano al objeto de investigación es el que ofrece el Consejo Superior de Administración Electrónica [CSAE], (2010), quien denomina a los activos como "los recursos del sistema de información o relacionados con este, necesarios para que la organización funcione correctamente y al alcance los objetivos propuestos por su dirección". Sin embargo y

para delimitar de forma correcta el alcance de un sistema de seguridad de información, solo se pondrán en consideración los llamados activos de información. La información es considerada como insumo fundamental que actúa como facilitador para los objetivos de la organización, con base en ella se desarrolla su negocio y es un elemento vital para el desarrollo modelo de negocio de la organización. En el contexto de la norma ISO 27001:2010, un activo de información será: "…algo a lo que una organización directamente le asigna un valor y, por lo tanto, la organización debe proteger".

Con base en los procesos definidos en el alcance del SGSI, se listan los activos de información asociados a estos, igualmente se listan los componentes críticos tales como software, hardware e infraestructuras que soporten dichos procesos. La identificación de estos activos es esencial para saber que hay que proteger y para hacer una correcta clasificación mediante criterios de confidencialidad, integridad y disponibilidad.

Siguiendo los estándares de la norma ISO 17799:2010, los activos de información para las entidades del sector bancario se pueden clasificar en las siguientes categorías:

- Activos de Información. Ficheros, bases de datos de clientes, bases transaccionales, documentos del sistema, manuales de usuario, procedimientos

documentados, planes de continuidad, información archivada en medios digitales o impresos.

- Documentos legales. Contratos con proveedores relacionados con los procesos críticos.
- Activos de Software. De aplicación, del sistema operativo, nuevos desarrollos que puedan exponer información critica del negocio.

- Activos de Hardware. Servidores de aplicación

- Servicios. De red (TCP/IP, FW, Router, Switch).

- Personas. Clientes y empleados.

- Otros. Imagen corporativa, objetivos, reputación.

Dado que los activos de información abarcan diferentes elementos, es básico que se tenga claro este concepto y sus diferentes clasificaciones, sin embargo y con base en el método de elipses se puedan categorizar e identificar dichos activos de forma más exacta.

La tasación de activos, se puede determinar con base en instrumentos de recolección de datos, la escala Likert como método estadístico permite clasificar y jerarquizar con base en las preguntas realizadas, los activos que afectan la confidencialidad, integridad y disponibilidad.

La responsabilidad sobre cada uno de estos activos recae en cada uno de sus propietarios quien tiene la tarea de clasificar su nivel de seguridad, derechos de acceso y el mantenimiento de controles apropiados.

4.2.5 Análisis y evaluación de riesgos

El análisis de riesgos facilita la selección de los mecanismos de protección, permiten estimar las pérdidas potenciales que dichos mecanismos ayudan a reducir facilitando la selección de los mismos.

Como lo señala, el documento que de esta etapa se derive, será el que se implantará durante la fase de implementación del SGSI y sus acciones serán de corto, mediano y largo plazo.

La *metodología de análisis y gestión de riesgos de los sistemas de información* – MAGERIT - es el núcleo de las actuaciones relacionadas con el análisis, la

evaluación y la gestión del riesgo. Esta metodología analiza los riesgos, identifica las amenazas y su impacto y gestiona el riesgo basado en:

- Elementos (activos, amenazas, vulnerabilidades, riesgos, impactos, salvaguardas)
- Eventos (estáticos, dinámicos organizativos, dinámicos físicos)
- Procesos (planificación, análisis de riesgos, gestión de riesgos, selección de salvaguardas)

4.2.6 Amenazas.

De acuerdo con la normas ISO 27000, se considera amenaza aquella causa potencial de un incidente no deseado, el cual puede causar daño a un sistema o a una organización.

Se coinciden en que las amenazas se pueden clasificar en grandes grupos para facilitar la toma de decisiones genéricas que reduzcan grupos de amenazas bajo una sola acción. Los grupos propuestos son:

- Naturales. Fuego, inundación, terremotos, etcétera.
- Humanas Accidentales. Desconocimiento, negligencia, despidos, pérdida no intencional de información.
- Humanas Intencionales. Robo de información, ataques.

