UNIVERSIDAD DE COSTA RICA

Administración de Riesgos

Prof. Carlos Vega Alvarado

Tratamiento a los Riesgos

Agenda

- Generalidades
- Planes de tratamiento a riesgos
- Plan de recuperación ante desastres
  - Objetivos de punto y tiempo de recuperación
  - Estrategias de recuperación
  - Alternativas de recuperación
- Plan de continuidad del negocio

Tratamiento a Riesgos

- El objetivo del **tratamiento al riesgo** es seleccionar y aplicar una o más opciones para modificar los riesgos identificados.
- Implica un proceso cíclico de:
  - Evaluar cada alternativa de tratamiento;
  - Decidir si el nivel de riesgo residual es tolerable o no (en este caso, se debe escoger otra alternativa); y
  - Evaluar la eficacia del tratamiento.

Tratamiento a Riesgos

- Requiere del establecimiento de **indicadores de riesgo** que sean capaces de demostrar el grado de exposición de la organización.
- Deben considerar:
  - El impacto en caso de que se materialice el evento;
  - El esfuerzo para aplicar, medir y reportar resultados;
  - La fiabilidad con respecto a la exposición al riesgo; y
  - La sensibilidad con respecto a la precisión para identificar diferencias en el riesgo.

Planes de Tratamiento

- La selección del tratamiento a los riesgos consiste en lograr equilibrar los costos y beneficios de dicho tratamiento con respecto a los beneficios obtenidos de su aplicación.
- Las opciones de tratamiento no tienen que ser excluyentes: pueden darse combinaciones para obtener mayores beneficios.
- El tratamiento puede conllevar riesgos, los cuales deben ser considerados antes de decidir aplicarlos.

Planes de Tratamiento

Preparación y ejecución:

- Deben incluir información con respecto a:
  - Las razones para la selección del tratamiento y los beneficios esperados;
  - El personal responsable de aprobar el plan;
  - El personal responsable de ejecutar el plan; y
  - El conjunto de acciones propuestas.

Planes de Tratamiento

Seguimiento y revisión:

- Las actividades de seguimiento y revisión deben ser parte del proceso de gestión de riesgos.
- El control y vigilancia pueden ser periódicos o ad hoc.
- Los resultados deben ser registrados y utilizados como insumo para la revisión del marco de gestión de riesgos.

Planes de Tratamiento

Registro del proceso de gestión de riesgos:

- Se debe considerar registrar actividades para que la gestión de riesgo sea rastreable.
- Los registros permiten mejorar los métodos y herramientas, considerando:
  - Necesidades de aprendizaje continuo;
  - Costo/esfuerzo para crear y mantener registros;
  - Requerimientos legales y normativos;
  - Periodos de retención; entre otros.

Plan de Recuperación

- El **plan de recuperación ante desastres** *(DRP – Disaster Recovery Plan)* puede ser definido como las acciones tendientes a recuperar el negocio ante diferentes tipos de desastres:
  - Climáticos;
  - Accidentales;
  - Tecnológicos; entre otros.
- Incluye desastres a nivel lógico y físico.
- Genera los documentos necesarios para realizar las acciones incluidas en el plan.

Plan de Recuperación

- Puede estar sujeto a varios requerimientos de cumplimiento que, en caso de usar tercerización, los terceros también deben respetar.
- La mayoría se centran en asegurar la continuidad del servicio y la seguridad del personal.
- Tanto el programa de pruebas como las pruebas deben probarse regularmente para todas las funciones críticas y para verificar la seguridad de la información.

Plan de Recuperación

- Es una parte importante de los procesos de gestión de riesgos y de Plan de Continuidad del Negocio (BCP).
- Su propósito es garantizar que existen *controles rentables* para evitar posibles situaciones que inhabiliten las operaciones a través de las TI y para recuperar la capacidad de TI de la organización en caso de una interrupción.

Plan de Recuperación

Objetivos RPO y RTO:

Objetivo de Punto de Recuperación (RPO)	Objetivo de Tiempo de Recuperación (RTO)
Se determina con base en la pérdida de datos aceptable en caso de una interrupción.	Es el tiempo máximo establecido para la recuperación de una función o recurso del negocio.
Indica el tiempo mínimo posible en el que se pueden recuperar los datos.	Varía entre las diferentes prioridades organizacionales.
Cuantifica efectivamente la cantidad permisible de pérdida de datos en caso de interrupción, por lo que se asocia a la frecuencia de los respaldos.	

