PARTE IV

6. Conclusiones.

1. La cultura organizacional se refiere a un sistema de significado compartido entre sus miembros y que distingue a una organización de otra, en nuestra organización financiera analizada, se determina que los principales conceptos por que la organización comparte son la innovación, el trabajo en equipo, con orientación a resultados, donde el conocimiento académico es de gran importancia, y las normas de la organización son valores positivos en la organización.

2. La cultura desempeña varias funciones en una organización. Principalmente se orienta a la definición de fronteras entre organizaciones, es decir cerca de la frontera de cada organización, su territorio y espacio. Se utiliza como transmisor de un sentido de identidad entre los miembros, facilita o contribuye a la generación de un compromiso organizacional es decir con un interés más grande que sólo un interés personal entre individuos.

3. La cultura que fue corroborada en este trabajo de campo fue una cultura de tipo club o tradicionalista. Se valoran la edad y la experiencia; recompensan la lealtad y la adaptación. Los gerentes trabajan en diversas tareas durante un ascenso lento, pero continuo en la organización. Dentro de esta organización podemos encontrar a empresas como los bancos comerciales, empresas de servicio público.

4. Capital Intelectual**,** son todos aquellos activos intangibles de una organización y comprenden a todos aquellos conocimientos tácitos o explícitos que en general dan valor económico para la empresa. La competencia efectiva estará menos basada en estrategias sobre recursos financieros y físicos, y más en estrategias de administración de conocimiento, y una de sus partes es el capital intelectual, formado por el capital humano, capital estructural y capital del cliente.

5. En el conocimiento es el activo más importante y usualmente es el valor que el personal ofrece a la institución que trabaja en una organización y que puede incrementar la calidad de atención al cliente; el cual es la aportación que pueden hacer los individuos en cuanto a la búsqueda de eficientar procesos y ser innovador, de tal suerte que constantemente se mejore la manera de trabajar con el objetivo de mantenerse como una empresa líder en su ramo.

6. La seguridad de la información, que se trata principalmente de un concepto el cual es importante que se introduzca dentro de la cultura de la organización, ya que se orienta a la protección de la información desde varios puntos de vista, no sólo el informática, por lo cual, se recomienda que se integre a la misión y a la visión de la organización, para que pueda conformarse como parte de la sangre organizacional o estrategia que moverá cada elemento de la empresa, sin olvidar el objetivo principal de la organización.

7. Las hipótesis planteadas en este trabajo de investigación fueron comprobadas; debido a que se comprobó que existe una relación directa entre la efectividad del establecimiento de una estrategia de protección de la información y la cultura organizacional en la organización del sector financiero que fue analizada en este trabajo.

8. La cultura organizacional, como se ha podido observar en los resultados obtenidos, dificulta la implantación de una estrategia de protección de información relacionada con la seguridad de la información, debido a que la cultura tradicionalista es muy arraigada y ha significado un factor que ha impedido la efectividad de la misma.

9. Respecto al capital intelectual se considera que es necesario que se de un mayor auge en la organización financiera, en la organización se reconoce que el conocimiento de procesos y metodología hace que el desempeño de cualquier organización mejore.

10. La dificultad para la implantación de la estrategia de seguridad de la información en una cultura de tipo tradicionalista, con un concepto relacionado con el capital intelectual con poco auge, aunque se cuenta con una Intranet donde de manera general se utiliza para la diseminación del conocimiento, se ve directamente relacionada con la cultura en todos los empleados y que se logre una implementación homogénea en todos los ambientes tecnológicos, ya que existe en la organización financiera de nuestro estudio una falta de cultura informática y una fuerte resistencia al cambio por parte de los usuarios del ambiente.

11. El personal encuestado y entrevistado en la organización financiera, el cual se encarga directamente de la implantación de la estrategia dentro de la misma, indica que la efectividad del programa ha dependido básicamente del tipo de cultura organizacional que se tiene debido a que dentro de una cultura organizacional de tipo tradicionalista, como la que se determinó en nuestro estudio, la efectividad de la implantación de la estrategia de seguridad de la información no ha sido del todo eficiente ya que la cultura es una cultura arraigada, con historicidad y que le ha sido difícil adaptarse a un nuevo ambiente de control.

12. La cultura actual piensa que se esta poniendo en tela de juicio y rompiendo un paradigma que hasta ahora había sido el pilar dentro de esta organización, lo cual era la confianza en los empleados que laboran en la misma.

13. El implantar controles dentro de la cultura organizacional tradicionalista objeto de nuestro estudio, ha hecho sentir a la organización de tipo financiero que los controles no son necesarios debido a que piensan que nunca les va a ocurrir un hecho en contra debido a que históricamente no se ha presentado.
14. Los esquemas de seguridad y la implantación de controles, dentro de la organización financiera de nuestro estudio, se consideran como incómodos, así como los implantadores no le dedican el tiempo necesario y otros puntos específicos a nivel tecnológico han generado puntos de conflicto para la organización.

