Sourcing (abastecimiento)

- Se relacionan con la forma en que la organización va a obtener las funciones de SI requeridas
  - In-sourcing: que el servicio sea desarrollado in-house
  - Out-sourcing: desarrollado por alguien extra
  - Híbrido

-90-

Sourcing

- Las funciones de SI pueden ser realizadas alrededor del mundo, ventaja por zonas horarias
  - Onsite: el staff trabaja en el lugar del departamento de SI
  - Offsite: un lugar fuera del depto pero en el área geográfica
  - Offshore: un lugar remoto lejos del área geográfica

-91-

¿Cómo elegir?

- ¿Son los SI una función clave?
- ¿Requiere esta función conocimiento específico, procesos y staff crítico para alcanzar los objetivos?
- ¿Puede esta función realizarse en otro lugar con el mismo o más bajo costo sin incrementar los riesgos?
- ¿Qué experiencia tiene la organización usando servicios de terceros?

-92-

Si se decide usar outsourcing

- Definir la función de SI que será implementada mediante outsourcing
- Describir los niveles de servicio requeridos y las métricas mínimas
- Conocer el nivel de habilidades y calidad deseadas
- Conocer el costo in-house para comparar con lo ofrecido

Realizar una revisión a conciencia de los posibles proveedores

-93-

Outsourcing

- Requiere que la gerencia revise el sistema de control sobre el cual puede depender
- El objetivo es mejorar los procesos de negocio a través de una reestructuración para tomar ventaja sobre la competencia

-94-

Razones

- La organización desea concentrarse en actividades centrales
- Presión sobre los márgenes de ganancia
- Incremento de la competencia, hay que ahorrar dinero
- Flexibilidad con respecto a la organización y la estructura

-95-

Ejemplos de servicios

- Data entry
- Diseño y desarrollo de nuevos sistemas
- Mantenimiento de aplicaciones existentes
- Conversión de aplicaciones legacy
- Operación del help desk o call center

-96-

Exhibit 2.9—Advantages, Disadvantages and Business Risks and Risk Reduction Options Related to Outsourcing

Possible Advantages	Possible Disadvantages and Business Risks	Risk Reduction Options
• Commercial outsourcing companies can achieve economies of scale through the deployment of reusable component software. • Outsourcing vendors are likely to be able to devote more time and to focus more effectively and efficiently on a given project than in-house staff. • Outsourcing vendors are likely to have more experience with a wider array of problems; issues and techniques than in-house staff. • The act of developing specifications and contractual agreements using outsourcing services is likely to result in better specifications than if developed only by in-house staff. • Because vendors are highly sensitive to time-consuming diversions and changes, feature creep or scope creep is substantially less likely with outsourcing vendors.	• Costs exceeding customer expectations • Loss of internal IS experience • Loss of control over IS • Vendor failure (ongoing concern) • Limited product access • Difficulty in reversing or changing outsourced arrangements • Deficient compliance with legal and regulatory requirements • Contract terms not being met • Lack of loyalty of contractor personnel toward the customer • Disgruntled customers/employees as a result of the outsource arrangement • Service costs not being competitive over the period of the entire contract • Obsolescence of vendor IT systems • Failure of either company to receive the anticipated benefits of the outsourcing arrangement • Reputational damage to either or both companies due to project failures • Lengthy, expensive litigation • Loss or leakage of information or processes	• Establishing measurable, partnership-enacted shared goals and rewards • Using multiple suppliers or withholding a piece of business as an incentive • Performing periodic competitive reviews and benchmarking/benchtrending • Implementing short-term contracts • Forming a cross-functional contract management team • Including contractual provisions to consider as many contingencies as can reasonably be foreseen

Qué más considerar

- Incorporar que se espera de la calidad del servicio (CMM, ISO, ITIL, etc)
- Reporte incumplimientos y seguimiento
- En el desarrollo asegurar que se incluyan controles de cambios y requerimientos de testeo

-98-

Qué más considerar

- Detallar parámetros específicos de performance
- Un criterio de resolución de conflictos
- Idemnización por daños
- Claúsulas sobre derechos a auditar
- Mantenimiento de CIA

