MAESTRÍA EN SISTEMAS DE INFORMACIÓN GERENCIAL

ESCUELA SUPERIOR POLITECNICA DEL LITORAL
ESPOL

Tema de Tesis:

"Creación de un Marco de Control para la Administración del Riesgo Operativo relacionado con la Tecnología de Información como modelo para las Cooperativas de Ahorro y Crédito del Ecuador"

Presentado por:

Jimmy Brito Domínguez

INTRODUCCIÓN

- Escándalos Financieros y caída de las torres gemelas, mayor énfasis en la administración de riesgos.
- El riesgo y la gestión empresarial
- El riesgo y las Instituciones financieras
- Las Cooperativas en el Sistema Financiero Ecuatoriano
- Las Cooperativas y la Tecnología
- Las Cooperativas frente a los Organismos de Control
- Las Cooperativas frente al Riesgo Operacional

OBJETIVOS GENERALES

- ✓ Establecer los lineamientos de control para la Gestión Integral de Riesgos tecnológicos en las Cooperativas de Ahorro y Crédito del Ecuador bajo las normas internacionales vigentes y aquellas establecidas por la Superintendencia de Bancos y Seguros del Ecuador.

- ✓ Determinar la factibilidad de implementación a la que se enfrentan las Cooperativas de Ahorro y Crédito Ecuatorianas para la implementación de los controles de la gestión tecnológica bajo el marco de regulación gubernamental existente.

- ✓ Presentar la visión gerencial sobre la forma en que se implementa un adecuado gobierno de tecnología de información que agrega valor a los procesos de los diferentes niveles en la pirámide organizacional de las Cooperativas de Ahorro y Crédito Ecuatorianas.

OBJETIVOS ESPECÍFICOS

- Analizar el impacto que tienen los sistemas de información en el Sistema Financiero Cooperativo y su aprovechamiento dentro de sus operaciones así como en la toma de decisiones a nivel gerencial.

- Analizar la forma en que el control interno interviene dentro de la gestión de tecnología de información.

- Identificar los estándares, lineamientos y mejores prácticas relacionadas con una gestión de tecnología de información exitosa enfocada en la mitigación de los riesgos relacionados.

- Analizar la evolución y aplicación de las normas y lineamientos sobre la gestión del riesgo operativo por parte del Sistema Financiero Cooperativo.

OBJETIVOS ESPECÍFICOS

- Establecer las diferentes variables que debe considerar una Cooperativa de Ahorro y Crédito para la implementación de los controles tecnológicos.

- Determinar la forma en que el control interno interviene dentro de la cadena de valor de una Cooperativa de Ahorro y Crédito y el impacto que ésta genera.

- Analizar la forma en que las herramientas informáticas apoyan en la gestión del riesgo operativo tecnológico.

- Definir un Marco de Control Integral para la gestión del riesgo tecnológico dentro de las Instituciones Financieras del sector de cooperativas.

Impacto de la Tecnología de Información en el Sistema Financiero Cooperativo

- Evolución del Cooperativismo en el Ecuador.
- El Cooperativismo y el Microcrédito.
- Impacto del Cooperativismo en la Economía Ecuatoriana
- Principios de las Microfinanzas
- La bancarización en los servicios ofrecidos en las Cooperativas
- Automatización de operaciones del core del negocio
- Toma de decisiones gerenciales

