Desarrollo de la estrategia de mitigación de riesgos

Ing. Fredy Bustamante

Desarrollo de la estrategia de mitigación de riesgos

- Tipos de estrategias de mitigación de riesgos
- Proceso de mitigación de riesgos
- Mitigación de riesgos de TI
- Consideraciones sobre respaldo y recuperación

Desarrollo de la estrategia de mitigación de riesgos

- Mitigación de riesgos: **adopción de medidas para reducir los efectos adversos**.
  - En esta fase se desarrollan estrategias para **aceptar, evitar, reducir o transferir** riesgos relacionados con posibles interrupciones del negocio.
- La mitigación de riesgos es común utilizarla en diferentes ámbitos de la empresa, por ejemplo, en administración de proyectos se debe evitar o minimizar los efectos de eventos que puedan afectar el buen término de estos.
- El enfoque que veremos es específico para la continuidad de negocios y recuperación de desastres y veremos aspectos únicos relacionados con TI.

Desarrollo de la estrategia de mitigación de riesgos

Desarrollo de la estrategia de mitigación de riesgos

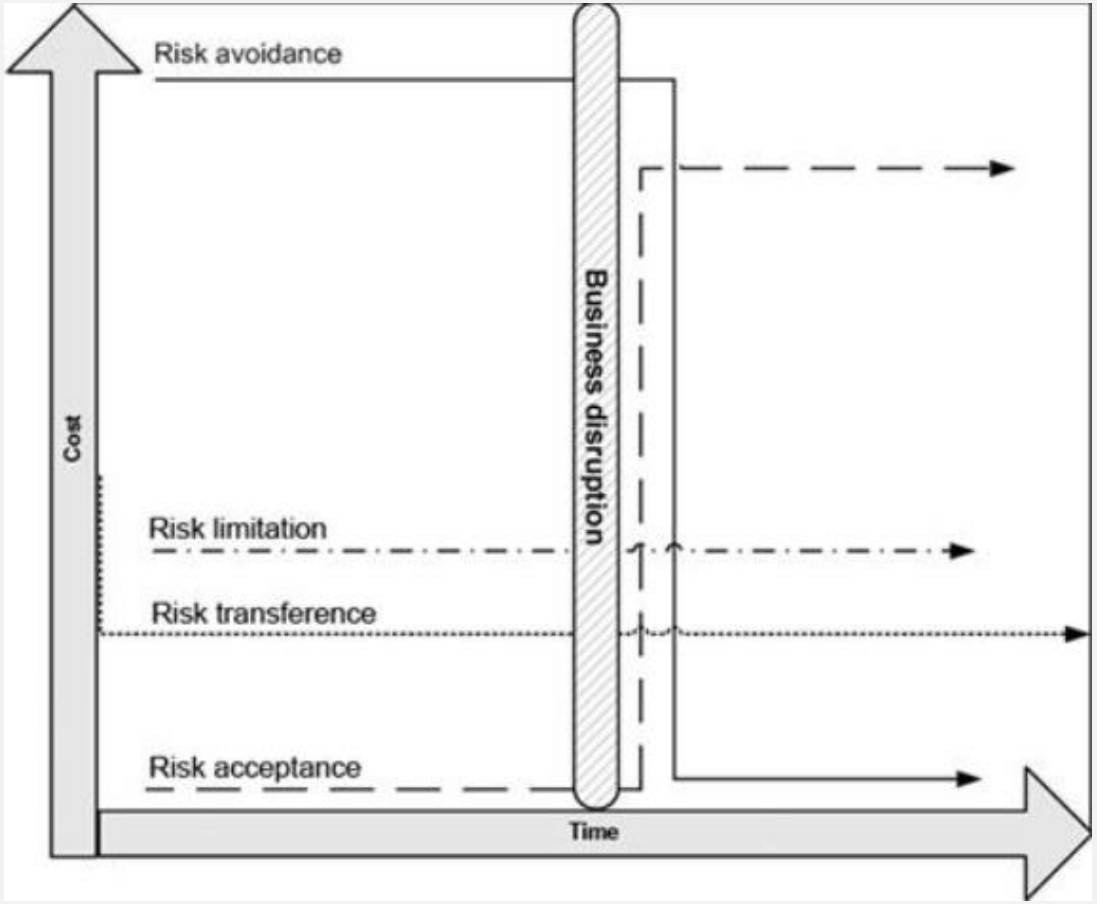
- Es importante tomar en cuenta que la estrategia de mitigación de riesgos debe ir acorde al perfil de la empresa, por ejemplo, si su empresa es aversa al riesgo y desea evitarlo a casi cualquier costo, sus estrategias deberán ser apropiadas a este objetivo.
- Debe mantenerse enfocado en las prioridades, como ya se habrá dado cuenta, este proceso es exhaustivo por lo que una de sus tareas es priorizar y cubrir los elementos clave.