-99-

Tener en cuenta

- Outsourcing no sólo es una decisión en cuanto a costos
- Es una decisión estratégica
- Calidad del servicio, continuidad, procedimientos de control, ventaja competitiva y conocimiento técnico
- Es clave elegir bien el supplier
- Buen contrato y **SLA (service level agreement)**

-100-

SLA

- Son una forma contractual de ayudar al depto de SI de gestionar los recursos de información bajo el control de un proveedor
- Comprometen al proveedor a un nivel requerido de servicio y soporte
- Establecen requerimientos de HW y SW
- Establecen penalidades y opciones de enforcement

-101-

Monitoreo de outsourcing

- Se debe monitorear y revisar regularmente y realizar auditorías
- Hay que asegurar que se cumplen las condiciones del contrato y SLA
- También que los incidentes sean reportados y gestionados en forma apropiada

-102-

Casos de estudio 2A y 2B

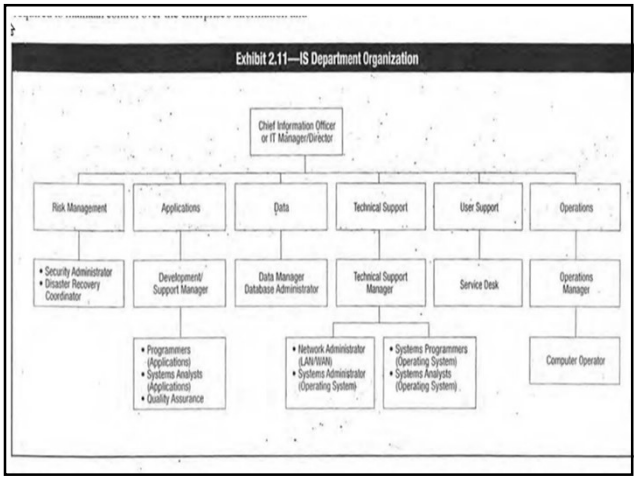
- Ver Manual de ISACA Capítulo 2
- Ejemplo template sla

-103-

Cómo organizar la función de SI

- Un departamento de SI puede ser organizado de muchas maneras
- Los organigramas organizacionales son importantes para mostrar como está estructurada una empresa
- El auditor debe determinar si la estructura y las descripciones de cada rol son las adecuadas

-104-



Funciones

Analista de Sistemas:

- elucidar requerimientos de información de aplicaciones nuevas y actuales
- diseñar arquitectura de SI para satisfacer los requerimientos
- facilitar la implementación de los SI
- escribir procedimientos y documentación para usuarios finales

-106-

Funciones …

Analista Programador:

- diseñar programas para satisfacer los requerimientos de información:
- codificar
- testear y corregir
- documentar programas
- modificar programas para remover errores, mejorar la eficiencia y satisfacer nuevas necesidades.

-107-

Funciones …

Programador de Sistemas:

1. mantiene y mejora:
   a. el software operativo,
   b. el software de librerías,
   c. el software utilitario
2. provee asistencia cuando ocurren fallas de sistemas no usuales.

-108-

Funciones …

Administrador de Datos:

1. relevar los requerimientos de datos de los usuarios
2. formular políticas a seguir sobre datos
3. planificar la evolución de las bases de datos de la organización
4. mantener la documentación sobre los datos

-109-

Funciones …

Administrador de Base de Datos:

1. responsable por la eficiencia operativa de las bases de datos de la organización
2. mantener el control de accesos a las bases de datos
3. asistir a los usuarios a utilizar mejor las bases de datos

-110-

Funciones …

Administrador de Seguridad:

1. implementar y mantener la seguridad física y lógica sobre la función de los SI
2. controlar el estado de la seguridad sobre la función de los SI
3. investigar las violaciones a la seguridad
4. asistir a los usuarios a diseñar controles
5. mantener los mecanismos de control de acceso

-111-

El Auditor Debe Evaluar…

- Las responsabilidades de cada puesto deben estar claras.
- Las personas deben comprender correctamente:
  - sus obligaciones
  - su autoridad
  - sus responsabilidades

-112-

Separación de Obligaciones - Motivo….