15. La principal conclusión radica en que las hipótesis fueron comprobadas y que este tipo de organización debe reconocer el tipo de cultura organizacional que tiene para poder determinar los factores que pueden ayudar en el arraigo dentro de los factores culturales el de la seguridad de la información.

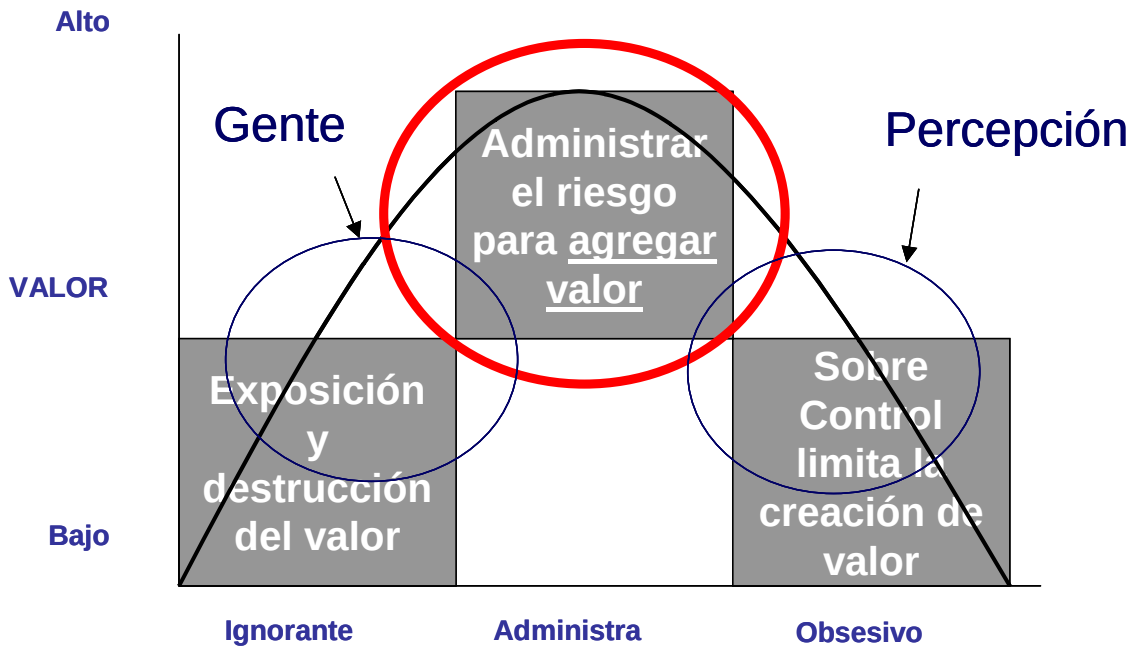
16. El programa podría mejorar mucho haciendo una evaluación global de la situación y estableciendo planes de acción conjuntos buscando metas muy especificas y a plazos cortos. Este plan debe abarcar todos los aspectos relacionados con un proceso y la evaluación deberá ser detallada en cada uno de estos aspectos, recibiendo mejor apoyo necesario de las personas directamente relacionadas en la implementación.

17. Es necesario que exista más apoyo de los directores de las diferentes áreas y mayor presupuesto para hacer mejores campañas y talleres donde todos puedan ver si sentir alguno de los impactos de no respetar las normas y como se pueden presentar las violaciones a estar reglas, esto podría enriquecer el dominio e interés de cada persona a fin de enfocar a esta cultura.

Otro punto de vital importancia que ayudará en mejor establecimiento del programa de seguridad de la información es la medición y revisión entre áreas por especialistas del grupo de la implantación que se ha seguido respecto al programa de seguridad de la información, no sólo basado en mediciones de períodos y comparaciones.

