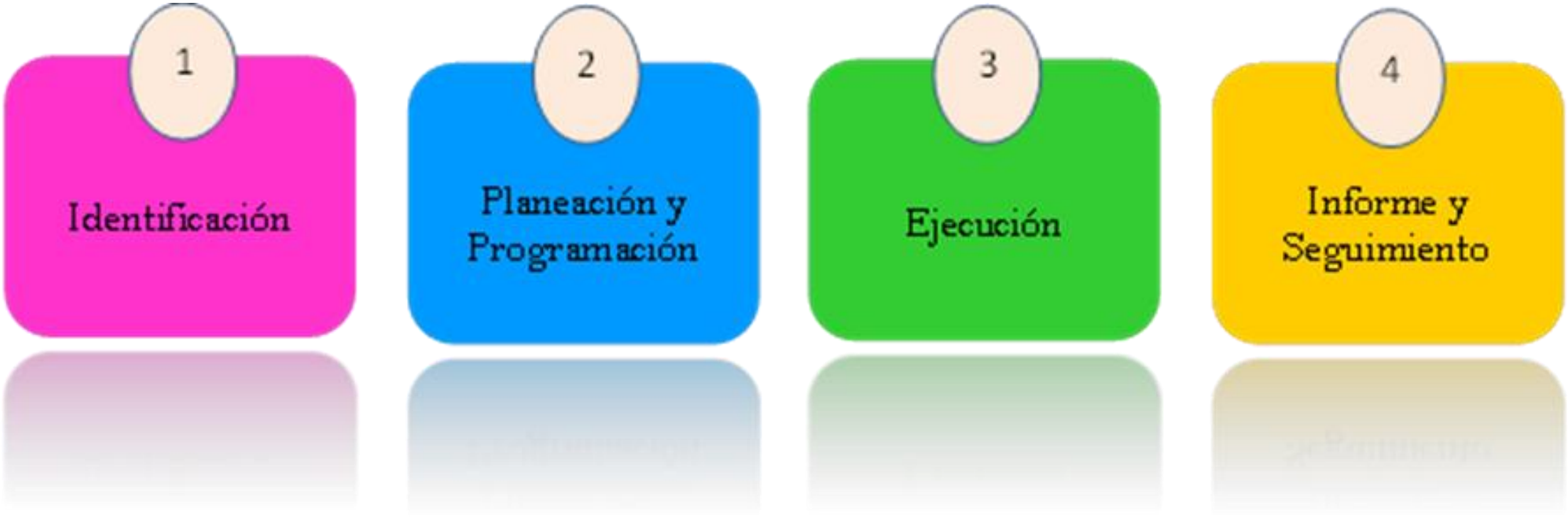
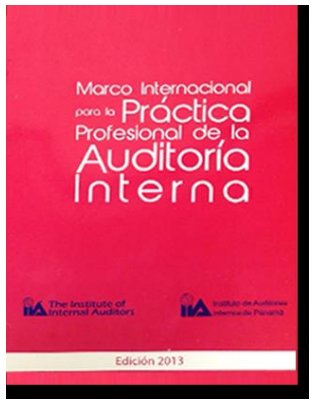
Proceso de Auditoria de Sistemas de Información



Inga. Evelyn Lobos Barrera -M.A., CISA

QUE ES AUDITORIA ?

ASPECTOS IMPORTANTES A CONSIDERAR…



Marco Internacional para la práctica Profesional IIA

ISACA es el acrónimo de Information Systems Audit and Control Association (Asociación de Auditoría y Control de Sistemas de Información).

ISACA®
Trust in, and value from, information systems
Guatemala City Chapter

AUDITORÍA INTERNA

La Auditoría interna es una actividad **independiente y objetiva** de **aseguramiento y consulta,** concebida **para agregar valor** y mejorar las operaciones de una organización. Ayuda a una organización a **cumplir sus objetivos** aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno.