- **O**curre que había que hacer un trabajo importante, y ***Todos*** sabía que ***Alguien*** lo haría. ***Cualquiera*** podría haberlo hecho, pero ***Nadie*** lo hizo.
- ***Alguien*** se enojó cuando se enteró, porque le hubiera correspondido a ***Todos***.
- **E**l resultado fue que ***Todos*** creía que lo haría ***Cualquiera***, y ***Nadie*** se dio cuenta de que ***Alguien*** no lo haría.

-113-

Separación de Obligaciones

- Se debe preservar la separación de obligaciones.
- En organizaciones descentralizadas es más difícil la separación de funciones - el usuario analiza, programa, y opera.
- En algunos casos las personas que realizan estas tareas no cuentan con el perfil de un profesional en SI.

-114-

Separación de obligaciones

- Si una sola persona es responsable de diversas aplicaciones críticas...
  - Entonces es posible que ocurran errores que no se detecten en tiempo y forma
- Es importante para prevenir y detectar actos maliciosos

-115-

Qué hay que separar

- Custodia de activos
- Registro de transacciones
- Autorizaciones

-116-

Si hay separación de obligaciones

- Acceso a las computadoras, programas en producción, datos en producción y sistema operativos deben estar limitados
- **El daño potencial debido a las acciones de una sóla persona se reduce!**

-117-

Combinaciones

- El departamento de sistemas y el de usuarios finales deben estar separados
- Los auditores de SI deben entender el riesgo de combinar funciones incompatibles!

-118-

Exhibit 2.12—Segregation of Duties Control Matrix

	Control Group	Systems Analyst	Application Programmer	Help Desk and Support Manager	End User	Data Entry	Computer Operator	Database	Network	Systems	Security Administrator	Systems Programmer	Quality Assurance
Control Group		X	X	X		X	X	X	X	X		X	
Systems Analyst	X			X	X		X				X		X
Application Programmer	X			X	X	X	X	X	X	X	X	X	X
Help Desk and Support Manager	X	X	X		X	X		X	X	X		X	
End User		X	X	X			X	X	X			X	X
Data Entry	X		X	X			X	X	X	X	X	X	
Computer Operator	X	X	X		X	X		X	X	X	X	X	
Database Administrator	X		X	X	X	X	X		X	X		X	
Network Administrator	X		X	X	X	X	X	X					
System Administrator	X		X	X		X	X	X				X	
Security Administrator		X	X			X	X					X	
Systems Programmer	X		X	X	X	X	X	X		X	X		X
Quality Assurance		X	X		X							X	

X—Combination of these functions may create a potential control weakness.

	Grupo de Control	Analista de Sistemas	Progr. Aplicaciones	HELP DESK /soporte	Usuario Final	Admin. Base de Datos	Admin. Redes	Admin Sistemas	Admin Seguridad	Program de Sistemas	Quality Assurance
Grupo de Control		■	■	■		■	■	■		■	
Analista de Sistemas	■			■	■				■		■
Programador de Aplicaciones (ie: Sistema Operativo)	■			■	■	■	■	■	■	■	■
HELP DESK /soporte	■	■	■		■	■	■	■		■	
Usuario Final		■	■	■		■	■			■	■
Admin. Base de Datos	■		■	■	■	■		■		■	■
Admin. Redes	■		■	■	■					■	
Admin Sistemas	■		■	■		■				■	
Admin Seguridad		■	■							■	
Programador de Sistemas	■		■	■	■	■		■	■		■
Quality Assurance		■	■		■					■	

-120-

Mecanismos de control

- Para asegurar la separación de obligaciones
- Autorización de transacciones: es resposabilidad del departamento de los usuarios
- Se deben realizar chequeos periódicos para saber si se realizan transacciones no autorizadas