- Tecnológicas. Virus, hacker, crackers, pérdida de datos, fallas de software, hardware ó de red

Las amenazas reales y exitosas en su intención son aquellas que dejan al descubierto varias vulnerabilidades en los sistemas, aplicaciones o servicios.

Luego de identificadas todas las amenazas, se evalúa su probabilidad de ocurrencia bajo el modelo Likert, a cargo del grupo de expertos de la organización. El resultado de esta evaluación permitirá identificar las amenazas de mayor a menor concurrencia y la decisión sobre cuales atacar y cuales descartar de acuerdo con criterios técnicos, legales y de costos.

4.2.7 Vulnerabilidades.

Las vulnerabilidades están asociadas a debilidades de los activos de información. La vulnerabilidad en el contexto de los sistemas de información, es considerada como la ausencia o debilidad en los controles que ayudan a mitigar un riesgo, aumentando el nivel de impacto y el factor de exposición. Es una debilidad en el sistema, aplicación, infraestructura, control o diseño de flujo que puede ser explotada para violar la integridad del sistema. En general se puede considerar entonces que el concepto de vulnerabilidad se centra en la incapacidad que pueda tener un sistema de seguridad

En esta parte del proyecto, el equipo de trabajo tiene por objetivo identificar las ausencias o debilidades que potencializan los riesgos. Un proceso de entrevistas individuales de manera estructurada, profunda y directa con las personas que tienen a su cargo la tarea de ejecutar las políticas de seguridad de la organización, permitirá evidenciar posibles fallas en los sistemas de información y en la implementación de los mecanismos de control y de defensa que actualmente se tienen, adicionalmente se deberá realizar un conjunto de pruebas de vulnerabilidad e intrusiones sobre la infraestructura tecnológica que soporta los procesos para los cuales se va a implementar el SGSI con el objetivo de verificar su nivel de seguridad e identificar los riesgos existentes en estos dispositivos. El modelo de Likert es un método útil para identificar y jerarquizar las vulnerabilidades que luego servirán para determinar los procedimientos para mitigar los riesgos a los que se expongan los sistemas de información.

Dado que las amenazas y las vulnerabilidades tienen interrelación, se parte de la pregunta sobre cuáles vulnerabilidades son aprovechadas por las amenazas, pues, una vulnerabilidad identificada genera amenazas que se convierten en un riesgo expuesto sobre cualquier sistema de información de una entidad bancaria, esto es lo que para expertos en temas de seguridad de información se conoce como la *relación causa-efecto entre el elementos del análisis de riesgo*, por lo tanto, el siguiente paso será el de integrar estos elementos para analizar y definir los niveles de riesgo que

luego permitirán implementar los procedimientos que ayudarán a mitigar tales riesgos y eliminar las vulnerabilidades.

4.2.8 Procedimiento para el análisis y evaluación de riesgos.

Un procedimiento ordenado y lógico para el análisis de riesgo contiene los siguientes pasos:

1. Identificación de activos relevantes para la organización. El valor y la interrelación se basan en el costo del perjuicio que este genere.
2. Determinación de los controles de seguridad dispuestos y su eficacia
3. Identificación de las vulnerabilidades para cada activo de información.
4. Determinación de las amenazas a las que están expuestas estos activos
5. Cálculo de la probabilidad de ocurrencia de una amenaza sobre las vulnerabilidades identificadas.
6. Estimación del nivel de riesgo, definido como la magnitud del impacto sobre la explotación exitosa de la vulnerabilidad.

El análisis de riesgo permitirá identificar y calcular el riesgo sobre los activos basados en amenazas y vulnerabilidades, sin embargo, para cada organización, el concepto de riesgo varía según su objeto de negocio y los activos de información que posee. Se considera riesgo a cualquier hecho definido como incierto que genera impactos negativos, sin embargo y llevando el concepto de riesgo a la información

misma, se considerará el riesgo en los activos de información como la probabilidad de que una amenaza se materialice aprovechando las vulnerabilidades de un sistema de información (Guía de de implantación de un sistema de gestión de seguridad de la información basado en el estándar ISO/IEC27001:2005, 2010).

