ISACA®
Al servicio de los profesionales encargados de la gobernabilidad de la tecnología de la información
Mexico City Chapter

Modelo de Control para la Administración de Riesgos de TI

MsC. Carlos Zamora Sotelo, CISA, CISM

ISACA®
Al servicio de los profesionales encargados de la gobernabilidad de la tecnología de la información
Mexico City Chapter

Agenda

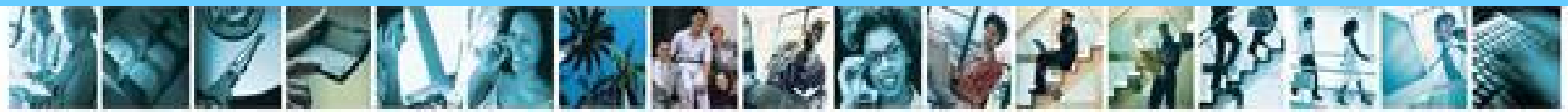
1. Objetivo de la Sesión.
2. La Administración de Riesgos en la Estrategia de Negocios.
3. El papel de la administración de riesgos de Tecnología de Información como parte de la estrategia de la Gestión del Riesgo en la Organización.
4. Elementos que deben conformar un modelo de administración de Riesgos de TI.
5. Modelo o marco de trabajo para realizar un modelo de Administración y control de Riesgos de TI.

Agenda

5. Premisas para la realización de un proceso de análisis y evaluación de riesgos desde el punto de vista de un modelo de control.
6. Marco metodológico sugerido para desarrollar un modelo de control interno en Tecnología en materia de Administración de Riesgos.
7. Cómo justificar el desarrollo y aplicación de un modelo de control para la gestión de riesgos de Tecnología.
8. Requerimientos y Factores críticos de éxito para el logro de objetivos del modelo de gestión de riesgos.
9. Análisis de un caso de estudio.

Agenda

10. Conclusiones del Caso de Estudio
11. Respuestas a las Preguntas más frecuentes



Objetivo de la Sesión

- Establecer el modelo de Control de Tecnología de Información para la Identificación, Análisis, Evaluación, Disminución de Riesgos de Tecnología de Información.
- Contar con métricas e indicadores de riesgos típicos de un área de Tecnología de Información.
- Conocer una estrategia real de aplicación de un modelo de control para la administración de Riesgos de Tecnología de Información.

Proceso de Administración de Riesgos de T.I.

Análisis y Evaluación

Mitigación Aceptación

Implementar Medidas de Control

Evaluación y Seguimiento

Activos de la Organización

Procesos

Información

Comunicaciones

Operaciones de Cómputo

Infraestructura HW, SW, DBMS, Red

Sistemas Operativos

Sistemas Aplicativos

Proyectos

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la tecnología de la información
Mexico City Chapter

La Administración de Riesgos en la Estrategia del Negocio

Reducir y Controlar

Gobierno Corporativo & Gobierno de TI

Optimizar

Riesgo Negocio/ Financiero

ESTRATEGIA

- Generar Costos Competitivos
- Maximizar Productividad de las áreas
- Maximizar Creación de Valor
- Aumentar Retorno

- *Inversión*
- *Rentabilidad*
- *Transparencia*

Riesgo Operativo / Funcional

PROCESOS

- Aumentar Formalización y Control Interno
- Incrementar Manejo de Calidad
- Optimizar Procesos Críticos y de Soporte
- Alinear Estrategias por área
- Mayor Flexibilidad, Robustez en la Cadena de Valor

- *Desempeño*
- *Seguimiento*
- *Confiabilidad*

Riesgo Tecnológico

MODELO TECNOLÓGICO/INFORMACIÓN

- Estandarizar Plataformas y Arquitecturas
- Integrar Metodologías y Estándares
- Asegurar Niveles de Servicio
- Adecuar Tecnologías Emergentes
- Incrementar Seguridad

- *Innovación*
- *Flexibilidad*
- *Disponibilidad*

Modelo Integral de Administración de Riesgos

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la tecnología de la información
Mexico City Chapter

La Administración de Riesgos en la Estrategia del Negocio

PROCESOS CRÍTICOS DEL NEGOCIO

ECPF | Estado de Resultados | EVCC | Notas | otros

Procesos de Negocio / Tipos de Transacciones

Proceso A | Proceso B | Proceso C

SISTEMAS APLICATIVOS CRÍTICOS DE NEGOCIO

Aplicación A | Aplicación B | Aplicación C

Control de Aplicaciones
- Totalidad
- Exactitud
- Validez
- Autorización
- Segregación de Funciones

Controles Generales de TI
- Desarrollo de Programas
- Cambios de Programas
- Operación de Computadoras
- Acceso a Programas y Datos
- Ambiente de Control