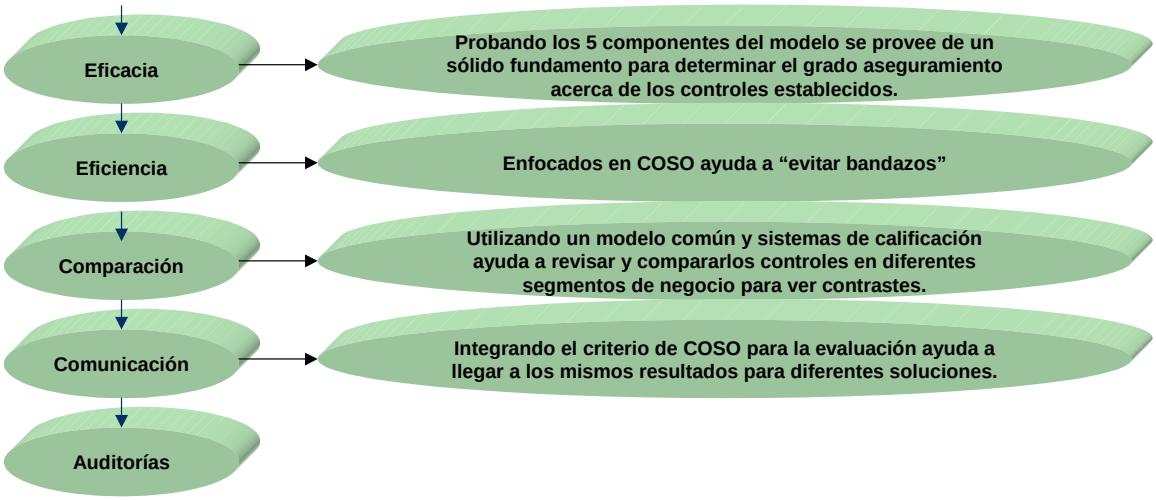
6.2 Aportaciones

En seguida se presenta una propuesta de una estrategia a seguir para poder retomar el tema de la cultura dentro de la organización objeto de este trabajo, lo cual es la aportación que se da a la organización, primero la organización se encuentra en el siguiente esquema:

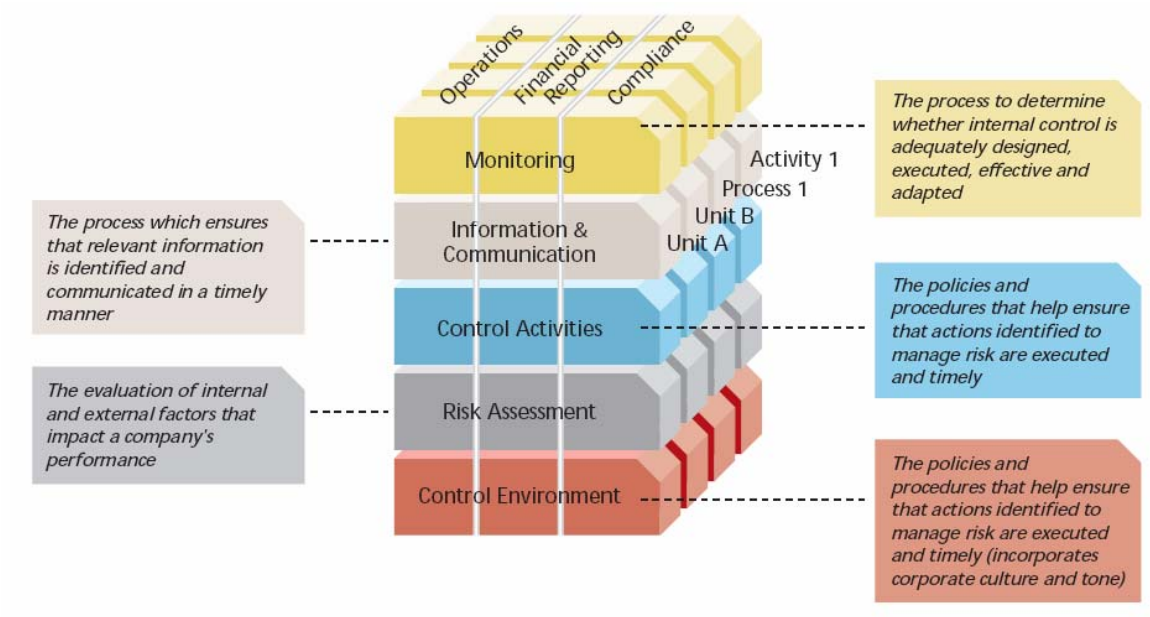


ENFOQUE AL RIESGO

El esquema que busca la organización se propone que se enfoque los siguientes puntos basados en el modelo COSO (***Committee of Sponsoring Organisations of the Treadway Commission)***:



Lo anterior puede estar basado en los componentes del modelo COSO:



El modelo anterior se recomienda basarse en los siguientes puntos:

- Descentralizar estandarizando los procesos de identificación de riesgos e implementación controles y pruebas.
- Permear la cultura de auto evaluación a mayor número de niveles de la estructura.
- Énfasis en la responsabilidad individual sobre la administración de riesgos.
- Sensibilizar a clientes, respecto al establecimiento de controles con base en riesgos.
- Diseñar productos y servicios con controles y requerimientos normativos con base en el riesgo.
- Automatizar la generación de indicadores clave enfatizando su monitoreo.
- Automatización orientada al autoservicio.