El Control Interno dentro del Gobierno de TI: Lineamientos y Estándares Vigentes

Estándares para el Control Interno de TI

- COBIT 4.1
- ISO 27002:2005
- ITIL 3
- PMBOK 3

El Control Interno dentro del Gobierno de TI: Lineamientos y Estándares Vigentes

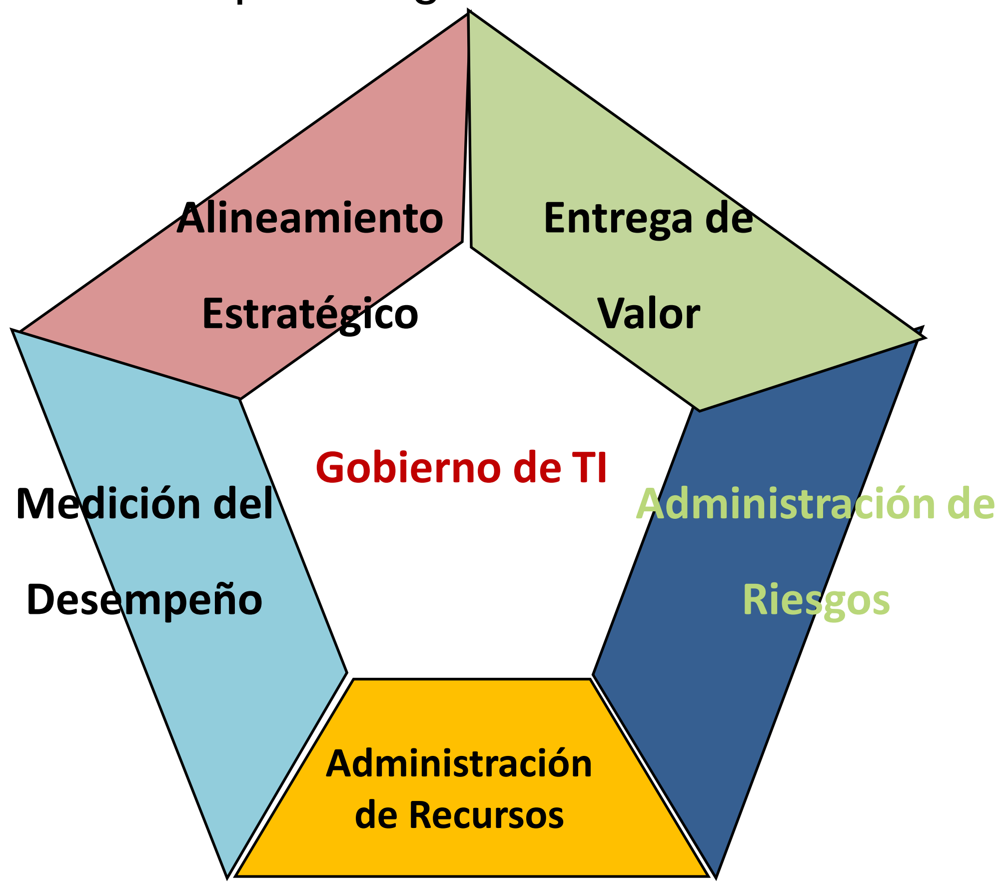
COBIT y el Gobierno de TI

- ISACA: Asociación en Control y Auditoría de Sistemas de Información
- IT Governance: Objetivos y Filosofía
  - Que la TI esté alineada con la empresa y produzca los beneficios prometidos.
  - Que la TI habilite a la empresa al explotar oportunidades y generar los máximos beneficios.
  - Que se mida el desempeño de los procesos de TI en forma eficiente y continua.
  - Que los recursos de la TI se empleen responsablemente.
  - Que los riesgos relacionados con la TI se manejen adecuadamente.

El Control Interno dentro del Gobierno de TI: Lineamientos y Estándares Vigentes

COBIT y el Gobierno de TI

- Áreas de acción para la gestión de TI:



El Control Interno dentro del Gobierno de TI: Lineamientos y Estándares Vigentes

COBIT y el Gobierno de TI

- COBIT: Objetivos de Control para tecnología de información y tecnología relacionada

- Misión de COBIT:
  Investigar, desarrollar, publicar y promover un conjunto internacional y actualizado de objetivos de control para tecnología de información que sea de uso cotidiano para gerentes y auditores.

El Control Interno dentro del Gobierno de TI: Lineamientos y Estándares Vigentes

COBIT y el Gobierno de TI

- Características de COBIT:
  - Orientado al negocio
  - Alineado con estándares y regulaciones “generalmente aceptadas”
  - Basado en una revisión crítica y analítica de las tareas y actividades en TI
  - Alineado con estándares de control y auditoría (COSO, IFAC, IIA, ISACA, AICPA)

Procesos de TI

COBIT
Objetivos del Negocio
Objetivos del Gobierno

ME1. Monitorear y Evaluar el desempeño de TI
ME2. Monitorear y Evaluar el Control Interno
ME3. Asegurar el cumplimiento de requerimientos Externos
ME4. Proveer gobierno de TI

Información
Efectividad, Eficiencia, Confidencialidad, Integridad, Disponibilidad, Cumplimiento, Confiabilidad

PO1. Definir un plan estratégico de TI
PO2. Definir la arquitectura de información
PO3. Determinar la dirección tecnológica
PO4. Definir los procesos, organización y relaciones de TI
PO5. Administrar la inversión de TI
PO6. Comunicación de la directrices Gerenciales
PO7. Administración del Recurso Humano de TI
PO8. Administrar con Calidad
PO9. Analizar y Administrar Riesgos
PO10. Administración de Proyectos

Monitorear y Evaluar

Recursos de TI
Aplicaciones
Información
Infraestructura
Personas

Planeación y Organización

Adquisición e Implementación

Procesos de TI
Dominios, Procesos y Tareas

DS1. Definir y administrar del nivel de servicio
DS2. Administrar servicios de terceros
DS3. Administrar el desempeño y la capacidad
DS4. Asegurar el servicio continuo
DS5. Garantizar la seguridad de los sistemas
DS6. Identificación y asignación de costos
DS7. Educar y Entrenar a los Usuarios
DS8. Administrar la Mesa de Servicio y los Incidentes
DS9. Administración de la configuración
DS10. Administración de problemas e incidentes
DS11. Administración de datos
DS12. Administración del Ambiente Físico
DS13. Administración de Operaciones

Entregar y dar Soporte

AI1. Identificación de soluciones automatizadas
AI2. Adquisición y mantenimiento de Software de aplicación
AI3. Adquisición y mantenimiento de la infraestructura tecnológica
AI4. Facilitar la Operación y el Uso
AI5. Proveer Recursos de TI
AI6. Administración de Cambios
AI7. Instalar y Acreditar soluciones y cambios