-121-

Mecanismos de control

- Custodia de activos: se debe determinar y asignar apropiadamente
- El dueño de los datos se asigna a un departamento en particular
- Tiene la responsabilidad de determinar el nivel de seguridad apropiado para proteger los activos

-122-

Mecanismos de control

- Se proveen mediante una combinación de seguridad
  - Física
  - De aplicaciones
  - Del sistema
- Las decisiones de control de acceso se basan en una política organizacional

-123-

Mecanismos de control

- Los controles no deben interrumpir el ciclo normal de trabajo
- Tampoco deben sobrecargar demasiado a los administradores o auditores
- Las políticas de control de acceso suelen discrecionales o mandatorias

-124-

Compensando la falta de separación

- En algunas organizaciones pequeñas pueden no haber suficiente personal
- Qué hacemos en este caso?
- Tenemos que implementar controles que mitiguen los riesgos

-125-

Compensando la falta de separación

- Uso de audit trails: permiten al auditor crear un mapa que sigue hacia atrás el flujo de la transacción
- Son un buen control para compensar la ausencia de separación de obligaciones
- El auditor debe determinar quien inició la transacción, tiempo, cambios de información y que actualizó

-126-

Compensando la falta de separación

- Reconciliación
- Reporte de excepciones
- Logs de transacciones
- Revisión de los supervisores
- Revisiones independientes

-127-

Ubicación de la Función de SI

- La ubicación de la función de los SI dentro de la organización tiene un impacto significativo en la efectividad de los SI.
- El auditor debe:
  - determinar la importancia asociada a los SI,
  - evaluar si la función de los SI está ubicada correctamente, para asegurar la autoridad e independencia.

-128-

Ubicación – Ejemplo 1

.Si según McFarlan si la organización es estratégica, debe:

- ser un grupo independiente y
- estar ubicada alta en la jerarquía (para participar en la toma de decisiones estratégicas).

-129-

Ubicación – Ejemplo 2

- Si la organización es soporte, su ubicación es menos y importante.
- Puede no ser un sector independiente y la función estar diseminada en áreas usuarias
- Puede depender de la gerencia mas importante, ej: Contaduría
- Puede no estar ubicada alta en la jerarquía ya que no participa de las decisiones estratégicas

-130-

Conducir

- La conducción es una función gerencial compleja diseñada para influir en el comportamiento de un individuo o grupo.
- El proceso de conducción requiere que la gerencia: motive a los subordinados, dirija sus tareas y comunique información.

-131-

Conducir – Control 1

- Para el auditor es difícil evaluar esta tarea.
- Si no se conduce correctamente, el personal puede:
  - no comprender los objetivos generales,
  - estar desmotivado,
  - no comunicar los resultados que obtiene

-132-

Conducir – Control 2

- Para poder evaluar la conducción se deben comprender tres aspectos claves:
  - cómo motivar subordinados
  - cómo encontrar un estilo de liderazgo para las características del trabajo
  - cómo comunicarse claramente con los subordinados

-133-

Conducción del Personal

La mayoría de las teorías se basa en que no existe la mejor manera de motivar a toda las personas.

Si existen dos analistas de sistemas:

- A tiene facilidad para trabajar con la incertidumbre
- B es más conservador y le molesta la incertidumbre

A quien asignamos en cada tipo de proyecto?

-134-

Motivación del Personal - Control

Los auditores no tienen los conocimientos ni la experiencia para evaluar si cada persona está correctamente motivada.

Se examinan indicadores:

- estadísticas de rotación de personal
- fracasos frecuentes de proyectos en cuanto a satisfacer presupuestos
- niveles de ausentismo

-135-

Estilos de Conducción

- Los estilos varían de democráticos a autoritarios.
- No existe un estilo único apropiado para todo. Varía dependiendo de las personas y las tareas.
- Algunas personas requieren mayor conducción que otras.
- Algunas son más inseguras o inexpertas que otras.

-136-

Estilos de Conducción - Control

- Ideal: buscar gerentes con estilos de conducción adaptables.
- Se pueden capacitar para este fin
- Sucede lo mismo que con la otra función (motivación), es difícil para el auditor evaluarla.
- Debe analizar rotación, cumplimiento de presupuestos e inasistencias.