Una vez se listan y clasifican los activos y se identifican las amenazas y vulnerabilidades, se procede al cálculo del riesgo. Este cálculo utilizará valores cuantitativos pues el valor de un activo de información se tasa en el impacto en pérdidas económicas que el mismo genera si es vulnerado.

El análisis de riesgo se puede realizar de 2 formas:

- Análisis cuantitativo. Basado en la métrica y el cálculo de valores que determinen el costo-beneficio, su cálculo demanda un gran esfuerzo, pero permiten la comparación de valores.
- Análisis cualitativo. Es más ágil, pero sus resultados son más subjetivos los cuales no se basan en cifras y contienen análisis sencillos. No permiten la comparación de valores más allá del orden relativo.

Los expertos en temas de seguridad de información coinciden en afirmar que el análisis de riesgo es un proceso permanente pues las organizaciones son sistemas abiertos, complejos y en constante readaptación, por lo que los análisis cualitativos pueden ofrecer los mejores resultados, sin embargo y tal como lo plantean, serán la

naturaleza del proyecto y la disponibilidad de tiempo y dinero las que influyan en la técnica a utilizar.

Las entidades del sector bancario colombiano, dada su infraestructura, los altos costos de operación, la complejidad de sus sistemas de información, la sensibilidad de la información allí almacenada y otros aspectos tales como la determinación de primas de reaseguradoras, hacen que sea necesaria la aplicación de técnicas cuantitativas, dado que la implementación de un sistema de seguridad de información es visto como un proyecto de gran escala y de alta complejidad. Los métodos cuantitativos y de modelamiento mas recomendados son el análisis de árboles de decisión, la simulación y el análisis de sensibilidad.

4.2.9 Plan de tratamiento de riesgos

A partir del informe de evaluación de riesgos se procede a examinar cual es el tratamiento más adecuado para cada uno de los riesgos que han sido identificados.

Siguiendo los lineamientos del al norma ISO 27001:2010, el tratamiento de riesgos comprende los siguientes enfoques:

- Determinar si el riesgo es aceptable o si requiere un tratamiento, en cuyo caso se identificará una de las siguientes alternativas:
- Reducir el riesgo a un nivel aceptable, implantando algún control (combinación de personas, procesos y herramientas).

- Aceptar el riesgo porque no es posible realizar un tratamiento o porque éste resulta demasiado costoso.
- Evitar el riesgo.
- Transferir el riesgo a una tercera parte (Por ejemplo, Compañías de Seguros).
- En caso de que se decida mitigar el riesgo se debe definir que controles del SGSI se deben implementar. Además, si se considera necesario se pueden seleccionar controles específicos adicionales.
- Preparar un documento de Declaración de Aplicabilidad (DDA), en el que se detalle la relación de controles que se van a implantar.
- Establecer el nivel de riesgo aceptable para la Organización.
- Obtener la aprobación de la dirección a la DDA y a los riesgos no cubiertos.
- Formular un plan de tratamiento de riesgos en el que se establecerán las acciones necesarias para conseguir mitigar los riesgos a un nivel aceptable y para implantar los controles que se consideren necesarios según requerimiento de la norma ISO/IEC 27001:2010 en sus numerales 4.2.1.f, g y h.
- Preparar los procedimientos necesarios para la implantación de controles. En cada procedimiento se detallarán los objetivos que se pretenden cubrir, las razones para su elección, cómo se implanta el control y las responsabilidades asociadas

4.3 Desarrollo de la Propuesta de Tesis aplicando el modelo de Seguridad para la Información en las Instituciones financieras de la ciudad de Babahoyo

4.3.1 Definición de las políticas de seguridad

Luego de establecer el alcance del SGSI, será necesario definir y documentar la política de seguridad. Se establece *"*concebir y redactar la política recae sobre los responsables del funcionamiento de la misma (…) el elemento fundamental de estos documentos es que expresan el consenso de quienes conocen mejor que nadie los *principios* operativos, económicos y éticos que conducirán al éxito colectivo*". La política incluirá los siguientes principios básicos:*

- Reconocimiento y concientización de la importancia de la seguridad de la información para los resultados del negocio.
- Señalar el riesgo al que están expuestos los sistemas de información y a su vez el efecto inmediato sobre las operaciones del negocio bancario.
- Seguimiento estricto a las normas legales y los estándares internacionales para el manejo seguro de la información.
- Coparticipación, compromiso y co-responsabilidad de todos los miembros de la organización de manera individual y como organización.
- Visión de largo plazo pero con capacidad de autoevaluación y reajuste

Estas políticas se convierten entonces en una declaración expresa de la intención de conseguir algo que contribuye a la seguridad de la información, definiendo que

necesita protegerse y cómo hacerlo, oponiéndose a las amenazas identificadas y satisfaciendo las exigencias de seguridad de la información que definen las normas legales y los estándares internacionales.