El Control Interno dentro del Gobierno de TI: Lineamientos y Estándares Vigentes

La Administración de Servicios a través de ITIL

- ITIL: Librería de Infraestructura de TI
- Mejores prácticas de gestión y ***entrega de servicios de TI***
- Calidad y eficiencia en las operaciones de TI, abarcando la infraestructura, desarrollo y operaciones de TI.
- Áreas de la organización como “clientes”:
  - Niveles de Servicio
  - Alta disponibilidad y continuidad
  - Alta tecnología a menor costo y oportunamente
  - Enfoque en los procesos del negocio
  - Agregar valor al negocio: Utilidad + Garantía

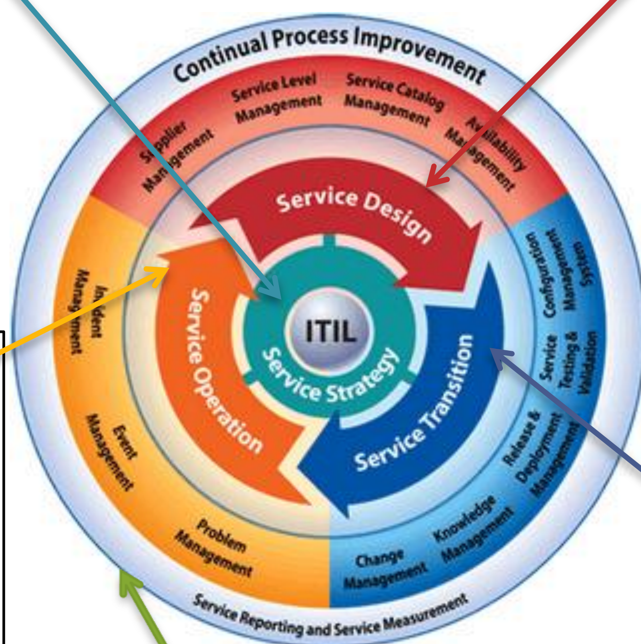
MAESTRÍA EN SISTEMAS DE INFORMACIÓN GERENCIAL

El Control Interno dentro del Gobierno de TI: Lineamientos y Estándares Vigentes

La Administración de Servicios a través de ITIL

Estrategia de Servicio:
- Generación de Estrategias
- Gestión del Portafolio de Servicios
- Gestión de la Demanda
- Gestión Financiera

Operación del Servicio:
- Gestión de Eventos
- Gestión de Incidentes
- Gestión de Peticiones
- Gestión de Problemas
- Gestión de Accesos
- Monitorización y Control
- Operación de TI
- Centro de Servicio al Usuario



Mejoramiento Continuo:
- Proceso de Mejora del Ciclo de Vida del Servicio
- Informes del Servicio

Diseño del Servicio:
- Gestión del Catálogo de Servicios
- Gestión del Nivel de Servicio
- Gestión de la Capacidad
- Gestión de la Disponibilidad
- Gestión de la Continuidad del Servicio de TI
- Gestión de la Seguridad de la Información
- Gestión de Proveedores

Transición del Servicio:
- Planificación y Soporte de la Transición
- Gestión de Cambios
- Gestión de la Configuración y Activos del Servicio
- Gestión de Entregas y Despliegues
- Validación y Pruebas del Servicio
- Evaluación
- Gestión del Conocimiento

El Control Interno dentro del Gobierno de TI: Lineamientos y Estándares Vigentes

La Administración de Seguridad a través de ISO 27000

ISO 27001:
Requisitos para establecer, implantar, poner en funcionamiento, controlar, revisar, mantener y mejorar un SGSI documentado.

ISO 27002:
Características de un SGSI, cómo se diseña, cómo se aplica y como se mantiene. Conjunto de buenas prácticas sobre objetivos de control de la seguridad de la información, compuesta por 11 dominios, 39 Objetivos de control y 133 controles.

Busca tres características de la información:

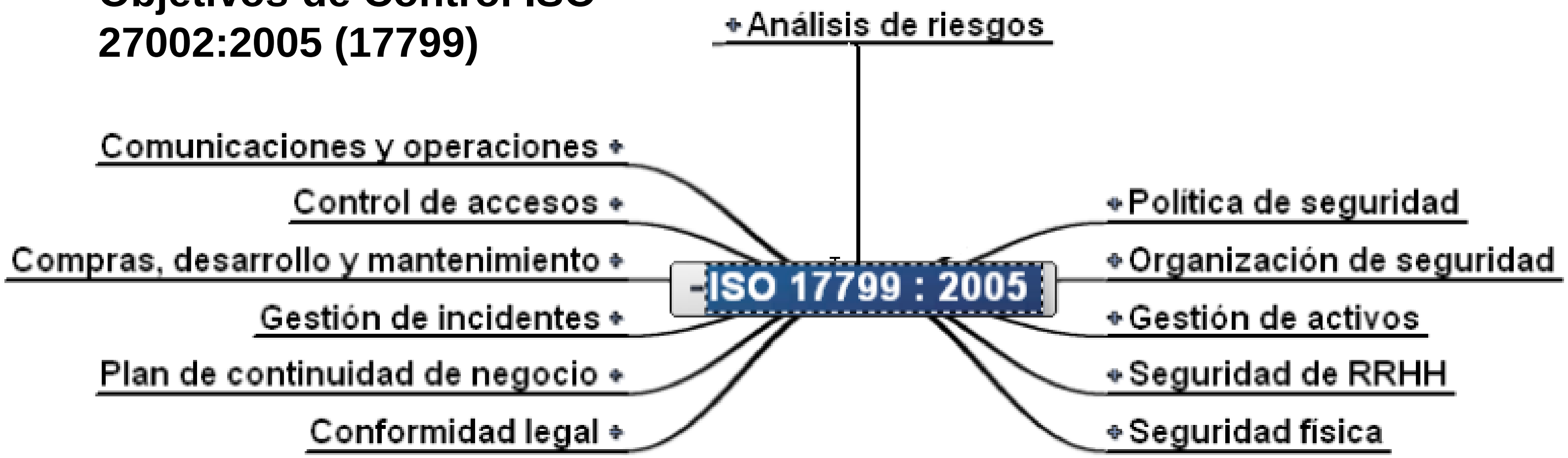
- **Confidencialidad**
- **Integridad y,**
- **Disponibilidad**