Tipos de estrategias de mitigación de riesgo

Tipos de estrategias de mitigación de riesgo

- Las 3 opciones estándar son:
  - Aceptar
  - Evitar
  - Limitar
  - Transferir

Relación entre tiempo y costo para las opciones de mitigación



Tipos de estrategias de mitigación de riesgo

- **Aceptar el riesgo**
  - No es realmente una estrategia de mitigación pues no se está reduciendo de ninguna forma el efecto sino simplemente se está aceptando.
  - Sin embargo, el aceptar un riesgo es una opción legítima cuando administramos el riesgo.
  - La razón más común para tomar esta opción es que el costo de reducir en alguna medida el riesgo es más caro que el efecto que este tiene.
    - No vale la pena gastar $10,000 en un segundo servidor si el estar sin el servicio asociado tiene un costo de $1,000 mensuales.
  - Esta opción es prácticamente la opción de "no hacer nada" que se utiliza en varios ámbitos de toma de decisiones.
  - Para esta opción el costo antes de un evento es el más bajo y suele ser el más alto después de este (comparando entre estrategias para el mismo riesgo).
  - El problema de esta opción es que suele ser la que más utilizan las empresas sin realizar un verdadero análisis, por esto es importante que en la elaboración de su plan de BC/DR se analicen las diferentes opciones de forma correcta.

Tipos de estrategias de mitigación de riesgo

- **Evitar el riesgo**
  - Tomar medidas para que el riesgo se aborde por completo y no pueda ocurrir.
  - Esta opción es la opuesta a la anterior y se trata de evitar totalmente el riesgo.
  - Por ejemplo, si en la entrada de la empresa hay un árbol que, en caso de lluvia muy fuerte, puede botar una rama y caer sobre una persona o un vehículo, la opción anterior es aceptar que podría pasar y si pasa pagar los gastos y demanda correspondiente, mientras en esta opción se quitaría el árbol por completo para evitar cualquier riesgo.
  - Por ejemplo, en TI, tener un sitio totalmente redundante que sea capaz de sostener todos los servicios de la empresa y que los datos sean actualizados en el instante en que estos cambian en el sitio original.
  - Esta opción suele ser la más cara de implementar y mantener antes de un evento y es la que suele tener menor costo adicional después de este (costo de estar fuera y de recuperarse).
  - Evitar el riesgo suele no ser factible para todos los riesgos y/o todas las empresas por diferentes razones (no solo la financiera) pero debe ser analizada para poder determinarlo y no tomar decisiones sin tener la información correspondiente.
  - La decisión suele centrarse en determinar si se debe gastar tiempo y dinero hoy (mitigar) o después (remediar).

Tipos de estrategias de mitigación de riesgo

- Limitar el riesgo
  - Es la estrategia más comúnmente utilizada y consiste en limitar la exposición al riesgo tomando una serie de acciones.
  - Por ejemplo, realizar backup de los datos todos los días es una estrategia de mitigación pues limita la pérdida de datos (efecto) a causa de algún evento (riesgo), realmente no estoy evitando quedarme sin un disco por un fallo, pero limito el efecto.
  - Esta opción está entre aceptar y evitar tanto en el tema de costo antes como después de un evento.

Tipos de estrategias de mitigación de riesgo

- Transferir el riesgo
  - Implica transferir el riesgo a un tercero dispuesto a hacerlo.
  - Muchas empresas subcontratan ciertas operaciones como servicio al cliente, nómina, entrega de productos, etc. Aunque normalmente lo hacen para enfocarse en sus competencias básicas, pero también pueden hacerlo como parte de la gestión de riesgos.
  - Un ejemplo de transferencia es la contratación de seguros a empresas que están dispuestas a aceptar el riesgo a cambio de dinero o contratos de servicio que incluyen atención a emergencias a cualquier hora y el cambio de piezas si fuera necesario.
  - Una diferencia importante entre limitar y transferir es que limitar suele incluir un pago inicial (compra de equipo) y pagos recurrentes (por mantenimiento, licencias, etc.) mientras que transferir suele ser un gasto fijo cada periodo (mes, año, etc.)
  - Se debe considerar que normalmente el transferir el riesgo es únicamente la parte de costos, no podrán ser incluidos efectos como la reputación ante los clientes.