Servicios de Infraestructura de TI

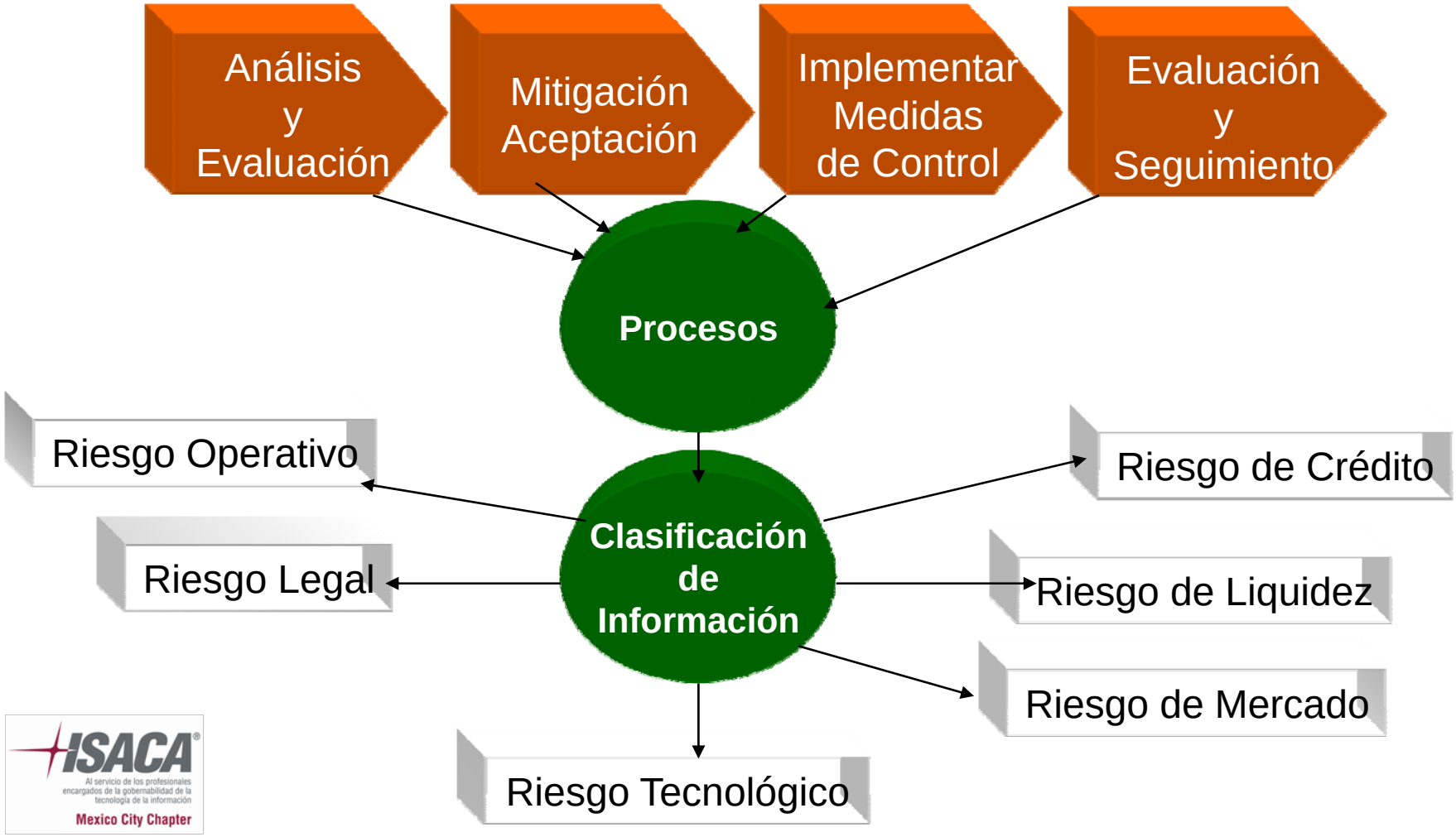
Base de Datos

Sistemas Operativos

Red

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la tecnología de la información
Mexico City Chapter

EL PAPEL DE LA ADMINISTRACIÓN DE RIESGOS DE TECNOLOGÍA DE INFORMACIÓN EN LA GESTIÓN DE RIESGOS EN LA ORGANIZACIÓN



ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la tecnología de la información
Mexico City Chapter

ELEMENTOS QUE CONFORMAN UN MODELO DE GESTIÓN DE RIESGOS DE T.I.

Análisis y Evaluación

Mitigación Aceptación

Implementar Medidas de Control

Evaluación y Seguimiento

Clasificación de Información

Proyectos

Comunicaciones

Riesgo de Tecnología de Información

Sistemas Aplicativos

Operaciones de Cómputo

Infraestructura HW, SW, DBMS, Red

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la tecnología de la información
Mexico City Chapter

Proceso de Administración de Riesgos de T.I.

Análisis y Evaluación

- Análisis de Procesos
- Clasificación de Activos
- Identificar Amenazas
- Identificar Vulnerabilidades
- Identificar Ocurrencias
- Identificar Impacto
- Calificar Cualitativamente
- Calificar Cuantitativamente

Toma de Decisiones

- Análisis Costo/Beneficio
- Determinar Acción vs. Riesgo
- Establecer Estrategia de Control
- Identificar Políticas y Proc.
- Identificar Estándares
- Id. Técnicas y Metodologías
- Establecer Indicadores
- Establecer Límites

Implementar Medidas de Control

- Definir Funciones
- Implementar Políticas
- Implementar Procedimientos
- Inst. Mecanismos de Monitoreo y Control
- Definir respuestas a Incidentes
- Comunicar y Educar

Medición y Seguimiento

- Establecer Base de Datos Histórica
- Evaluación del Proceso
- Verificar Procs. de Monitoreo y Control
- Revisión a los Datos y Registros
- Evaluación de Seguridad
- Auditoría Interna
- Auditoría Externa

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la tecnología de la información
Mexico City Chapter

Marco de Trabajo para el modelo de Administración de Riesgos de T.I.