MAESTRÍA EN SISTEMAS DE INFORMACIÓN GERENCIAL

El Control Interno dentro del Gobierno de TI: Lineamientos y Estándares Vigentes

La Administración de Seguridad a través de ISO 27000

Objetivos de Control ISO 27002:2005 (17799)



La Administración del Riesgo Operativo en el Sistema Financiero Cooperativo

Estándares de Control Interno

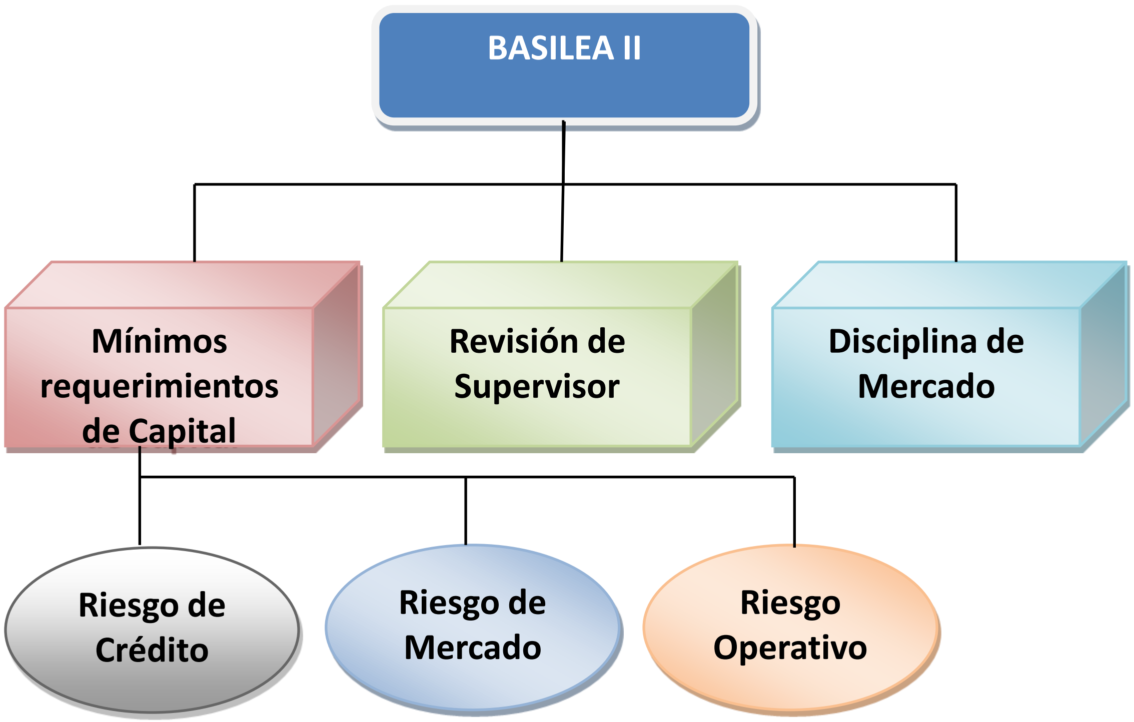
COSO-ERM:

Marco Control Interno Organizacional basado en el riesgo

La Administración del Riesgo Operativo en el Sistema Financiero Cooperativo

Estándares de Control Interno

BASILEA II:
Directrices para el funcionamiento y operación de las Entidades Financieras