ELEMENTOS CLAVES DE LA DEFINICIÓN. LA AUDITORÍA INTERNA

1) Es independiente y objetiva.
2) Se dedica a actividades de aseguramiento y consultoría.
3) Agrega valor y mejora las operaciones.
4) Tiene un enfoque sistemático y disciplinado.
5) Evalúa la gestión de riesgos, el control y el gobierno.

FUNCIÓN DE AUDITORIA DE SI

ROLES DE LA AUDITORÍA INTERNA

NORMA DE DESEMPEÑO 2100- NATURALEZA DEL TRABAJO.

La actividad de auditoria interna debe evaluar y contribuir a la mejora de los procesos de **gestión de riesgos, control y gobierno,** utilizando un enfoque sistemático y disciplinado.

Las normas emplean la palabra "debe" para referirse a un requisito incondicional.

ROLES DE LA AUDITORÍA INTERNA

La función de auditoria debería asegurar a la alta dirección las contribuciones al valor agregado respecto a la eficiente gestión de TI y al logro de los objetivos del negocio.

ISACA

ROLES DE LA AUDITORÍA INTERNA

El rol fundamental de la auditoría interna respecto a la gestión de riesgos -ERM- es:

Proveer aseguramiento objetivo a la junta sobre la efectividad de la gestión de riesgos en la organización, para ayudar a asegurar que los riesgos claves de negocio están siendo gestionados apropiadamente y que el sistema de control interno esta siendo operado efectivamente

ROLES LEGÍTIMOS DE AUDITORÍA INTERNA QUE DEBEN REALIZARSE CON SALVAGUARDA

Facilitación, identificación y evaluación de riesgos.

Entrenamiento a la gerencia sobre respuesta a riesgos.

Coordinación de actividades de gestión de riesgos.

Consolidación de reportes sobre riesgos.

Mantenimiento y desarrollo del marco de gestión de riesgos.

Defender el establecimiento de la gestión de riesgos.

Desarrollo de estrategias de gestión de riesgo para aprobación de la junta.

ROLES QUE AUDITORÍA INTERNA NO DEBE REALIZAR

Establecer el apetito de riesgo.

Imponer procesos de gestión de riesgo.

Manejar el aseguramiento sobre los riesgos.

Tomar decisiones en respuesta a los riesgos.

Implementar respuestas a riesgos a favor de administración.

Tener responsabilidad de la gestión de riesgo.

RECURSOS DE AUDITORIA DE SI

RECURSOS DE AUDITORÍA DE SI

Los estándares de auditoria de SI de ISACA requieren que el auditor de SI sea técnicamente competente (S4 Competencia técnica) y que posea las habilidades y conocimientos necesarios para realizar el trabajo de un auditor.

El auditor de SI debe mantener su competencia técnica a través de una educación profesional continua.

La Gerencia de auditoría de SI también debe proporcionar los recursos de TI necesarios para realizar auditorias de SI apropiadamente de naturaleza altamente especializada (por ejemplo, herramientas, metodología, programas de trabajo).

ESCENARIO DE LAS ORGANIZACIONES DE LA ACTUALIDAD

1. Incremento en las regulaciones de todo tipo
2. Incremento en el riesgo operativo
3. Incremento del riesgo operacional
4. Alta competencia producto de la globalización
5. Constantes cambios producto de fusiones, adquisiciones, expansión.
6. Incremento en la complejidad de transacciones
7. Seguridad en las Transacciones

NECESIDADES DE EVALUACIÓN, CONTROL Y SEGUIMIENTO

1. Soporte Tecnológico incremental
2. Cumplimiento regulatorio
3. Escacez de Recursos
4. Exigencia de Rentabilidad y Competencia
5. Incremento en los Alcances y coberturas de evaluación
6. Presupuestos Limitados
7. Personal Calificado

REQUERIMIENTOS PARA EL AUDITOR POR PARTE DE LA ORGANIZACIÓN

1. **Estándares y Procedimientos de Auditoría**
2. Gestión y Gobierno de Tecnología de Información
3. Infraestructura, Redes y Telecomunicaciones
4. Bases de Datos
5. Administración de la Seguridad de la Información
6. Desarrollo y Adquisición de Sistemas

PERFIL DEL AUDITOR DE T.I.