-137-

Comunicación Efectiva

- La función de SI requiere que se realicen tareas de manera precisa, la comunicación entre supervisor y subordinados es crítica.
- Los mensajes deben comprenderse claramente.
- El auditor puede evaluar los canales formales e informales de comunicación.

-138-

Canales Formales

- planificación de sistemas,
- documentación de estándares,
- documentación de políticas,
- minutas de reuniones,
- memorandums enviados al personal..

-139-

Canales Formales

Se debe estar alerta a elementos que distorsionan la buena comunicación:

- mensajes ambiguos,
- mensajes con mucha información filtrada,
- mensajes que sólo reflejan un punto de vista

-140-

Canales Informales

- Incluyen:
  - entrevistas con el personal (auditor-personal),
  - observaciones sobre si un propósito existe entre los miembros del equipo,
  - evaluación de las tareas que se realizan.
- En entrevistas con la alta gerencia, el auditor puede analizar cómo el gerente se comunica con sus empleados.

-141-

Comunicación Efectiva ...

- Los problemas de comunicación pueden tener un efecto directo e inmediato,
- Una mala decisión de diseño puede ocasionar problemas indirectos y a largo plazo, ej: pérdida de respeto al personal superior, y rotación de personal.
- Los auditores deben poder evaluar las consecuencias de la falta de comunicación a corto y largo plazo.

-142-

Evaluar la Función de Control

- Determinar cuando las tareas actuales de las funciones de los SI, se desvían de las actividades planificadas.
- Cuando la alta gerencia controla la función de los SI, surgen 2 preguntas:
  - ¿Cuánto debe invertir la organización en la función de los SI?
  - ¿Tiene la organización un beneficio económico por la función de los SI?

-143-

Evaluar la Función de Control

Los gerentes buscan los promedios del mercado, para determinar cuanto se debería invertir (benchmarking)

-144-

Evaluar la función de control

Puede ser problemática por que:

- refleja una instancia reactiva en lugar de proactiva,
- podría desviarse voluntariamente (ej: tecnológicamente atrasados o adelantados),
- la inversión en la función de los SI podría no estar ligada a la estrategia general de la organización.

-145-

Evaluar la Función de Control

- La alta gerencia ve a la función de SI como un gasto y no como una inversión de capital.
- Si es una inversión de capital, se debe invertir hasta que no haya pérdidas o haya beneficios.
- El problema de esta visión es que los SI están plagados de intangibles y tienen un alto riesgo de pronta obsolescencia

-146-

Evaluar la Función de Control

- Los auditores deben evaluar si:
- la alta gerencia decide sobre cuanto invertir,
- controla cuidadosamente el análisis de inversión de capital.

-147-

Evaluar la Función de Control

Para la pregunta, (¿existe beneficio económico?) no existe un método fácil para evaluar:

- se puede realizar algo con post-auditoría y proyectos muy controlados.
- es muy difícil en entornos distribuidos y con varios proyectos en simultáneo.

-148-

Plan de Continuidad de Negocio

149

Bussines continuity planning

- El objetivo es permitir que el negocio siga ofreciendo los servicios críticos en el evento de un disrupción
- También sobrevivir a una interrupción desastrosa
- El primer paso para diseñar un BCP es identificar los procesos de negocio de importancia estratégica

-150-

Bussines continuity planning

- El análisis de riesgo los bienes que soportan los procesos clave
- También las listas de vulnerabilidades y la probabilidad de que sucedan
- El gerenciamiento de estos riesgos se aborda en la preparación del **BCP / DRP**

-151-

BCP

- Es responsabilidad de la alta gerencia
- El plan debe abordar todas las funciones y los bienes necesarios para producir un nivel reducido pero suficiente de funcionalidad
- Incluye procedimientos para minimizar las consecuencias