MAESTRÍA EN SISTEMAS DE INFORMACIÓN GERENCIAL

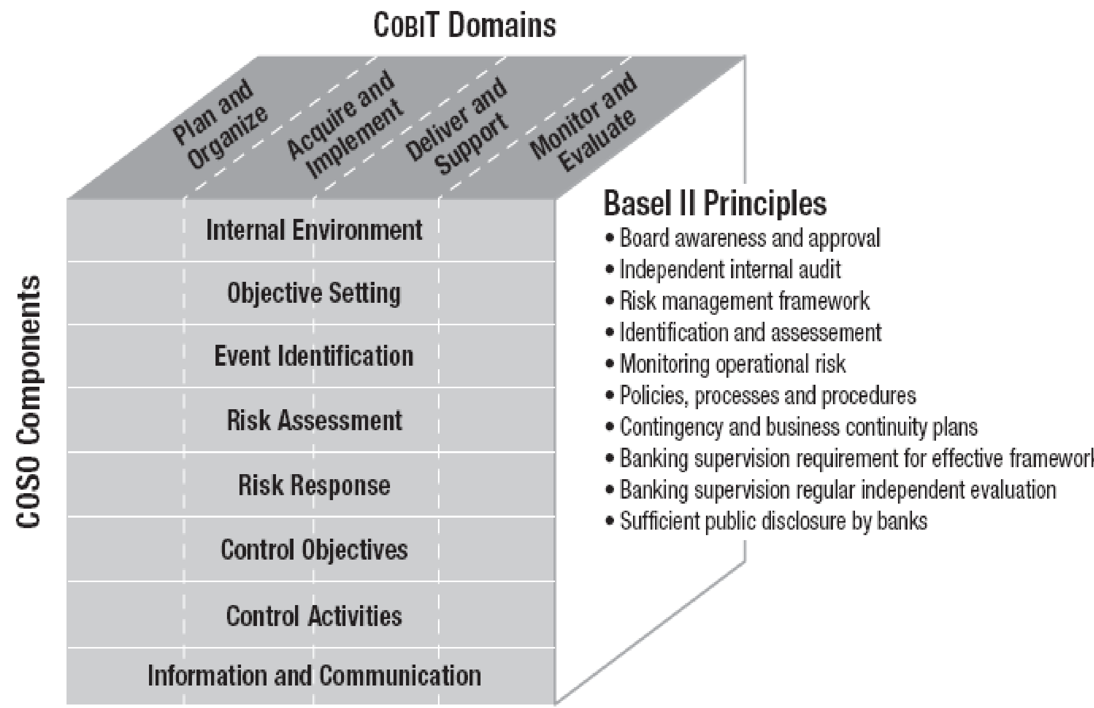
La Administración del Riesgo Operativo en el Sistema Financiero Cooperativo

Estándares de Control Interno

BASILEA II define el riesgo operativo como:

La posibilidad de que se ocasionen pérdidas financieras por eventos derivados de fallas o insuficiencias en los procesos, personas, tecnología de información y por eventos externos

IT controls should consider the overall governance framework to support the quality and integrity of information.



Competency in all eight layers of COSO's framework is necessary to achieve an integrated control framework.

Estándares de Control Interno

La Norma 834 (Emitida por la SBS el 20 de Octubre del 2005):

En la norma 834 de Riesgo Operativo se establecieron los lineamientos mínimos que deben seguir las entidades financieras para garantizar la continuidad del negocio frente a posibles riesgos a los que pudiera estar expuesta la entidad. Para ello, establece que se deben administrar en forma apropiada los procesos, personas, tecnología de información y los eventos externos.

Estándares de Control Interno

La Norma 834:

* Se requiere complementar la administración del Riesgo Legal

La Administración del Riesgo Operativo en el Sistema Financiero Cooperativo

La Administración del riesgo Operativo en las COAC's

- La SBS emprendió una campaña masiva de capacitación y difusión
- En el mes de Julio del 2009 emprendieron una revisión de monitoreo.
- Dificultades para la implementación del riesgo operativo: Falta de recursos financieros, tecnológicos y de personas.
- Resistencia al cambio o poco entendimiento de los beneficios de implementación
- Necesidad de que los sistemas de información incorporen mejores mecanismos de seguridad y sean flexibles para la incorporación de los lineamientos de la administración del riesgo operativo.

La Administración del Riesgo Operativo en el Sistema Financiero Cooperativo

La Administración del riesgo Operativo en las COAC's

- El Consejo de Administración y los diferentes comités de apoyo administrativo tienen una alta responsabilidad en la administración del riesgo operativo.

- Responsabilidades del Comité de Riesgos.

- Mayor enfoque de auditoria orientado hacia el riesgo de Auditores Externos y Calificadoras de Riesgo.

- Pilares para la gestión del riesgo en las COAC's: Gobierno Corporativo, Administración del Riesgo y Cumplimiento.

La Administración del Riesgo Operativo en el Sistema Financiero Cooperativo

La Administración del riesgo Operativo en las COAC's

En general, para una adecuada gestión de riesgos es necesario que se cumplan con los siguientes lineamientos:

- ❖ Establecer un adecuado ambiente de administración de Riesgos.
- ❖ Realizar una gestión proactiva de los riesgos.
- ❖ Asumir e implementar las observaciones y recomendaciones de las entidades de control.
- ❖ Transparencia de la información financiera y de la gestión de riesgos realizada.

La Administración del Riesgo Operativo en el Sistema Financiero Cooperativo

La Administración del riesgo Operativo en las COAC's

En general, para una adecuada gestión de riesgos es necesario que se cumplan con los siguientes lineamientos:

- Establecer un adecuado ambiente de administración de Riesgos.
- Realizar una gestión proactiva de los riesgos.
- Asumir e implementar las observaciones y recomendaciones de las entidades de control.
- Transparencia de la información financiera y de la gestión de riesgos realizada.