MEDIDAS DE PREVENCIÓN

- Segregación de Funciones
- Control de cambios
- Administración de identidades y accesos basados en roles
- Diseño y control de la Arquitectura Tecnológica
- Seguridad en la operación de sistemas de información
- Administración de la Seguridad en los Sistemas
- Operación de la Seguridad de la Red
- Administración de la Seguridad de la Red
- Medidas de respaldo
- Negociación de contratos con terceros
- Establecimiento y administración de Niveles de Servicio

MEDIDAS DE DETECCIÓN

- Administración y respuestas ante la identificación de accesos
- Integridad de procesamiento y datos
- Monitoreo de Accesos
- Generación de reportes de control de Accesos
- Identificación y respuesta ante Fraudes

MEDIDAS DE RESPUESTA

- Re-establecimiento de los servicios de Tecnología
- Planes de recuperación y continuidad de negocio

CUMPLIMIENTO

- Políticas, Procedimientos y estándares
- Monitoreo de regulaciones y alineamiento de procesos de conformidad con la normatividad
- Implementación de informes de cumplimiento hacia la autoridad

GOBIERNO (IT GOVERNANCE)

- Generación, implantación y medición de métricas de desempeño
- Alineamiento y soporte entre los riesgos de negocio y los riesgos tecnológicos

Aplicación de los Factores de Riesgo

	Riesgos para:		
PREVENCION	**C**	**I**	**A**
Segregación de Puestos			
Control de Cambios			
Administración de identidades y accesos basados en roles			
Diseño y Control de Arquitectura Tecnológica			
Operación de la Seguridad de Sistemas			
Administración de Seguridad de Sistemas de Inf.			
Operaciones de Seguridad de la Red			
Administración de Seguridad de la Red			
Controles de Respaldo y Recuperación de Operaciones			
Negociación de contratos con Terceros			
Administración y Monitoreo de Niveles de Servicio			
Control Technology R&D			
Detección			
Identificación de Incidentes y respuestas ante los mismos			

C= Comunicaciones, I= Infraestructura, A= Aplicaciones

Análisis y Evaluación

Análisis de Procesos

Proceso de Administración de Riesgos de T.I.

MODELO DE PROCESOS DE UNA COMPAÑÍA DE SEGUROS

PROMOCIÓN Y Comercialización	EVALUACIÓN TÉCNICA	EMISIÓN	ATENCIÓN DE SINIESTROS
Contacto con el cliente	Recepción de Solicitud	Recibe Autorización de Áreas Técnicas	Recepción de Reporte de Siniestro
Solicitud de Documentación	Análisis Técnico De Aceptación de Riesgos	Suscripción De Riesgos	Atención del Siniestro
Evaluación De la documentación	Elaboración de Reporte Técnico	Entrega de Poliza	Evaluación del Siniestro
Cotización	Análisis de Reaseguro		Dictamen del Siniestro
	Autorización de Emisión		Pago del Siniestro
			Aceptación de Finiquito

SOPORTE DE SISTEMAS	ADMON DE RECURSOS HUMANOS	SERVICIOS GENERALES	AUDITORÍA INTERNA	ADMON Y FINANZAS
ADMON DE RIESGOS	SOPORTE CUENTAS ESPECIALES			

Objetivo:

Administrar los riesgos propios de la Compañía y de sus clientes, a través de la evaluación Técnica, emisión y atención de siniestros, asesorando, controlando y manteniendo de manera eficiente la posición financiera y contable de los recursos y activos de Compañía

Entradas:

- Solicitud de producto y servicios de administración de riesgos sobre activos de terceros.
- Documentación requerida para registro de alta, baja o modificación de datos de clientes y sus activos.
- Instrucciones de operación (aceptación, reaseguro y atención de siniestros) de los riesgos de suo de sus clientes
- Solicitud de Transferencia de Riesgos a través de traslado de servicios.
- Ingresos por concepto de Pago de Primas
- Ingresos por concepto recuperaciones
- Ingresos por venta de salvamentos
- Ingresos por Reaseguro
- Ingresos por Venta de Activo Fijo
- Ingresos por Servicios en General
- Ingresos por Administración de las Inversiones

Salidas:

- Contrato de servicios (Póiliza de Seguro)
- Estado de Cuenta de Agentes
- Emisión y renovación de las Polizas emitidas
- Estados Financieros para el consejo de administración.
- Informes y reportes financieros y de operación para entidades gubernamentales y regulatorias
- Pagos a Asegurados por concepto de Siniestros
- Pagos por concepto de Contratación de Productos y Servicios