La política de seguridad tendrá como mínimo los siguientes elementos:

- Una definición de seguridad de la información y sus objetivos globales.
- El establecimiento del objetivo de la dirección que soporte los objetivos y principios de la seguridad de la información.
- Una explicación detallada de las políticas, principios, normas y requisitos mas importantes para la entidad bancaria:
- Conformidad con los requisitos legislativos y contractuales
- Requisitos de capacitación en temas de seguridad
- Prevención y detección de virus y software malicioso
- Gestión de continuidad del negocio
- Consecuencias sobre la violación de la política de seguridad
- Requisitos de uso para sistemas de información
- Controles técnicos
- Controles a proveedores externos y el teletrabajo.

4.3.2 Desarrollo de procedimientos para la Gestión de la Seguridad de la Información

Todas las amenazas y las vulnerabilidades evidenciadas hay que enfrentarlas, lo que requiere una planificación constante de las diferentes alternativas de solución, por lo tanto luego de haber sido definidas las políticas de seguridad de la información, se elaborarán los procedimientos de seguridad para soportar el SGSI y el modelo de seguridad diseñado.

El desarrollo de procedimientos para la gestión de seguridad de la información se traduce en el desarrollo de políticas, normas y procedimientos y junto a ellos la aplicación de salvaguardas y controles que verifican y garantizan que cada amenaza tiene su respuesta adecuada.

La definición de estos procedimientos de gestión de seguridad facilita la transferencia de conocimiento que en el futuro ayudará en la aplicación de mejoras al sistema de gestión por cuenta del personal interno de la organización.

Todo este conjunto de políticas y procedimientos de seguridad para establecer un SGSI, deben estar alineados con el estándar ISO/IEC 27001:2010 que se compone de 11 dominios:

1) Política de seguridad

2) Organización de la seguridad de la información

3) Administración de recursos

4) Seguridad de los recursos humanos

5) Seguridad física y del entorno

6) Administración de las comunicaciones y operaciones

7) Control de acceso

8) Adquisición, desarrollo y mantenimiento de sistemas de información

9) Administración de los incidentes de seguridad

10) Administración de la continuidad de negocio

11) Cumplimiento (requerimientos legales, estándares, técnico y auditorías)

Durante la ejecución del proyecto se considera el desarrollo de los siguientes procedimientos esenciales en seguridad, indicados por el estándar ISO/IEC 27001:2010, a saber:

- Control de Documentos
- Control de Registros
- Controles de acceso
- Proceso de auditorías internas
- Acciones Preventivas (Salvaguardas técnicas, físicas, medidas de organización)
- Acciones Correctivas

- Proceso de revisión Gerencial
- Gestión de Incidentes de seguridad
- Gestión de copias de respaldo y Backup de Información
- Gestión de RR.HH. (Políticas de personal, Administración de Usuarios y Contraseñas)
- Control de Cambios
- Inventario y Clasificación de Activos de información
- Seguridad de los Medios e Información en Tránsito

4.3.3 Fase I Plan de Concientización en Seguridad de la información

Esta fase comprende las actividades necesarias, para establecer la estrategia de sensibilización y divulgación de políticas y procedimientos para la Gestión de la Seguridad de la Información, con el propósito de establecer al interior de la organización un grado de compromiso y concientización con respecto al SGSI.

Las actividades de concientización no solo se deben orientar hacia los temas de seguridad que es importante que se refuercen mediante una campaña de comunicación. Un criterio igualmente importante es la respuesta de la audiencia frente a los diferentes medios de difusión o divulgación de los contenidos.