- Lic./Ing en Tecnología, Administración, Contabilidad y Finanzas
- Especialización en Tecnología y/o Finanzas
- Conocimiento del Sector o Negocio
- Bilingüe
- Certificación (CIA, CISA, CISM, CISSP)
- Conocimiento de Herramientas de Tecnología
- Conocimiento de Administración de Proyectos
- Experiencia en el desarrollo y/o Gestión de Proyectos de Tecnología

CÓDIGO DE ÉTICA

Principios Relevantes para la profesión y práctica de la Auditoria Interna

Integridad La integridad de los auditores internos establece confianza y, consiguientemente, proporciona la base para confiar en su juicio.

Objetividad Los auditores internos exhiben el más alto nivel de objetividad profesional al reunir, evaluar y comunicar información sobre la actividad o proceso a ser examinado. Los auditores internos hacen una evaluación equilibrada de todas las circunstancias y forman sus juicios sin dejarse influir indebidamente por sus propios intereses o por otras personas.

CÓDIGO DE ÉTICA

Confidencialidad Los auditores internos respetan el valor y la propiedad de la información que reciben y no divulgan información sin la debida autorización a menos que exista una obligación legal o profesional para hacerlo.

Competencia Los auditores internos aplican el conocimiento, aptitudes y experiencias necesarios al desempeñar los servicios de auditoría interna.

PREGUNTA 1

Cuál de las siguientes situaciones se permitiría bajo el Código de Ética del IIA

a) Como respuesta a una citación, un auditor apareció en una corte y reveló información confidencial y relacionada con auditoría que podría dañar a la organización del auditor.

b) Un auditor utilizó información relacionada con auditoría al tomar la decisión de comprar acciones emitidas por la corporación del empleador.

c) Después de elogiar a un empleado en una comunicación de un trabajo de auditoría reciente, un auditor aceptó un obsequio de él.

d) Un auditor no informó observaciones significativas sobre actividad ilegal al consejo porque la gerencia indicó que resolvería la cuestión.

PREGUNTA 2

Como parte de un programa de reconocimiento de méritos, una división ofreció a un auditor interno un premio de valor económico significativo en reconocimiento de los ahorros que se lograron por las recomendaciones del auditor. De acuerdo con el Marco para la Práctica Profesional, ¿cuál es la acción más apropiada que el auditor debe tomar?

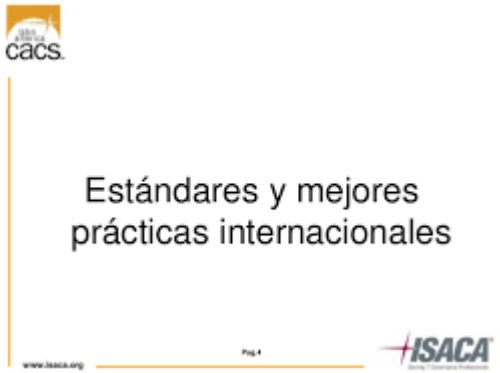
- a. Aceptar el premio, pues el trabajo ya concluyó y se emitió el informe.
- b. Aceptar el premio con la condición de que se done lo recaudado a una institución de beneficencia.
- c. Informar a la gerencia de auditoría y consultarle si debe aceptar el premio.
- d. Rechazar el premio e informar al gerente de la división.

PREGUNTA 3

Al evaluar el riesgo asociado con una actividad un auditor interno debe:

- a. Determinar cómo administrar mejor el riesgo.
- b. Proveer aseguramiento en la administración de riesgo.
- c. Actualizar el proceso de administración de riesgos sobre la base de las exposiciones al riesgo.
- d. Diseñar controles para mitigar los riesgos identificados.