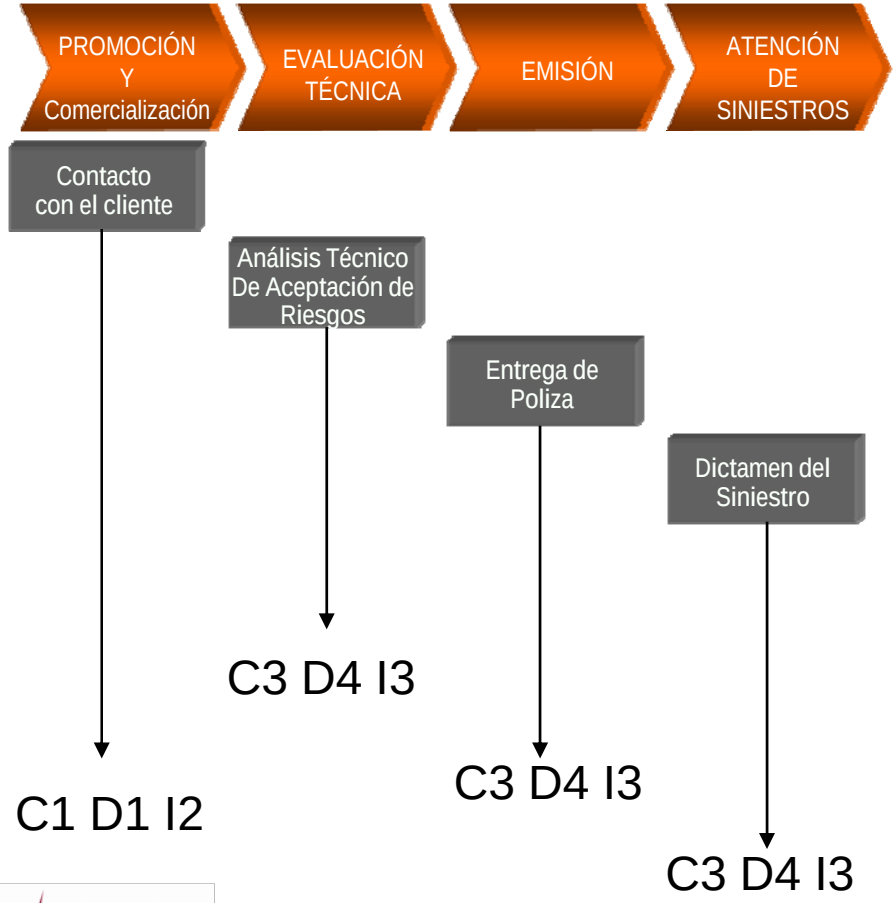
ISACA Mexico City Chapter

Análisis y Evaluación

Clasificación de Los activos

Proceso de Administración de Riesgos de T.I.

CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN



Después de un análisis con el Consejo de Administración y de reuniones con los Dueños de cada uno de los procesos se ha determinado que la información de cada uno de los proceso ha sido clasificada de la siguiente Forma:

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la tecnología de la información
Mexico City Chapter

Análisis y Evaluación

Proceso de Administración de Riesgos de T.I.

Identificar Amenazas

Identificar Vulnerabilidades

Identificar Ocurrencias

Identificar Impacto

Calificar Cualitativamente

PROMOCIÓN Y Comercialización	EVALUACIÓN TÉCNICA	EMISIÓN	ATENCIÓN DE SINIESTROS
Contacto con el cliente	Recepción de Solicitud	Recibe Autorización de Áreas Técnicas	Recepción de Reporte de Siniestro
Solicitud de Documentación	Análisis Técnico De Aceptación de Riesgos	Suscripción De Riesgos	Atención del Siniestro
Evaluación De la documentación	Elaboración de Reporte Técnico	Entrega de Poliza	Evaluación del Siniestro
Cotización	Análisis de Reaseguro		Dictamen del Siniestro
	Autorización de Emisión		Pago del Siniestro
			Aceptación de Finiquito

SOPORTE DE SISTEMAS	ADMON DE RECURSOS HUMANOS	SERVICIOS GENERALES	AUDITORÍA INTERNA	ADMON Y FINANZAS
ADMON DE RIESGOS	SOPORTE CUENTAS ESPECIALES			

Después de un análisis con el Consejo de Administración y de reuniones con los Dueños de cada uno de los procesos el análisis ha determinado que los procesos de acuerdo a la naturaleza de la información y al impacto han sido calificados de la siguiente forma:

BAJO Menor Moderado Alto

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la tecnología de la información
Mexico City Chapter

Proceso de Administración de Riesgos de T.I.

Análisis y Evaluación	Mitigación Aceptación	Implementar Medidas de Control	Evaluación y Seguimiento
Análisis de Procesos	Analisis Costo/Beneficio	Def. Segregación De Funciones	Auto evaluación CSA
Clasificación de Los activos	Determinar Acción Vs Riesgo	Implementar Políticas	Verif. Mecanismos De Monitoreo Cont.
Identificar Amenazas	Establecer Estrategia de Ctrl	Implementar Procedimientos	Revisión a los Datos y Registros
Identificar Vulnerabilidades	Identificar Políticas y Proced.	Inst. Mecanismos De Monitoreo Cont.	Evaluación de Seguridad
Identificar Ocurrencias	Identificar Estándares	Def. Respuestas a Incidentes	Auditoría Interna
Identificar Impacto	Id. Técnicas y Metodologías	Comunicar y Educar	Auditoría Externa
Calificar Cualitativamente			
Calificar Cuantitativamente			

ISACA
Mexico City Chapter

Proceso de Administración de Riesgos de T.I.