Existen diferencias en el aprendizaje de las personas que deben ser contempladas a la hora de diseñar una campaña de concientización. Un enfoque muy eficaz consiste en determinar para una audiencia dada los siguientes criterios:

- El estilo preferido de aprendizaje.
- El nivel de conocimientos actual

Debido a que la seguridad de la información es una preocupación nueva para las organizaciones y que el tema de concientización es considerado parte integral de las soluciones de seguridad, se proponen las siguientes actividades:

- Determinar cuál es el estado actual de conciencia sobre la seguridad de la información en las áreas de la Organización involucradas en la implementación del SGSI. Una forma de llevar a cabo esta actividad, es mediante la selección de un grupo de funcionarios seleccionados por muestreo para que contesten un cuestionario sobre conceptos básicos de seguridad de la información. Esta información será tabulada y se generaran las estadísticas que permitan conocer el grado de cultura en seguridad que tiene la organización. En esta fase también se evaluarán los medios que actualmente posee la organización para los procesos de divulgación y que hayan resultado efectivos.

- Una vez se determine el estado de concientización en la organización, se contará con la información necesaria para el diseño y documentación de la mejor estrategia para la concientización y divulgación de los aspectos de seguridad y del SGSI de la organización.

4.3.4 Fase II – El Monitoreo y control al SGSI

El rápido avance en el desarrollo de la tecnología impacta los planes de seguridad de la información en cualquier organización y ello hace que los mecanismos de seguridad implementados puedan deteriorase con el paso del tiempo. Un plan de monitoreo ayudará a revelar nivel de deterioro en el que se encuentra el SGSI y a definir las acciones correctivas necesarias.

"El monitoreo y el control de riesgos involucra la ejecución de los procesos de la administración del riesgo para responder a los eventos que comprometen la seguridad de la información".

La revisión es un ejercicio práctico con resultados métrico orientado a calcular el nivel de eficiencia en la respuesta del SGSI. Los procedimientos para llevar a cabo este monitoreo y la revisión están detalladas en la ISO 27001:2010 y de acuerdo con Guía de implantación et al. 2010 su ejecución debe ayudar a:

- Detectar errores

- Identificar las fallas de seguridad
- Controlar que las actividades de seguridad se realicen de acuerdo a lo establecido
- Definir las acciones a implementar para corregir errores y fallas

La norma ISO 27001:2010 estipula las siguientes actividades orientadas al monitoreo y revisión del SGSI:

- Identificación de eventos de seguridad y evasión de incidentes de seguridad.
- Evaluar la efectividad de las acciones ejecutadas para resolver los incidentes de seguridad.
- Establecimiento de criterios de medición de la efectividad de los controles.
- Revisión periódica de la política y del alcance del SGSI
- Revisión de los riesgos residuales y los riesgos aceptables
- Auditorias internas y externas del SGSI

En el caso de las auditorías, la misma norma recomienda la aplicación de auditorias periódicas pues esta actividad ayuda a determinar que los controles, los objetivos, los procesos y los procedimientos continúan actuando en conformidad con la norma y para analizar y planificar las acciones de mejora.

En este sentido los diferentes autores citados coinciden en que las auditorías internas y externas pueden ayudar a arrojar información mas confiable, objetiva y relevante para la ejecución de planes de mantenimiento o mejoras al SGSI.

Hasta acá entonces, se ha logrado dividir, conceptualizar y detallar paso a paso todas aquellas actividades que le permiten a una entidad financiera implementar un sistema de gestión de seguridad de la información, como todo sistema es evolutivo y su capacidad de respuesta y adaptación estará condicionado por las buenas practicas adoptadas desde la definición y hasta la puesta en marcha del proyecto. Existen otras actividades asociadas a este proyecto, pero se han dejado claras las mas relevantes y de mayor incidencia para el mismo y con las cuales garantizar su éxito.

4.3.5 Discusión

Hablar de seguridad de la información y de políticas y procedimientos para el manejo de la misma en Colombia es un tema que trascendió de la novedad a la exigencia y de ahí a ser inherente al desarrollo de un negocio. Todo este bagaje bibliográfico abordado para desarrollar el tema me ha permitido observar como la sociedad ha evolucionado. Décadas atrás el tema de la información como factor crítico del negocio era lejano, considerado por muchos como un intangible que carecía de fuerza para vulnerar la estabilidad y el futuro de una organización.