TAREA 1



Leer y comprender los Estándares para la Práctica Profesional de la Auditoría Sistemas de Información ISACA

ANÁLISIS DE RIESGOS

ANÁLISIS DE RIESGOS

El análisis de riesgos es parte de la planificación de auditoria y ayuda a identiticar los riesgos y vulnerabilidades para que el auditor de SI pueda determinar los controles necesarios para mitigar el riesgo.

Los auditores de SI deben ser capaces de identificar y diferenciar los tipos de riesgo y los controles usados para mitigarlos. Deben tener conocimiento de los riesgos comunes del negocio, riesgos de TI relacionados y controles relevantes.

Los auditores deben ser capaces de valorar el riesgo como ayuda para determinar el enfoque y planificar el trabajo de auditoria.

ANÁLISIS DE RIESGOS

Existen muchas definiciones de riesgo, lo que quiere decir que tiene distintos significados para diferentes personas. Tal vez una de las definiciones de riesgo más sucintas usadas en el negocio de la seguridad de la información es la provista por las Directrices para la Gestión de Seguridad de Tu publicada por la Organización Internacional de Estandarización (ISO).

“El potencial de que una amenaza determinada explote las vulnerabilidades de un activo o grupo de activos y, por consiguiente, ocasione pérdida o daño a la organización”

ANÁLISIS DE RIESGOS

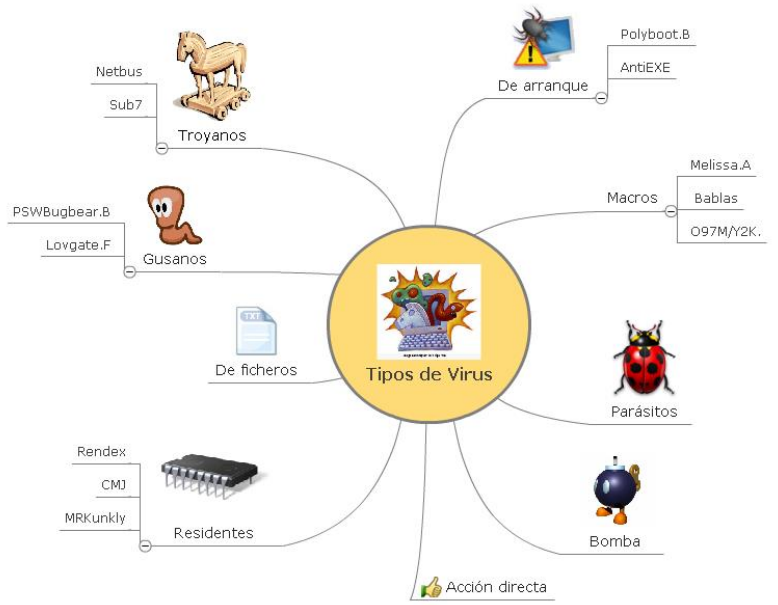
El auditor de SI está a menudo centrado en asuntos de alto riesgo asociados con la **confidencialidad, disponibilidad o integridad** de información sensible y crítica y con los sistemas y procesos subyacentes de información que generan almacenan y manipulan dicha información.