-152-

Qué incluye el BCP

- Plan para la continuidad de operaciones
- El DRP que se usa para recuperar una facilidad que se ha vuelto inoperable, incluyendo una posible relocación
- El plan de restauración para volver a la normalidad en un lugar nuevo o recuperado

-153-

BCP en los SI

- El acercamiento es el mismo, lo que está amenazado es la continuidad de los SI, que son de importancia estratégica
- El BCP de SI es muy importante y si es un plan separado debe ser consistente
- Debe ser actualizado si la estructura de IT cambia

-154-

Principales Amenazas

- Fuego
- Agua
- Variaciones de Energía
- Computadores
- Polucíon
- Daño Estructural
- Intromisión no autorizada

-155-

Daño por Fuego

- Generalmente, es la amenaza más seria a la seguridad física de los bienes de los SI.
- Las pérdidas por el fuego pueden ser sustanciales.
- Algunos países tienen servicios públicos u organizaciones gubernamentales que aconsejan sobre las medidas de protección contra incendios.

-156-

Daño por Fuego - Controles

- Los administradores de seguridad deben revisar y testear las protecciones contra incendios periódicamente.
- El uso correcto de estos sistemas requiere entrenamiento periódico del personal.
- Se deben documentar los procedimientos a realizar por emergencias.

-157-

Daño por Agua – Medidas y Control

- tener techos, paredes y puertas a prueba de agua – cuando sea posible
- asegurar que existe un correcto sistema de drenado
- instalar alarmas en lugares estratégicos
- cubrir el hardware con protectores cuando no se usa
- ubicar los bienes por encima del nivel del suelo.

-158-

Variaciones de Energía

- Pueden tomar la forma de:
  - aumento de poder (sobrecarga)
  - disminución
  - corte
- Las fuentes de energía deben monitorearse permanentemente para asegurar que sean adecuadas y confiables.

-159-

Variaciones de Energía - Medidas

- Para protección de aumentos temporarios, se instalan reguladores de voltaje.
- Para protección de aumentos sostenidos, se instalan interruptores de circuitos.
- Para protección contra pérdidas de energía, fuentes alternativas. Se instalan UPSs.
- Tener en cuenta otros objetos: lockeo de puertas.

-160-

Polución

- La polución puede dañar un dispositivo de disco, o puede causar un incendio.
- El mayor elemento de polución es el polvillo.
- Se debe filtrar el aire a través de los sistemas de aire acondicionado y evitar la acumulación de polvillo en techos y pisos.
- El café es un polutante que si cae sobre teclados o impresoras lo pueden dejar inoperable.

-161-

Intrusión No Autorizada

- Para cuando el intruso obtiene acceso físico al edificio:
  - paredes o cercos de protección a los edificios
  - seguridad de puertas y ventanas
  - sistema de lockeo de puertas con tarjetas magnéticas
  - seguridad en los conductos de aire acondicionado
  - etc

-162-

Seguridad lógica

- Determinar quien puede ir a donde y si están autorizados
- Identificación y autenticación de los usuarios es un prerequisito
- Luego se pueden aplicar otros controles como niveles de autoridad de los usuarios

-163-

Seguridad de las comunicaciones

- Los datos se deben proteger de las escuchas y/o manipulaciones
- Para esto es necesario una combinación de asegurar los medios de comunicaciones , asegurar el mensaje (encripción) y autenticación del mensaje
- De estos temas hablaremos un poco más adelante

-164-

Information security policy

- Para proteger en forma efectiva los bienes la politica de seguridad de la compañia debe proveer guías
- Servirán para determinar el valor de los recursos de información y el impacto de los eventos que podrían ocurrir
- También la gerencia puede detallar el nivel de riesgo que están dispuestos a aceptar

-165-

Que debe decir

- Que la información es un recurso importante que debe ser protegido
- Que para esto la organización cumplirá con todas las leyes aplicables y regulaciones
- Que el acceso a la información será garantizado a los individuos conforme lo requieran para realizar sus funciones
- Que se mantendrá la confidencialidad de la información