El rol de la Unidad de Riesgos

El rol de Auditoria Interna

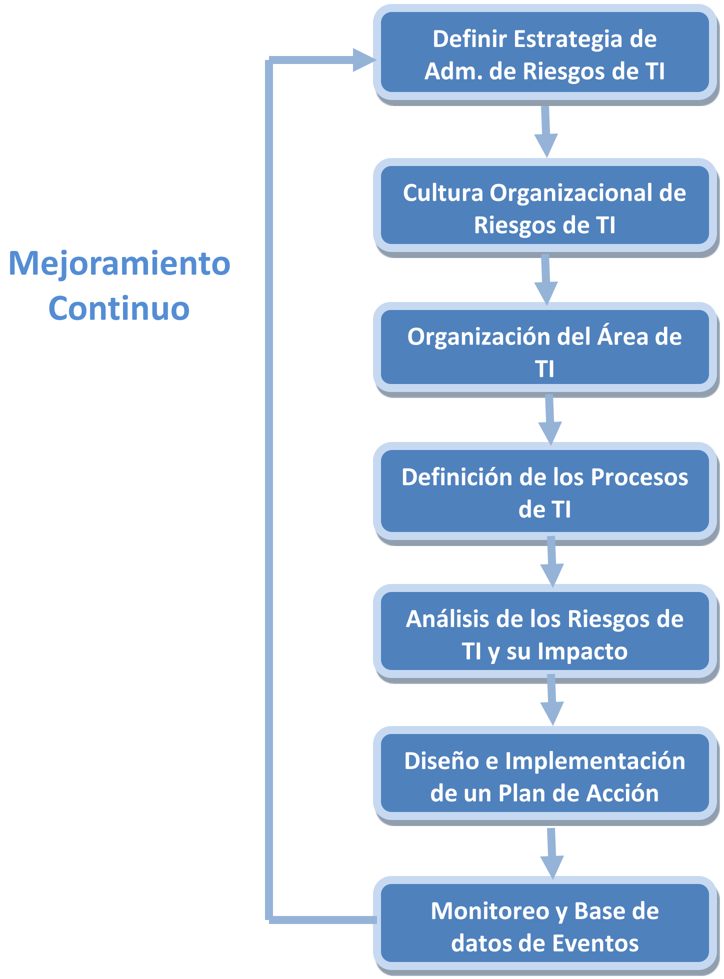
Marco de Control para la Administración del Riesgo Tecnológico

Lineamientos para la Administración del Riesgo Tecnológico

1. Definir una estrategia corporativa para administrar el riesgo tecnológico:
2. Crear una Cultura Organizacional enfocada al Riesgo Tecnológico:
3. Organización del Área de TI
4. Definición de los procesos de TI
5. Analizar y evaluar los riesgos de tecnología y su impacto sobre el negocio
6. Diseñar e Implementar un Plan de Acción continuo
7. Monitorear y alimentar una base de datos de Eventos:
8. Mejoramiento continuo

Marco de Control para la Administración del Riesgo Tecnológico

Lineamientos para la Administración del Riesgo Tecnológico



Marco de Control para la Administración del Riesgo Tecnológico

Planificación y Administración de la Tecnología de Información

- Evaluación de Riesgos de TI
- Planificación estratégica de Tecnología de Información alineado con la planificación estratégica del negocio
- Políticas y procedimientos inherentes al proceso de planeación estratégica
- Plan Operativo Anual de Tecnología de Información
- Presupuesto de TI
- Estructura Orgánico Funcional de TI
- Conformación de un Comité de Informática
- Actas de Aprobación del Plan estratégico, Plan Anual y Presupuesto por parte del Consejo de Administración

Marco de Control para la Administración del Riesgo Tecnológico

Planificación y Administración de la Tecnología de Información

- Manual de Políticas y procedimientos de TI aprobado y difundido.
- Plan de capacitación del personal de TI y plan de capacitación de Usuarios
- Políticas y procedimientos para la evaluación del personal de TI y la evaluación de la efectividad de los planes de capacitación. Código de Ética y Acuerdos de confidencialidad del personal
- Control e inventario de Activos de TI
- Políticas y procedimientos de adquisición de recursos de tecnología de información de acuerdo a la planificación estratégica
- Disponer de documentación técnica detallada de la infraestructura tecnológica

Marco de Control para la Administración del Riesgo Tecnológico

La Seguridad de la Información y la Alta disponibilidad

- Clasificar la Información
- Definir los roles de Propietario de la Información y de Jefe de Seguridad Informática
- Diseñar e implementar políticas y procedimientos de seguridad de la información aprobadas y difundidas formalmente. **La Política de Seguridad**
- Implementación de controles para minimizar el impacto de las vulnerabilidades e incidentes de seguridad
- Implementación de un sistema de Gestión de seguridad de la información
- Establecer políticas y procedimientos de control de acceso a la información y los recursos de TI.
- Definir los responsables de definir, implementar y controlar la gestión de seguridad de la información

Marco de Control para la Administración del Riesgo Tecnológico

La Seguridad de la Información y la Alta disponibilidad

- Evaluar el SGSI en forma periódica y promover su actualización y mejora continua
- Implementar mecanismos de protección y condiciones físicas y ambientales para el óptimo funcionamiento de los recursos de TI
- Gestión apropiada del personal de TI: selección, incorporación, evaluación y salida. Perfiles definidos e inducción al cargo.
- Adecuados controles lógicos para el acceso a los recursos de TI.