Análisis y Evaluación

- Análisis de Procesos
- Clasificación de Los activos
- Identificar Amenazas
- Identificar Vulnerabilidades
- Identificar Ocurrencias
- Identificar Impacto
- Calificar Cualitativamente
- Calificar Cuantitativamente

Equipo de Trabajo

- Dueño del Activo o Custodio
- Administrador de Riesgos
- Responsable de la Seguridad
- Auditor
- Usuarios

ISAC
Al servicio de los p
encargados de la gobern
tecnología de la
Mexico City Ch

Premisas para la Realización de un Proceso de Análisis de Riesgos

- Análisis y Evaluación
- Análisis de Procesos
- Clasificación de Los activos
- Identificar Amenazas
- Identificar Vulnerabilidades
- Identificar Ocurrencias
- Identificar Impacto
- Calificar Cualitativamente
- Calificar Cuantitativamente

Planeación y Preparación

- Desarrollar un plan de Proyecto & Equipo de Trabajo
- Administrador de Riesgos & Director de Negocio

Actividades de Análisis de Riesgo del Grupo

- Obtener la Información
- Equipo de Trabajo y Otros Expertos Calificados
- Identificar Amenazas — Equipo de Trabajo especializado
- Evaluar activos y Amenazas — Equipo de Trabajo
- Desarrollar escenarios
- Equipo de Trabajo
- Calificar cada escenario
- Equipo de Trabajo
- Identificar Medidas de Mitigación de Riesgos
- Equipo de Trabajo Y Unidad de Negocio

ISAC
Al servicio de los p
encargados de la gobern
tecnología de la
Mexico City Ch

Premisas para la Realización de un Proceso de Análisis de Riesgos

¿ Que variables conforman el proceso de análisis y evaluación de Riesgos ?

¿ Quiénes participan en un análisis y evaluación de Riesgos ?

¿ Qué criterios utilizo para realizar un análisis de Riesgos ?

¿ Con que periodicidad realizo un análisis de Riesgos ?

¿ Qué utilidad práctica tiene un análisis de Riesgos ?

Premisas para la Realización de un Proceso de Análisis de Riesgos

¿ Que variables conforman el proceso de análisis y evaluación de Riesgos ?

- Propietario o Custodio
- Clasificación del Activo
- Determinar las amenazas
- Determinar las Vulnerabilidades
- Determinar el Impacto
- Determinar la Probabiliad de Ocurrencia
- Realizar la Clasificación o Calificación del Riesgo

Premisas para la Realización de un Proceso de Análisis de Riesgos

¿ Quiénes participan en un análisis y evaluación de Riesgos ?

- Propietario o Custodio del Activo
- Especialista en Riesgos (IRM, ORM)
- Abogado del Diablo (Devil’s Advocate)
- Auditoría Interna
- Especialistas Externos (Sólo si aplica)

Premisas para la Realización de un Proceso de Análisis de Riesgos

¿ Qué criterios utilizo para realizar un análisis y evaluación de Riesgos ?

1. La Clasificación del (los) Activos.
2. La Metodología de Análisis de Riesgos.
3. La importancia o relevancia en la operación.
4. Identificar las etapas de análisis y la etapa de Evaluación.

Marco Metodológico sugerido para desarrollar un modelo de Control Interno de Gestión de Riesgos

MARCO NORMATIVO Y LEGAL APLICABLE

- ANALISIS DE LOS PROCESOS CRÍTICOS DEL NEGOCIO
- EVALUACIÓN DE RIESGOS DE NEGOCIO
- EVALUACIÓN DE RIESGOS DE T.I.
- DEFINICIÓN DE POLÍTICAS PROCED, ESTANDARES
- DEFINICIÓN DE METRICAS DE MEDICIÓN TABLERO DE CONTROL
- ESTABLECER TECNICAS DE MONITOREO CONTÍNUO