Plan de Recuperación

Objetivos RPO y RTO:

- Mientras más cerca del centro estén los requerimientos de tiempo, más alto será el costo de las estrategias de recuperación.

Plan de Recuperación

Estrategias de recuperación:

- Se consideran los siguientes parámetros:
  - *Ventana de interrupción:* es el periodo de tiempo máximo que puede esperar la organización desde el punto de fallo hasta la restauración de los servicios críticos, después de lo cual las pérdidas progresivas de la interrupción no se puede tolerar.
  - *Objetivo de entrega del servicio (SDO):* está directamente relacionado con las necesidades del negocio y define el nivel de servicios que se debe alcanzar durante el periodo de procesamiento alterno.

Plan de Recuperación

Estrategias de recuperación:

- Se consideran los siguientes parámetros:
  - *Máximo tiempo tolerable de interrupción:* es el tiempo máximo que la organización puede soportar el procesamiento en modo alterno, después de lo cual pueden surgir diferentes problemas, especialmente si el objetivo de entrega del servicio (SDO) alterno es más bajo que el SDO usual, por lo que la información en espera de actualización puede ser incontrolable.

Plan de Recuperación

Estrategias de recuperación:

- Los procedimientos de recuperación deben estar bien documentados para asegurar un adecuado retorno a las operaciones normales del sistema en caso de una interrupción.
- Estos procedimientos se basan en estrategias de recuperación y deben ser:
  - Recomendados y seleccionados por la alta dirección; y
  - Utilizados para desarrollar un plan de continuidad del negocio (BCP).

Plan de Recuperación

Estrategias de recuperación:

- La selección de la estrategia de recuperación depende de:
  - La criticidad de los procesos de negocio y sus aplicaciones asociadas;
  - Los costos y el nivel de seguridad; y
  - El tiempo de recuperación.
- En general, cada plataforma de TI que ejecuta una aplicación que soporta una función de negocio crítica requiere de una estrategia de recuperación.

Plan de Recuperación

Alternativas de recuperación:

- **Hot-Site** (sitio caliente):
  - Es una instalación que cuenta con todos los equipos de TI y con todas las comunicaciones que se requieren para respaldar las aplicaciones críticas;
  - Incluye una oficina para alojar al personal encargado de efectuar la recuperación de las operaciones.

Plan de Recuperación

Alternativas de recuperación:

- **Hot-Site** (sitio caliente):
  - Es una instalación que cuenta con todos los equipos de TI y con todas las comunicaciones que se requieren para respaldar las aplicaciones críticas;
  - Incluye una oficina para alojar al personal encargado de efectuar la recuperación de las operaciones.

Plan de Recuperación

Alternativas de recuperación:

- **Cold-Site** (sitio frío):
  - Es una instalación con el espacio apropiado y la infraestructura básica adecuada para apoyar la reanudación de las operaciones;
  - No incluye ni los equipos de TI o ni los equipos o dispositivos para comunicaciones;
  - No incluye programas, datos o soporte de oficina.

Plan de Recuperación

Alternativas de recuperación:

- **Acuerdos de reciprocidad:**
  - Son convenios entre compañías independientes que pueden funcionar de dos formas específicas:
    - En compañías similares, los participantes comparten las instalaciones de TI por un tiempo limitado cuando una de ellas pierde su capacidad de procesamiento.
    - En compañías que comparten equipos o aplicaciones únicas, los participantes se comprometen a ayudarse mutuamente durante los periodos de emergencia.

Plan de Continuidad

- El propósito del **plan de continuidad del negocio** *(BCP – Business Continuity Plan)* es permitir a una organización ofrecer sus servicios críticos después de un desastre y hasta que se recupere la operación normal.
- Su establecimiento es obligación de la alta dirección, quien es responsable de salvaguardar los activos de información y la viabilidad de la organización.

Plan de Continuidad

- Debe considerar:
  - Operaciones críticas necesarias para la sobrevivencia de la organización;
  - Recursos necesarios para apoyar el plan;
  - Procedimientos de evacuación y para declarar el desastre;
  - Identificación clara de responsabilidades;
  - Explicación paso a paso del proceso de recuperación;
  - Pruebas periódicas para medir el desempeño del plan y su adecuación a las operaciones actuales.

Referencias Bibliográficas

- ISACA. **Marco de Riesgos de TI**. ISACA, 2009.
  - *Capítulo #5:* Fundamentos de Gobierno del Riesgo

- **Norma ISO 31000:2009 – Gestión de Riesgos**.

- ISACA. **The Risk-IT Practitioners Guide**. ISACA, 2009.