El Plan de Continuidad del Negocio:

- Evaluar y medir los riesgos de TI y su impacto en el Negocio
- Definir el objetivo de Punto de recuperación y el Objetivo de Tiempo de recuperación
- Diseñar, implementar y difundir formalmente un Plan de Continuidad del Negocio
- Definir pruebas periódicas del BCP, establecer su efectividad y realizar las mejoras necesarias
- Establecer acciones preventivas, inmediatas y de recuperación, los responsables y los recursos necesarios para el cumplimiento del BCP
- Disponer de un Centro Alterno de Recuperación
- Procedimientos formales de respaldo de la información electrónica y documental; y, de los programas

Marco de Control para la Administración del Riesgo Tecnológico

La Entrega de Servicios y la Calidad de los procesos de TI

La Gestión de Servicios de Tecnología de Información:

- Disponer de políticas y procedimientos para la administración de eventos e incidentes
- Disponer de una Mesa de Ayuda o Help desk para atender los requerimientos de los Usuarios en forma oportuna bajo procedimientos claros y específicos
- Disponer de Acuerdos y niveles de servicio para la atención de requerimientos
- Disponer de Acuerdos de Nivel de Servicio y Acuerdos de Confidencialidad con los proveedores externos
- Políticas y procedimientos para la administración de servicios provistos por terceros
- Disponer de manuales operativos de las operaciones de TI
- Disponer de manuales de configuraciones de los recursos de TI

Marco de Control para la Administración del Riesgo Tecnológico

La Entrega de Servicios y la Calidad de los procesos de TI

Adquisición y mantenimiento de Sistemas de Información:

- Metodología para la administración de proyectos de sistemas de información
- Establecer una metodología formal para la administración del ciclo de vida de los sistemas de información, así como de nuevas adquisiciones y proyectos
- Adecuada segregación de funciones en el desarrollo de aplicaciones y control de versiones
- Separación de las áreas de desarrollo, preproducción y producción
- Adecuadas pruebas y autorización de cambios. Monitoreo de los cambios efectuados
- Adecuada capacitación y entrenamiento de los Usuarios en los cambios efectuados
- Disponer de manuales técnicos y de Usuario debidamente formalizados y actualizados

Marco de Control para la Administración del Riesgo Tecnológico

La Entrega de Servicios y la Calidad de los procesos de TI

Redes y Comunicaciones:

- Administración de las redes y comunicaciones es compleja, requiere de actualización técnica constante.
- Definición del rol de administrador de redes y comunicaciones
- Diseño integral de los servicios de redes y comunicaciones
- Planificación de medidas preventivas y correctivas contra amenazas y para la optimización y calidad de la infraestructura de la red corporativa
- Definir políticas y procedimientos para la administración integral de la red corporativa, lo que incluye su monitoreo y mejoramiento continuo
- Disponer de recursos y servicios de red de alta disponibilidad para garantizar la continuidad y calidad de las redes y comunicaciones de la Entidad

Marco de Control para la Administración del Riesgo Tecnológico

La Entrega de Servicios y la Calidad de los procesos de TI

Redes y Comunicaciones:

- Disponer de proveedores principales y secundarios de los servicios de red
- Implementar herramientas de administración monitoreo proactivos bajo protocolos que garanticen seguridad, control y calidad
- Políticas, procedimientos y mecanismos de protección frente a ataques internos y externos a la red corporativa
- Definir políticas de control de acceso y segregación de redes (VLAN's)
- Restricción de accesos remotos y protección de los mismos (VPN's)
- Estandarización y seguimiento de normas de seguridad para el cableado estructurado y diseño del core de la red
- Controles lógicos, protección perimetral y en profundidad y ethical hacking

Marco de Control para la Administración del Riesgo Tecnológico

Impacto de la Tecnología de Información en la cadena de valor del negocio

- Mejorar y formalizar los procesos
- Capacitar, concientizar y despertar en el personal el apetito hacia el riesgo
- Innovación de la seguridad y protección de uno de los activos mas preciado: la información
- Medición del riesgo y toma de decisiones oportunas basado en su impacto
- Eficiencia e innovación competitiva a través de la optimización y disminución de pérdidas ocasionadas por fraudes o errores operativos
- Comprensión de la alta dirección sobre el rol de TI en la organización y comprensión del área de TI sobre el servicio a sus “clientes”
- Garantizar el servicio continuo, minimizar el riesgo reputacional y mejorar la calidad en el servicio al cliente. Percepción positiva en los clientes

Herramientas para la Administración del Riesgo tecnológico

Existen diferentes herramientas informáticas para garantizar una adecuada gestión del riesgo tecnológico. Algunas de ellas son:

- COBIT ADVISOR
- ACL
- AUTOAUDIT
- Sistemas Internos (Bases de Datos de Eventos)

- Pistas de auditoria: control versus eficiencia
- Segregación de funciones en sistemas de producción

Conclusiones y recomendaciones

Conclusiones

- Las Cooperativas de Ahorro y Crédito en el Ecuador en los últimos años han tenido un crecimiento muy importante a nivel financiero y operacional, lo que se ve reflejado en el aumento de los depósitos a la vista y las operaciones de crédito; convirtiéndose después de los bancos, en el principal subsector financiero del País.