EVALUACIÓN DE RIESGOS

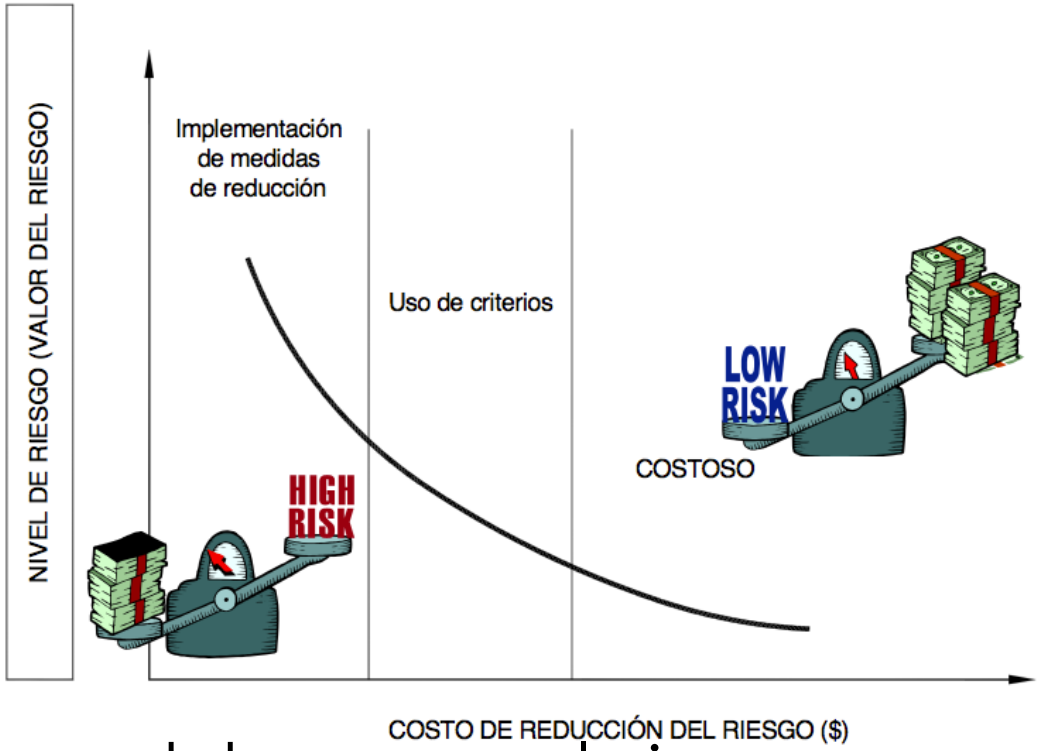
El proceso de evaluación de riesgos se caracteriza como un ciclo de vida iterativo que comienza **identificando los objetivos del negocio,** los activos de información y los sistemas o recursos de información subyacentes que generan/ almacenan, usan o manipulan los activos clave (hardware, software, base de datos, redes, instalaciones, personas, etc.) para lograr estos objetivos.

EVALUACIÓN DE RIESGOS

Identificados los activos de información sensible y/o crítica, **se realiza una evaluación de riesgos para identificar las amenazas y determinar la probabilidad de ocurrencia, impacto resultante y las medidas adicionales que mitigarían este impacto** a un nivel aceptable para la gerencia.



EVALUACIÓN DE RIESGOS



El análisis costo-beneficio es un proceso de análisis que puede basarse en cualquiera de las siguientes opciones:

El costo del control

La tolerancia a riesgo de la gerencia

Métodos preferidos de reducción de riesgos

La etapa final se relaciona con el monitoreo de los niveles de desempeño de los riesgos gestionados cuando se identifiquen cambios significativos en el ambiente.