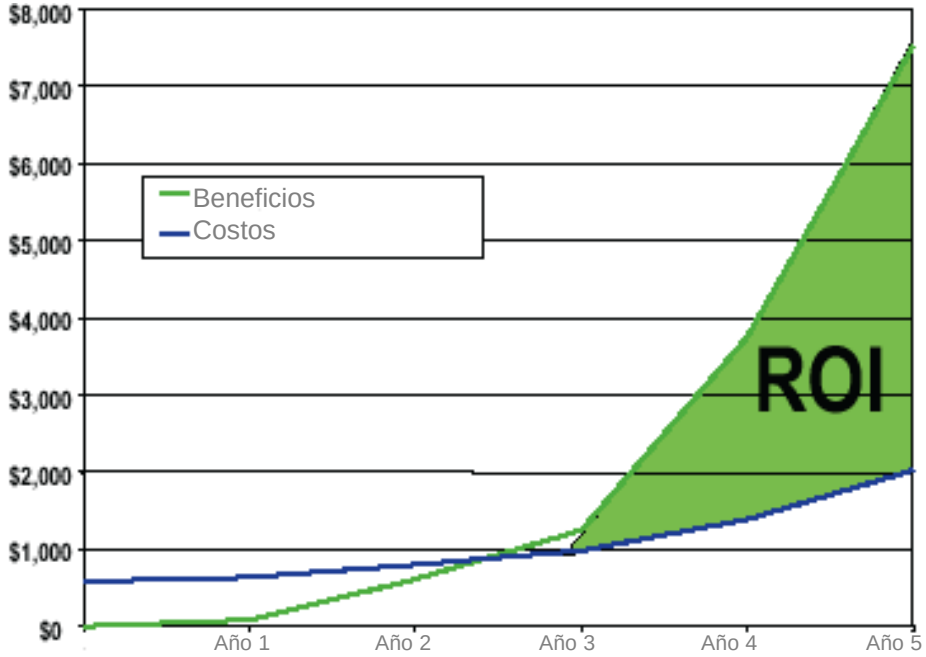
ANALISIS COSTO – BENEFICIO DE CONTROLES VS IMPACTO

VALIDACIÓN Y SOPORTE ESTRATÉGICO A LOS OBJETIVOS DE NEGOCIO

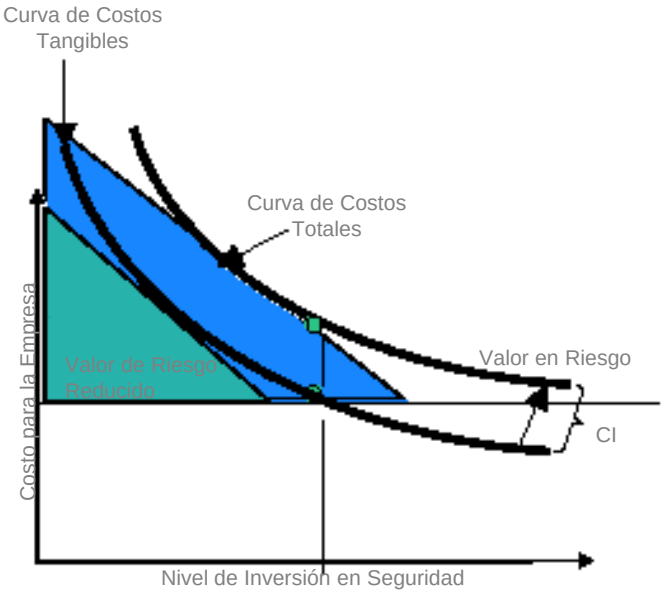
"...Recordar que la Gestión de Riesgos de Tecnología es un Proceso Más en la organización que debe contar con Personal, Técnicas, Metodologías y un Marco Normativo aplicable.."

Justificación del Modelo de Riesgos

ROI Tradicional



Retorno Basado en Riesgos



Justificación del Modelo de Riesgos

- Calcular el valor en riesgo.
- Estimar la ocurrencia de una amenaza.
- Evaluar el costo de propiedad.
- Calcular el valor de la reducción del riesgo.

Justificación del Modelo de Riesgos

1. Identificar los objetivos y procesos de negocio.
2. Identificar los activos (de información y digitales) que los soportan.
3. Estimar el valor de los activos (**VA**) considerando elementos como costo inicial, costo de mantenimiento, valor que representa para la Compañía y/o valor que representa en el mercado para la competencia.
4. Identificar amenazas por activo.
5. Identificar vulnerabilidades y el factor de exposición (**FE**) por activo.
6. Determinar la tasa de ocurrencia anual (**TOA**) de cada vulnerabilidad por activo.
7. Determinar la expectativa de pérdida simple (**EPS**) multiplicando **VA** por **FE** (por amenaza por activo).
8. Determinar la expectativa de pérdida anual (**EPA**) multiplicando la **TOA** por la **EPS** (por amenaza por activo).

Justificación del Modelo de Riesgos

9. Priorizar activos por **EPA**.
10. Diseñar soluciones por activo atendiendo a la priorización realizada y buscando alineamiento a la Política Directriz de Seguridad de la Información.
11. Estimar costo de soluciones considerando necesidades individuales y generales.
12. Comparar costo de soluciones contra la **EPA** de cada activo.
13. Estimar la recuperación de la inversión en función de la reducción de la **EPA** por activo.
14. Priorizar la ejecución de soluciones.
15. Ejecutar plan.
16. Mantenerlo.

Requerimientos y Factores Críticos de Éxito para un Desarrollo del Modelo de Gestión de Riesgos de T.I.