El avance tecnológico y el salto revolucionario no solo rompe con los esquemas en los que la humanidad ha vivido sino que dejan al descubierto nuevos valores y nuevos riesgos asociados a los mismos y es allí donde la información como cobra su papel preponderante. Las entidades financieras no difieren de cualquier otro tipo de organización de otros sectores, son sistemas abiertos, que reciben insumos de todo tipo que luego de ser procesados se convierten en productos y servicios para el mercado, sin embargo dentro de los insumos de entrada, es la información el que tiene mayor relevancia.

Los modelos de CRM, modelos predictivos, modelos de riesgo, estrategias comerciales selectivas, todo este conocimiento estratégico propio del negocio se basa en la información que se extrae de los clientes y del medio, pero es una información que está expuesta a riesgos, por lo tanto si las empresas no establecen sistemas que aseguren la integridad, la confidencialidad y la disponibilidad de la información jamás podrán mantenerse compitiendo en el mundo globalizado.

Implementar un modelo de SGSI de acuerdo con todos los autores es el camino correcto para garantizar que la información circulante dentro de una entidad financiera, se hace de forma segura. La problemática que se pueda estar presentando hoy es que tal vez las entidades financieras consideren que sus sistemas de seguridad de información son eficientes y que sus controles son adecuados, pero dichos sistemas y controles son meramente reactivos y no proactivos.

Uno de los elementos esenciales que deja este rastreo bibliográfico al tema de la gestión de seguridad de la información, es que los procedimientos son cíclicos y que la tecnología tiene vida y evoluciona cada vez con mayor complejidad por lo tanto no puede concebirse que un SGSI mida su eficiencia en la capacidad de adaptarse a cada riesgo asociado a los incidentes que van apareciendo. La verdadera capacidad de un SGSI debe ser la de poder atenuar el riesgo antes de que pueda atacar, por lo tanto los SGSI se implementan exclusivamente para mitigar los riesgos a los que están sujetos los activos de información y no para responder de forma reactiva en forma de ensayo y error cuando los incidentes ocurren.

4.4 CONCLUSIONES Y RECOMENDACIONES

4.4.1 Conclusiones

- Aunque el modelo presentado en este artículo y la normatividad internacional relacionada con el tema de la implementación de modelos de seguridad de la información son aplicables a cualquier tipo de organización, la implantación de un SGSI en entidades financieras tienen una mayor repercusión e importancia dada la diversidad de activos de información que estas organizaciones manejan y el nivel de criticidad de los mismos. Vulnerar la seguridad en la información de una entidad financiera no solo tiene un costo muy alto a nivel financiero sino también a nivel de imagen tanto de la entidad afectada como del sector financiero en general, sobre el cual recae la mayor parte del peso del desarrollo económico nacional y sobre el cual se ha depositado la confianza de miles de usuarios del sector bancario.

- Una de las razones mas importantes para implementar un SGSI es la de atenuar los riesgos propios de los activos de información de las entidades financieras. Una acertada identificación de tales activos, una definición correcta del alcance y unas políticas de seguridad claras y completas, son determinantes para la correcta implantación del SGSI.

- Un SGSI en una entidad bancaria no puede ajustarse cada vez que se genera un incidente de seguridad, pues la labor de quienes tienen la función de gerenciar la seguridad de la información en las entidades financieras no puede ser únicamente la de administrar los controles creados para cada situación de riesgo.

Se debe actuar de manera proactiva para tratar de anticiparse a tales hechos y para ello el SGSI debe estar en capacidad de ayudar a la alta dirección en la definición de acciones que mitigan los riesgos sobre los activos más críticos sin tener que esperar a que los eventos ocurran.

- La implantación de un SGSI requiere de una alta participación a nivel estratégico y su papel es protagónico, pues dicha implantación es un proyecto que reclama tiempos, actividades, recursos, por lo tanto la alta gerencia debe conocer y ser conciente de la importancia de la seguridad y de las consecuencias de no llevar a cabo su implementación.