TIPOS DE RIESGOS

1. Operacional
2. Tecnológico
3. Regulatorio
4. Fraude
5. Reputacional
6. otros

SISTEMA DE CONTROL INTERNO

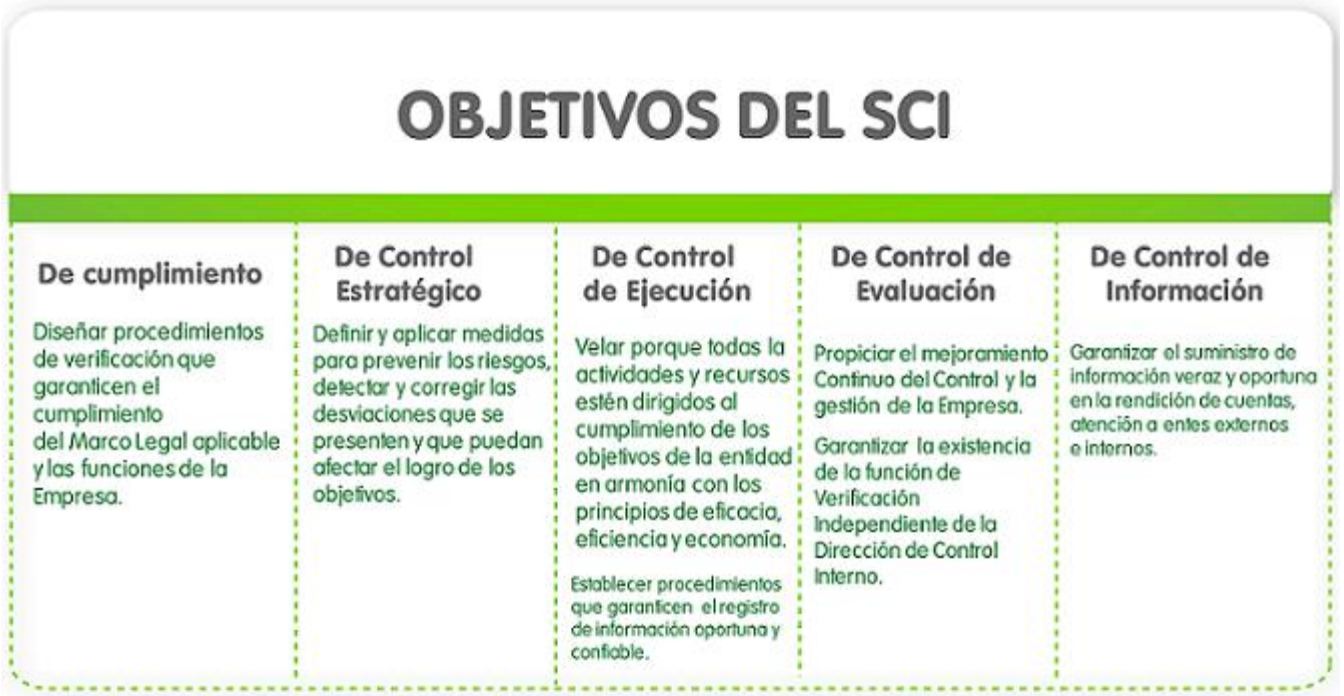
SISTEMA DE CONTROL INTERNO

Los controles internos están normalmente constituidos por políticas, procedimientos, prácticas y estructuras organizacionales implementadas para reducir los riesgos para la organización.

SISTEMA DE CONTROL INTERNO

SISTEMA DE CONTROL INTERNO

Los controles internos son desarrollados para proveer una certeza razonable a la gerencia de que se alcanzaran los objetivos de negocio de la organización y de que se prevendrán o detectarán y corregirán los eventos de riesgo.



CONTROLES GENERALES

- Plan de organización y operación
- Procedimientos de documentación, revisión y evaluación
- Controles de hardware
- Controles de acceso
- Controles de información y procedimientos