-166-

Que debe decir

- Que la información se protegerá en forma apropiada contra modificaciones no autorizadas
- Que la información estará disponible para soportar las decisiones de negocio
- Que se implementarán las estructuras de control apropiadas para garantizar integridad, confidencialidad y disponibilidad

-167-

Recuperación del desastre

168

Controles de Último Recurso

- A pesar de los resguardos que se puedan tomar, la función de los SI puede sufrir un desastre.
- En estas situaciones, quedan dos controles como último recurso:
- Plan de Recuperación de Desastre
- Seguros

-169-

Plan de Recuperación de Desastre

- Propósito: restaurar las operaciones de la función de los SI, en el evento de algún tipo de desastre.
- El impacto puede ser:
  - localizado: daño en una BD
  - generalizado: incendio en la instalación
- Se deben hacer ensayos
- Estos planes son muy caros, difíciles de preparar, mantener y testear.

-170-

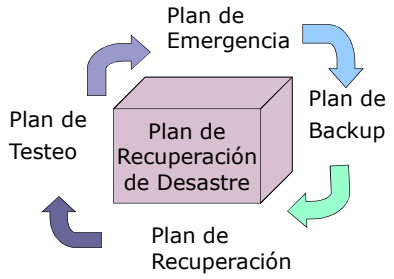
Plan de Recuperación de Desastre

- Los auditores deben evaluar que estos planes existan, estén en su lugar y sean adecuados.
- Los auditores externos están especialmente interesados en la habilidad del cliente de retomar sus operaciones
- Poner especial cuidado en demandas que puedan surgir por no cumplimientos de contratos con otras partes.

-171-

Plan de Recuperación de Desastre

- El plan incluye cuatro partes:



-172-

Plan de Recuperación de Desastre

- El plan debe proveer las políticas, guías y procedimientos a seguir para todo el personal que tiene responsabilidad en la función de los SI
- Ejemplo: procedimientos de backup a ejecutar diariamente.

-173-

Plan de Emergencia

- Plan de Emergencia (PE): especifica las acciones a realizar inmediatamente luego de producido el desastre.
- La gerencia debe identificar las situaciones en que se invoca el plan.
- Las acciones que se inicien, dependerán de la naturaleza del desastre.
- Irse enseguida, quedarse, etc..

-174-

Plan de Emergencia

- Identificar las situaciones en las cuales se necesita invocar al PE.
- Para cada situación incluir:
  - quién debe ser notificado inmediatamente cuando ocurre el desastre.
  - acciones a tomar. Ejemplo: apagar equipos, cortar llaves, remover archivos, etc.
  - procedimientos de evacuación y retorno
- Se debe especificar el responsable para cada tarea, y el procedimiento a seguir.

-175-

Plan de Backup - Contenido

- los tipos de backup que se deben mantener,
- la frecuencia de ejecución,
- los procedimientos,
- la ubicación de los recursos,
- el sitio donde estos recursos pueden restaurarse,

-176-

Plan de backup

- las operaciones para restaurar,
- el personal responsable de recolectar los recursos de back up
- las prioridades a asignar para recuperar los sistemas,
- un cronograma que muestre cuando cada sistema puede ser recuperado.

-177-

Plan de Backup - Controles

- El plan necesita actualización permanente. Ejemplo: personal que no trabaja más en la empresa, con tareas de responsabilidad dentro del plan actualización del inventario de hardware y software disponible.
- La mayor dificultad radica en asegurar que todos los recursos críticos están backupeados.

-178-

Plan de Backup – Recursos 1

- **personal:** entrenamiento y rotación de obligaciones entre el personal de SI, para facilitar reemplazos. Acuerdos con otras empresas para proveer personal.
- **hardware:** acuerdo con otra empresa para provisión del hardware
- **facilidades:** acuerdo con otra empresa para provisión de facilidades
- **documentación:** inventario de documentación almacenada de manera segura en el sitio y fuera del sitio.