- La implantación y operación de un SGSI ofrece ventajas para las entidades bancarias al disponer de una metodología dedicada a la seguridad de la información reconocida internacionalmente, contar con un proceso definido para evaluar, implementar, mantener y administrar la seguridad de la información, diferenciarse en el mercado frente a otras entidades financieras, satisfacer requerimientos de clientes, proveedores y organismos de control, formalizar las responsabilidades operativas y legales de los usuarios internos y externos de la Información y ayuda en el cumplimiento de las disposiciones legales nacionales e internacionales.

4.4.2 RECOMENDACIONES

- La información puede ser útil para la organización ya que ésta le permite establecer pautas de acción en cuanto al propósito de la misma.

- Dichas pautas van a transformarse luego en estrategias fundamentales para las empresas.

- La formulación de estrategias en las organizaciones se basa en un análisis detallado de los factores que intervienen y que ejercen influencia en ella.

- También, la información financiera facilita llevar un buen control administrativo para que propicie un mejoramiento continuo de las actividades que realizan las empresas. Permitiendo así, medir y corregir los resultados obtenidos diariamente y compararlo con los objetivos planeados.

- Además, le brinda una gran ayuda al proceso de la estrategia para determinar cuál deberá ser la estrategia competitiva hacia dónde debe orientarse la empresa y lograr una posición atractiva en el mercado.

4.5 BIBLIOGRAFIA

- Alexander, A. G. (2007). Diseño de un sistema de gestión de seguridad de la información. Bogotá: Alfaomega.
- Alonso, M.C. (2005). Impacto social de las tecnologías de la información en las formas de vida. Ahciet:Revista de Telecomunicaciones, 75.
- Ambriz, R. (2004, Enero 14). Una herramienta práctica y sencilla para definir el alcance del proyecto: los mapas mentales. The project manager"s homepage, Articulo 67924, Extraído el 8 de marzo de 2009 en:
- http://www.allpm.com/modules.php?op=modload&name=News&file=article&sid=937&mode=thread&order=0&thold=0
- Campos J. M. & Duque G. (2008). Comportamiento y evolución del sistema bancario colombiano de 1990 al 2006. Memorias para optar el título de Magister en Ingeniería Industrial, Escuela de Ingeniería, Universidad de los Andes, Bogotá D.C.
- Corlettti, A. (2006, Abril 4). Análisis de ISO-27001:2005. Articulos de seguridad informática. Extraído el 13 de abril de 2009 en:
- Daltabuit, E., Hernández, L., Mallen, G. & Vasquez, J. (2007). *La seguridad de la información*. Mexico: Limusa Ediciones
- Drucker, P. (2005). *Gerencia para el futuro*. Bogotá: Norma.
- Del Carpio, G. (2006). Análisis del riesgo en la administración de proyectos de tecnología de información, [Versión electrónica], Industrial Data, 1 (9), 104-107
- España, Consejo Superior de Administración Electrónica. (2006). Metodología de análisis y gestión de riesgos de los sistemas de información [Versión electrónica].
- Colombia, Etek International Holding Corp. (2008). Guía de implantación de un sistema de gestión de seguridad de la información basado en el estándar ISO/IEC27001:2005. Manuscrito no publicado.

- Hernández, J. (2009). La gestión de la información en las organizaciones: Una disciplina emergente. [Versión electrónica]. Documentación de las ciencias de la información, 13, 133-148.
- López, J. & Sebastian, A. Gestión Bancaria. *Los nuevos retos en un entorno global*. España: McGraw Hill/Interamericana.
- López, N. (2005). La seguridad más que un valor agregado en los sistemas de información. *Revista universidad católica de oriente.* 19, 107 - 117
- Muñoz, J.J. (2004). Metodología para la incorporación de medidas de seguridad en sistemas de información de gran implantación: confianza dinámica y regulación del nivel de servicio para sistemas y protocolos de internet. Trabajo de grado para optar al título de doctor, Escuela de ingeniería de sistemas telemáticos, Universidad Politécnica de Madrid, Madrid, España.
- Ozz, E. (2007). *Administración de Sistemas de Información (2ª ed*). México: Thomson Learning.
- Puig, T. (2008, Mayo 15). Implantación de un sistema de gestión de seguridad. Cursos de Tecnologías de Información. Extraído el 15 de marzo de 2009 en: http://www.mailxmail.com/curso/empresa/gestiondeseguridad
- Peña, D., Aguilar, M., Belloso, N., & Parra, J. (2005). Factores de cambio en los sistemas de información del sector bancario [Versión electrónica]. *Revista Venezolana de gerencia, 23, 480-495*
- Tipton H. F., Krause M. (2007). Information security management handbook. Palm Beach, FL: CRC Press.
- Vittoriano E. (2008, Agosto). La información como activo. Conferencia presentada en la Conferencia latinoamericana de auditoria, control y seguridad (Latin America CACS) 2008, Santiago, Chile.