CONTROLES DE APLICACIÓN

Controles de ingreso de datos

Controles de proceso

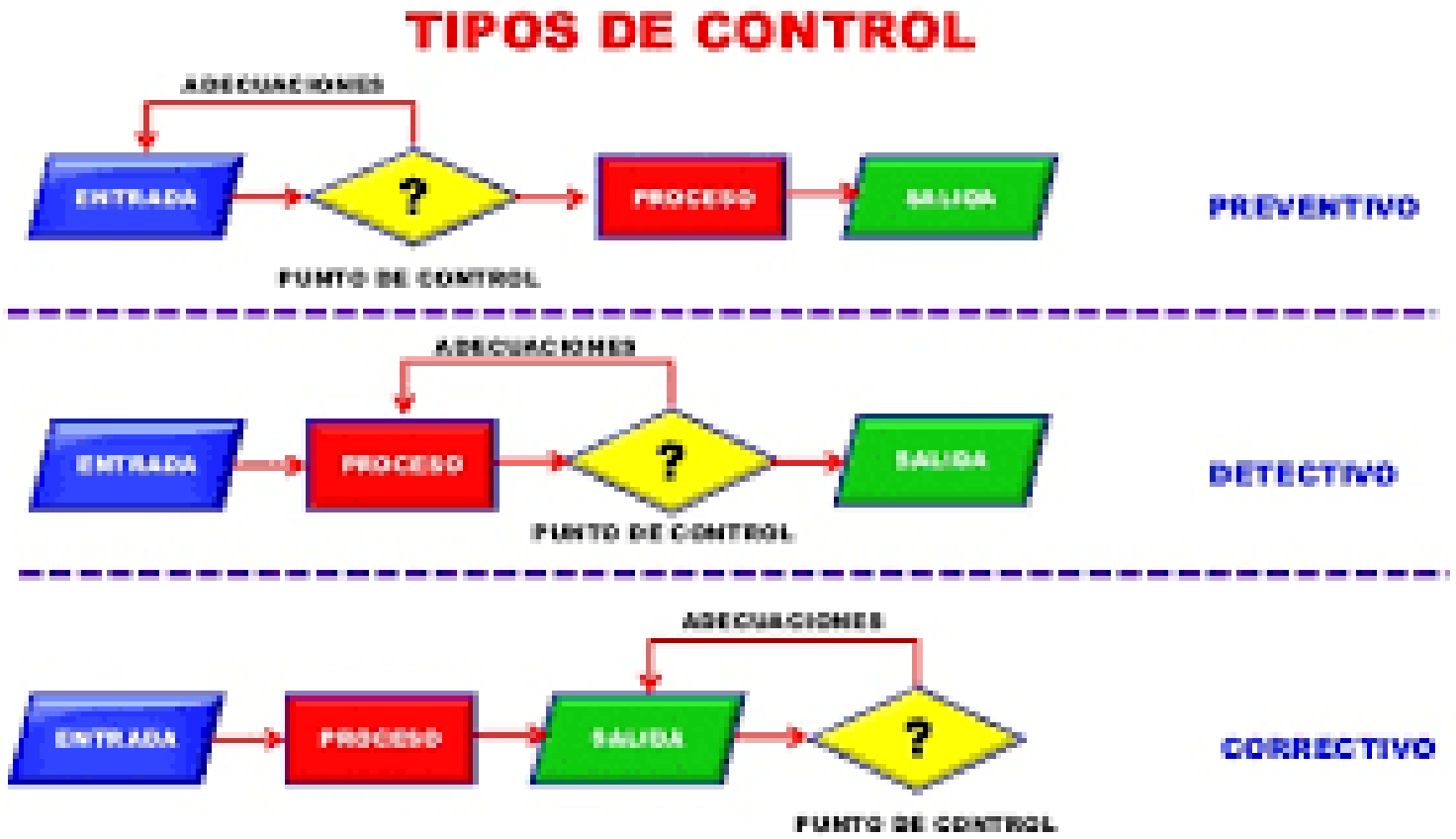
Controles de salida

CONTROLES INTERNOS

Los controles internos no sólo tratan los objetivos de negocio/operativos, sino que también deberían estar preparados para tratar eventos no deseados a través de la prevención, detección y corrección.

Los elementos de control están clasificados como preventivos, detectivos o correctivos de acuerdo a su naturaleza.

CLASIFICACIÓN DEL CONTROL



PREGUNTA 1

Una compañía pretende adquirir un ERP ya que ha escuchado que el uso de este tipo de herramientas permite hacer más eficiente las actividades administrativas, ¿cuál es la actividad más importante que tiene que llevar a cabo la empresa durante el inicio del proyecto?

A. Estudio de impacto y riesgo

B. Adecuar las políticas, filosofía y prácticas administrativas a la forma en que operan los ERPs

C. Análisis de principales vendedores de ERPs

D. Aprobación de cambios en la arquitectura de sistemas y orientación tecnológica

RESPUESTA

La respuesta correcta es la A.