-179-

Plan de Backup – Recursos 2

- **insumos:** inventario de insumos críticos almacenados de manera segura en el sitio y fuera del sitio, con listas de vendedores que provean los insumos
- **datos/información:** inventario de archivos almacenados de manera segura dentro y fuera del sitio
- **software de aplicación (sistema):** inventario del software de aplicación (sistema) almacenado de manera segura dentro y fuera del sitio

-180-

Plan de Backup - Sitios

Un tema importante es la selección del sitio de backup. Se pueden estudiar las siguientes alternativas:

- cold site
- hot site
- warm site
- acuerdo recíproco

-181-

Plan de Backup – Cold Site

- Si la organización tolera un tiempo sin sistema, ésta alternativa podría ser adecuada.
- El lugar tiene todas las facilidades para instalar los equipos necesarios.
- La organización puede tener su propio sitio o firmar un contrato con otra empresa.

-182-

Plan de Backup – Hot Site

- Todo el hardware y las facilidades de operación deben estar disponibles en el sitio.
- En algunos casos, se guarda acá el software, los datos, e insumos.
- Son caros de mantener.
- Se comparte entre varias organizaciones.

-183-

Plan de Backup – Warm Site

- Provee un nivel de backup intermedio.
- Tiene todas las facilidades del cold site, más el hardware que podría ser difícil de conseguir o instalar.

-184-

Plan de Backup – Acuerdo Recíproco

Dos o más organizaciones pueden tener un acuerdo de proveerse mutuamente facilidades de backup en caso de sufrir un desastre alguna de ellas.

- Es una alternativa barata.
- Se debe tener suficiente capacidad de procesamiento.
- A menudo es informal.

-185-

Plan de Backup - Contratos

Si se usa un sitio de backup de otra empresa, los administradores de seguridad deben asegurar que los contratos incluyan:

1. en qué tiempo estará disponible el sitio de backup,
2. el número de organizaciones que simultáneamente pueden usar el sitio de backup,
3. la prioridad que se asignará a usuarios concurrentes en el caso de un desastre común

-186-

Plan de Backup - Contratos

4. el período por el cual se puede usar el sitio,
5. las condiciones bajo las cuales se puede usar el sitio,
6. las facilidades y servicios que se comprometen a proveer en el sitio,
7. qué controles se implementarán en el sitio.

-187-

Plan de Recuperación

- Plan de Recuperación (PR): define los procedimientos para restaurar las capacidades completas de los SI.
- Es específico y depende de las circunstancias del desastre.
- El plan debería especificar un comité de recuperación, las responsabilidades del comité, y proveer guías y prioridades e indicar qué aplicaciones recuperar primero.

-188-

Plan de Testeo

Plan de Testeo (PT): identifica las deficiencias en los PE, PB, PR, o en la preparación de la organización y del personal para un caso de desastre.

- Debe permitir simular desastres, y especificar el criterio por los cuales los PE, PB, y PR pueden considerarse satisfactorios.
- Se deben ejecutar periódicamente, esto es simular los desastres y requerir al personal que cumpla con los procedimientos estipulados en los planes.

-189-

Plan de Testeo

Inconvenientes:

–interrumpir las operaciones diarias

–que ocurra un desastre como resultado del testeo de procedimientos.

Soluciones: que se testee mediante inspecciones formales, y no en la práctica.

Planificar el testeo en un horario de poca carga - día y hora no conflictivos.

-190-

Auditar la continuidad del negocio (BCP)

- Evaluar la conexión de la estrategia del BCP con los objetivos de negocio
- Comparar el BCP con estándares y regulaciones existentes
- Verificar que el plan sea efectivo revisando testeos anteriores
- Verificar como se transportan los datos resguardados

-191-

Auditar la continuidad del negocio (BCP)

- Evaluar la respuesta del personal ante situaciones de emergencia
- Evaluar los manuales y procedimientos relacionados (que sean fáciles de entender)
- Ejercicio: consultar el manual de CISA para ver cuales son las preguntas usuales que debe realizar el auditor en este caso

-192-

Referencias

- Auditors guide to information systems auditing, R. Cascarino, Willey, 2007. Parte 2.
- CISA Manual 2013. ISACA. Capítulo 2.

-193-