Velásquez M., Mauricio A. (2006). Ceros y unos: La economía de la información. *Informática al día, 111,* 19-23

4.5.1 LINKOGRAFIA

- www.iin.oea.org/manual_proyectos.PDF

- http://www.unamosapuntes.com/code3/ceneval/finanzas/unamos6.html

http://orbita.starmedia.com/~unamosapuntes/presupuestos/presupuestosonline.htm

- http://www.gestiopolis.com/canales/financiera/articulos/24/tir1.htm

Anexos

Anexo 1

Presupuesto de Implantación del sistema de Información Gerencial

Presupuesto

Nombre: Martinez - Carpio	***Datos cliente***	
Dirección: Centro de la Ciudad	***Nombre***	Instituciones financieras de Babahoyo
Dirección	***Dirección***	Centro de la Ciudad
Provincia: Los Rios	***Población***	Babahoyo
CIF / NIF	***Provincia***	Los Ríos
Teléfono/fax: 052736548	***CIF / NIF***	

Fecha presupuesto/albarán:	27-nov-11	**Validez:**	**2 años**

DESCRIPCIÓN	UNIDADES	PRECIO	% DTO.	PRECIO DTO.	TOTAL
Tecnicos y asesores	3,00	600,00	3%	582,00	1.746,00
Programa informatico	1,00	1.200,00	2%	1.176,00	1.176,00
Capacitacion	8,00	84,00	3%	81,48	651,84
Contratacion de personal	5,00	400,00	5%	380,00	1.900,00
Equipos de video	5,00	145,00	5%	137,75	688,75
Equipos de computacion	2,00	640,00	5%	608,00	1.216,00
Adecuacion de Oficina	1,00	1.300,00	5%	1.235,00	1.235,00
			Total Bruto		**8.613,59**
			I.V.A. %	**16%**	**1.378,17**
			Total presupuesto.....		**9.991,76**

Forma de pago : **cheque/ingreso en cuenta/ en metálico (lo que corresponda)**

Nombre, apellidos y firma de la persona que confecciona el presupuesto.	**ACEPTO EL PRESUPUESTO.** Nombre, apellidos y firma del cliente.

Anexo 2

1. ¿Cree ud que la información generada por los bancos es de absoluta confianza?	**Datos**	%
Siempre		
no siempre		
Nunca		
Total		

2. ¿Las instituciones financieras al presentar una sistema de información real generarían credibilidad?	**Datos**	%
SI		
NO		
Total		

3 ¿Qué tipo información según su opinión es de total transparencia y veracidad?	**Datos**	%
Economica		
Operativa		
servicios generales		
Total		

4 ¿Habiendo un sistema de información interno adoptaría unp nuevo que tenga las siguientes características?	**Datos**	%
agil		
confiable		
eficiente		
ninguno		
Total		

5¿Se ha sentido satisfecho con el servicio de información que le ha brindado	**Datos**	%
cualquier tipo de banco de la ciudad?		
satisfecho		
Poco satisfecho		
Nada Satisfecho		
Total		

6 ¿En su opinión falta más cultura organizacional para aplicar un mejor sistema de información financiera?	**Datos**	%
si		
no		
Total		

7. ¿ Maneja procedimientos administrativos, operativos o de gestión en la institución financiera que labora	**Datos**	%
siempre		
casi siempre		
nunca		
Total		

8.¿Ha sido participativo como sujeto involucrado en la solución de problemas de la empresa financiera?.	**Datos**	%
siempre		
casi siempre		
algunas veces		
nunca		
Total		