- Desarrollar siempre el modelo considerando los procesos, objetivos y estrategias de la Organización.
- Involucrar siempre a las áreas de negocio, financiera y legal de la organización.
- Tener a la mano estadísticas internas, externas y referencias de la industria respecto a los riesgos de tecnología del sector
- Realizar ejercicios dinámicos para identificar amenazas, vulnerabiliades e impactos a la organización
- Cuantificar el impacto Vs el costo de implementar el modelo de control interno en Tecnología
- Involucrar siempre al área financiera y Auditoría.
- Realizar el análisis de Riesgos considerando siempre escenarios

Requerimientos y Factores Críticos de Éxito para un Desarrollo del Modelo de Gestión de Riesgos de T.I.

- Validar la calificación de riesgo y la cuantificación del riesgo.
- Generar el modelo de políticas, procedimientos, métricas y estándares asociados para mitigar los riesgos
- Desarrollar siempre el marco de monitoreo para la prevención y detección de Riesgos
- Considerar siempre la inversión en capacitación y soporte externo.
- Realizar sesiones de trabajo dinámicas para obtener mejores resultados.

Proceso de Administración de Riesgos de T.I.

Análisis y Evaluación de Riesgos

- **Análisis de Procesos**
- **Clasificación de Los activos**
- **Identificar Amenazas**
- **Identificar Vulnerabilidades**
- **Identificar Ocurrencias**
- **Identificar Impacto**
- **Calificar Cualitativamente**
- **Calificar Cuantitativamente**

Es un requerimiento y a la vez un factor Crítico de Éxito para los siguientes Procesos:

- Desarrollo de una Estrategia y Programa de Seguridad
- Estudio de Factibilidad Análisis Costo-Beneficio ROI T.I.
- Planeación y Administración de La Capacidad
- Administración de Proyectos
- Auditoría

ISAC
Al servicio de los p
encargados de la gobern
tecnología de la
Mexico City Ch

Requerimientos y Factores Críticos de éxito para el logro de Objetivos de un modelo de Gestión de Riesgos

Mitigación
Aceptación

- Analisis Costo/Beneficio
- Determinar Acción Vs Riesgo
- Establecer Estrategia de Ctrl
- Identificar Políticas y Proced.
- Identificar Estándares
- Id. Técnicas y Metodologías

- Políticas y Procedimientos de Operación de T.I.
- Políticas y Procedimientos de Administración
- Políticas y Procedimientos de Desarrollo, Mantenimiento y Soporte
- Políticas y Procedimientos de Seguridad
- Estándares de Tecnología

- ITIL
- CoBIT
- CMM
- ISO 17799

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la tecnología de la información
Mexico City Chapter

Políticas y Procedimientos de Operación y Administración de T.I.

Mitigación
Aceptación

- **Analisis Costo/Beneficio**
- **Determinar Acción Vs Riesgo**
- **Establecer Estrategia de Ctrl**
- **Identificar Políticas y Proced.**
- **Identificar Estándares**
- **Id. Técnicas y Metodologías**

Desarrollo de Sistemas
Compatibiliad e Interoperabilidad
Capacitación al Personal de Sistemas
Capacitación al los Usuarios
Perfiles de Software Institucional
Intercambio Electrónico de Datos
Evaluación de Proyectos
Atención de Usuarios
Desempeño del Personal
Uso y aprovechamiento del Software y Hardware Institucional
Evaluación periódica de la función Informática (Autoevaluación de Control Interno)

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la tecnología de la información
Mexico City Chapter

Políticas y Procedimientos de Operación y Administración de T.I.

Mitigación
Aceptación

- Analisis Costo/Beneficio
- Determinar Acción Vs Riesgo
- Establecer Estrategia de Ctrl
- Identificar Políticas y Proced.
- Identificar Estándares
- Id. Técnicas y Metodologías

- **Diseño y operación de redes**
- **Instalación y explotación de servicios de información financiera**
- **Explotación y administración de servicios de voz**
- **Administración de Bases de Datos**
- **Evaluación y Seguimiento de aplicaciones**
- **Administración y manejo de errores**
- **Implementación y liberación de requerimientos**
- **Políticas a seguir antes y durante el proceso de auditoría.**
- **Administración Financiera de Sistemas**
- **Manejo y contratación de servicios de proveedores o consultores externos**
- **Elaboración, autorización y seguimiento del presupuesto de sistemas**
- **Políticas para creación y seguimiento de comités**
- **Atención de usuarios a través del Help-Desk**
- **Evaluación de Riesgos**

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la tecnología de la información
Mexico City Chapter

Políticas y Procedimientos de Operación y Administración de T.I.

- **Justificación de Proyectos**
- **Administración de Proyectos**
- **Niveles de Servicio e Indicadores de Desempeño**
- **Organización y Administración de Personal de Sistemas**
- **Planeación Estratégica de Sistemas**
- **Dirección Tecnológica**
- **Administración y control de cambios**
- **Administración de operaciones**
- **Administración de Instalaciones**
- **Administración de Problemas e incidentes**
- **Administración de Datos e Información**
- **Evaluación y seguimiento de procesos del área de informática**
- **Autoevaluación de Control Interno**

Mitigación
Aceptación

- **Analisis Costo/Beneficio**
- **Determinar Acción Vs Riesgo**
- **Establecer Estrategia de Ctrl**
- **Identificar Políticas y Proced.**
- **Identificar Estándares**
- **Id. Técnicas y Metodologías**

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la tecnología de la información
Mexico City Chapter

Políticas y Procedimientos de Seguridad de T.I.