- El uso de la tecnología y los sistemas de información en las Cooperativas de Ahorro y Crédito es un aspecto fundamental dentro de la planificación estratégica, la realización de sus operaciones, el control interno y financiero y el mejoramiento de los productos y servicios ofrecidos a sus clientes.

Conclusiones y recomendaciones

Conclusiones

- El Control Interno es una herramienta fundamental para lograr la eficiencia, eficacia, productividad y el desarrollo operativo y administrativo de las COAC's, bajo un ambiente de prevención de riesgos y proactividad en el logro de los objetivos institucionales.

- Las Cooperativas de Ahorro y Crédito tienen la necesidad de adaptar su gestión hacia una cultura de prevención y administración de los diferentes riesgos a los cuales se enfrenta su giro de negocio; entre los que según el Acuerdo de Basilea se componen en riesgo de mercado, riesgo de liquidez y riesgo operacional.

Conclusiones y recomendaciones

Conclusiones

- La Superintendencia de Bancos y Seguros del Ecuador consciente de la necesidad de que las COAC's incorporen a sus procesos de negocio la administración integral de sus riesgos de acuerdo a los lineamientos del Acuerdo de Basilea, ha emitido un conjunto de resoluciones y normativas orientadas hacia una administración de los riesgos, responsable y eficaz en las Entidades Financieras que se encuentran bajo su control.

- La resolución conocida como 834 emitida por la Superintendencia de Bancos incorpora los lineamientos y mejores prácticas de control interno para la administración del riesgo operacional para las Entidades Financieras del Ecuador e identifica 4 aspectos de la administración del riesgo operacional que deben ser administrados en forma adecuada: los procesos, las personas, la tecnología de información y los eventos externos.

Conclusiones y recomendaciones

Conclusiones

- La administración del riesgo tecnológico es un aspecto fundamental dentro de la gestión de riesgo operativo y es una de las responsabilidades y desafíos más importantes a las cuales se enfrentan las COAC's en el Ecuador, debido a que involucra el uso de recursos organizacionales, humanos, financieros y tecnológicos.

- Existen en la actualidad una serie de lineamientos, estándares y mejores prácticas para una efectiva administración del riesgo, la entrega de servicios y la seguridad relacionada con la tecnología de información, entre los que se encuentran: COBIT, ISO 27001, ITIL, entre otros.

Conclusiones y recomendaciones

Conclusiones

- Es posible dentro de las COAC's crear un marco de control integral para la administración del riesgo tecnológico, basado en las directrices de COSO-ERM, ISO 27001, COBIT y la Resolución 834 que garantice la seguridad de la información, la salvaguarda de los recursos tecnológicos y la continuidad del negocio.

- El rol de auditoría ha evolucionado en los últimos años de tal forma que se ha convertido en un factor importante dentro de la evaluación del riesgo tecnológico y en la mejora continua de los procesos de TI, a través del uso de herramientas tecnológicas para el análisis de las operaciones, la evaluación de riesgos y la planificación de la auditoría.

MAESTRÍA EN SISTEMAS DE INFORMACIÓN GERENCIAL

Conclusiones y recomendaciones

Recomendaciones

- Las Cooperativas de Ahorro y Crédito deben estar conscientes sobre la necesidad de incorporar a sus procesos de negocio la administración del riesgo operacional y del control interno como una oportunidad para lograr los objetivos institucionales; agregar valor a sus líneas de negocio y estructuras organizacionales; alcanzar una ventaja competitiva frente a la competencia; y, garantizar en forma sustentable su desarrollo administrativo, operativo, financiero y tecnológico.

- Las Cooperativas de Ahorro y Crédito a través de los diferentes marcos de referencia, como COBIT, ITIL, ISO 27000 y la Norma 834, deben adaptar sus lineamientos, políticas y procedimientos de control interno hacia la administración y continuidad de sus procesos de Tecnología de Información, ya que estos últimos, son la base fundamental sobre la que se desarrollan sus operaciones y cuya interrupción pueden generar pérdidas importantes a nivel financiero y reputacional.

Conclusiones y recomendaciones

Recomendaciones

- La Administración del riesgo tecnológico permitirá a las COAC's hacer frente a diversos eventos y escenarios de riesgo que pudieran poner en peligro la continuidad operativa del negocio; y para ello, es necesaria la participación de toda la organización y el apoyo fundamental de la Gerencia General en la definición y formalización de las políticas de seguridad y en la implementación de un adecuado control interno de la tecnología de información.

- En el mercado están disponibles diversas herramientas informáticas para la administración del riesgo tecnológico basado en los estándares y mejores prácticas que pueden ser utilizados por los responsables de definir, implementar y controlar el riesgo tecnológico en las COAC's.