Cuando se considera un cambio de la magnitud que involucra un ERP, es imperativo que se lleve a cabo un estudio minucioso de impacto y riesgo. Los puntos B y D son consecuencia de este estudio. El punto C se lleva a cabo una vez que se ha decidido que si se efectuará una compra de un ERP

PREGUNTA 2

De los controles implementados para el lograr un adecuado control de acceso en los equipos remotos, cual sería él MÁS débil.

A. revisar periódicamente las operaciones realizadas en los equipos remotos.

B. La documentación técnica y manuales operativos de todos los sistemas está disponibles sólo para todo el personal de SI.

C. instalar software de control de acceso al equipo y archivos.

D. implementar cifras control para la transmisión de la información generada en los equipos remotos.

RESPUESTA

La respuesta correcta es la B.

Ya que es recomendable que toda la documentación técnica y operativa esté disponible a TODO el personal de SI, independientemente de la función que éste realice. La documentación debe ser accesible sólo por personal autorizado. Las opciones A, C y D son controles que ayudan a garantizar un adecuado control de acceso.

PREGUNTA 3

Un Auditor de Sistemas que participa en un Proyecto de Desarrollo de una Aplicación debe estar consiente que seguir una metodología de Ciclo de Vida de Desarrollo de sistemas (CVDS) diseñada de manera adecuada, no asegura que el Proyecto culmine con éxito, el Auditor debe revisar además los siguientes aspectos de la disciplina de administración de un proyecto, con EXCEPCIÓN DE

A. Soporte de la Alta Gerencia en las etapas de diseño y desarrollo del Proyecto de Software.

B. Prueba sistemática de los módulos, en una forma lineal paso por paso.

C. Planificación del Proyecto que incluye estimados efectivos de recursos y tiempo.

D. Seguimiento administrativo a las actividades de diseño y desarrollo de software.

RESPUESTA

La respuesta correcta es la B.

La Prueba sistemática de los módulos, en una forma lineal paso por paso, es parte de las actividades desarrolladas por los programadores durante la construcción del software. A, C y D son todos aspectos de la disciplina de administración de un proyecto que el Auditor debe revisar.

PREGUNTA 4

Si al estar evaluando la aplicación de nómina, el auditor de SI revisa la existencia de firmas en formularios para procesar lotes de datos, totales calculados y controles para rechazar sólo transacciones que tengan errores, que tipo de controles estará revisando:

A. controles de procesamiento

B. controles de salida

C. controles de entrada

D. Controles compensatorios

RESPUESTA

La respuesta correcta es la C.

Ya que las firmas en formularios para procesar lotes de datos pertenecen a los tipos de AUTORIZACION DE ENTRADA DE DATOS, totales calculados pertenecen a los CONTROLES Y BALANCE DE LOTES y controles para rechazar sólo transacciones que tengan errores, pertenecen al tipo de tratamiento que se le debe dar al REPORTE Y MANEJO DE ERRORES en la entrada de datos.

PREGUNTA 5

Las medidas que podría tomar un auditor de SI para alcanzar un entendimiento de negocio incluyen todo lo siguiente EXCEPTO:

A. Recorrer las instalaciones claves de la organización

B. Leer el material anterior que incluye publicaciones de la industria, reportes anuales y reportes de análisis financieros independientes.

C. Revisar los organigramas de la Alta Gerencia.

D. Estudiar los reportes regulatorios o las reglamentaciones que sean aplicables.

RESPUESTA

La respuesta correcta es la C.

Ya que Revisar los organigramas de la Alta Gerencia no es una medida que podría tomar el auditor de SI para alcanzar un entendimiento del negocio.

PREGUNTA 6

Una vez que los riesgos han sido identificados, se pueden evaluar los controles existentes o se pueden diseñar nuevos controles para:

A. Tener un mayor entendimiento de las características del negocio.

B. Alcanzar un nivel aceptable de riesgo.

C. Justificar el alcance de los programas de auditoría.

D. Garantizar la protección a los activos de la organización.

RESPUESTA

La respuesta correcta es la B.