Mitigación
Aceptación

- Analisis Costo/Beneficio
- Determinar Acción Vs Riesgo
- Establecer Estrategia de Ctrl
- Identificar Políticas y Proced.
- Identificar Estándares
- Id. Técnicas y Metodologías

- Administración y Control de Activos Informáticos
- Autenticación y Control de Accesos
- Respaldo y Restauración de Información
- Administración de la Continuidad de Negocio
- Manejo y Administración de Equipos de Cómputo
- Clasificación de Datos y Activos
- Separación y Desechos de Equipo, Dispositivos y Medios de Respaldo
- Comercio Electrónico
- Encripción de Información
- Cómputo de Usuario Final
- Conexiones Externas

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la tecnología de la información
Mexico City Chapter

Políticas y Procedimientos de Seguridad de T.I.

- Instalación, Configuración y Mantenimiento de Firewalls
- Evaluación de Riesgos
- Administración de Riesgos de Información
- Monitoreo de Operaciones
- Monitoreo de Transacciones
- Redes y Telecomunicaciones
- Equipo Portable (Laptops)
- Reporte de Incidentes de Seguridad
- Licenciamiento de Software
- Liberación y Puesta en Producción de Sistemas

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la tecnología de la información
Mexico City Chapter

Estándares de Seguridad de T.I.

- Antivirus
- Auditoría y Registro de Transacciones
- Autenticación mediante Tokens
- Cómputo de Usuario Final
- Arquitectura de Hardware, Software y Comunicaciones
- Programación y Mantenimiento de Sistemas
- Administración de Contraseñas
- Estándares de Seguridad en el Desarrollo y Mantenimiento de Sistemas
- Administración de Cuentas de Usuario

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la tecnología de la información
Mexico City Chapter

- Implementar Medidas de Control
  - **Def. Segregación De Funciones**
  - **Implementar Políticas**
  - **Implementar Procedimientos**
  - **Inst. Mecanismos De Monitoreo Cont.**
  - **Def. Respuestas a Incidentes**
  - **Comunicar y Educar**

Roles y Responsabilidades

- Director de Tecnología
- Gerencia Desarrollo y Mantenimiento
- Gerencia Soporte Técnico
- Bases de Datos
- Redes y Telecom.
- Atención a Usuarios
- Administrador De Librerias
- Operador del Centro de Datos
- Grupo de Control De Versiones
- Analistas
- Programadores

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la tecnología de la información
Mexico City Chapter

Administración de Riesgos de T.I.

Preguntas más Frecuentes

1. ¿Qué es la Gestión de Riesgos de T.I?
2. ¿Para que Sirve la Gestión de Riesgos de T.I.?
3. ¿Cuáles son los Beneficios de implantar este Proceso?
4. ¿Qué se requiere?

¿Qué es la Gestión de Riesgos de T.I.?

Es el proceso mediante el cual se van a establecer los mecanismos que le van a permitir a la empresa a disminuir y controlar los riesgos sobre los equipos, sistemas e ***INFORMACIÓN*** de la organización, es decir, es un mecanismo *DE PREVENCIÓN DE PERDIDAS.*

¿Para que le sirve a la *Compañía?*

Prevenir y/o en su caso Detectar:

- **Fraudes**
- **Pérdida de Información**
- **Violaciones a Leyes y Reglamentos**
- **Pérdida de Clientes**
- **Fracasos de Proyectos**
- **Oportunidad de Negocio**
- **Errores de Operación → Pérdidas/Costos**
- **Pérdida de Activos, entre otras.**
- **Sabotaje**

Beneficios

- Otorga *certidumbre* a los proyectos de inversión
- Reducción de Riesgo Operativo = aumento en la *confianza* de nuestros clientes
- Contribuye a *maximizar los beneficios* de la inversión en Tecnología.
- *Detección oportuna* de amenazas
- Contribuye a establecer un *ORDEN* en la empresa
- Detección de *Oportunidades de Mejora* en los procesos y sistemas de la organización
- *Cumplir con regulaciones* internas y externas
- Incide en la reducción del *TCO*

Requerimientos

- Requerimos ***SU APOYO Y DISPOSICIÓN*** Incondicionales (De la Dirección)
- ***Involucramiento*** de la Alta Gerencia
- Conformación/Creación de un ***Equipo de Trabajo*** Multidisciplinario
- ***Capacitación*** y desarrollo de un programa de ***conscientización*** y difusión
- ***Presupuesto*** para el desarrollo del Proyecto
- Este es un proyecto de largo Plazo por lo tanto su desarrollo e implantación es mayor a 18 meses

¿Preguntas?

ISACA®
Al servicio de los profesionales encargados de la gobernabilidad de la tecnología de la información
Mexico City Chapter

¡Gracias!

MsC. Carlos Zamora Sotelo, CISA, CISM

czamora@conseti.com

czamora@isaca.org.mx

ISACA®
Al servicio de los profesionales encargados de la gobernabilidad de la tecnología de la información
Mexico City Chapter