Proceso de mitigación de riesgos

Proceso de mitigación de riesgos

- Para desarrollar una estrategia de mitigación de riesgos debemos analizar las opciones.
  - Ya hemos visto que existen varios tipos de riesgos, amenazas, fuentes de amenazas, vulnerabilidad e impacto.
  - Luego tenemos que analizar el perfil de recuperación que incluye los requerimientos y opciones de recuperación, tiempos (MTD) y costos contra las opciones.
  - A partir de esto podemos seleccionar las opciones apropiadas y una vez conocidos estos elementos, se puede diseñar una estrategia integral.

Proceso de mitigación de riesgos

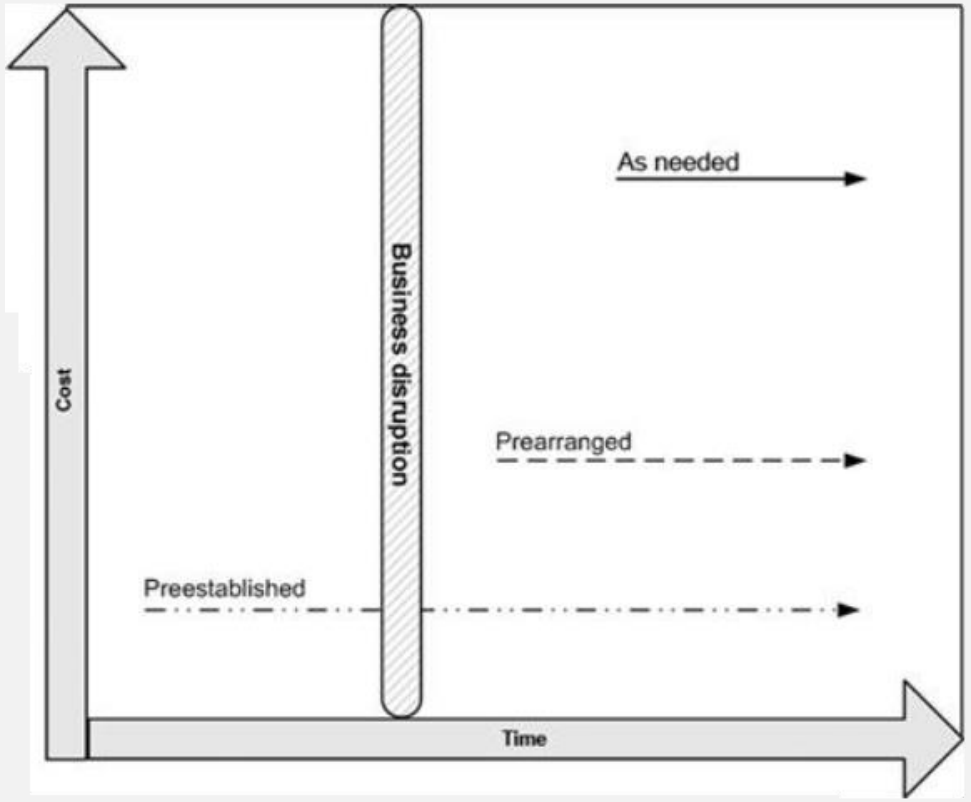
- Requerimientos de recuperación
  - Los requisitos de recuperación generalmente se desglosan por áreas funcionales, incluidas instalaciones y áreas de trabajo, sistemas de TI e infraestructura, fabricación y producción (operaciones) y datos críticos/registros vitales, en general, cualquier requisito importante que tenga su empresa.
  - Estos requerimientos de recuperación se desarrollan para los procesos críticos identificados en el BIA, lo que nos ayuda a identificar los recursos que deben ser el foco de la estrategia de recuperación.
  - Si un proceso no es de misión crítica o esencial no será un buen candidato para gastar tiempo y esfuerzo en este proceso de mitigación.
  - Se pueden clasificar respecto a las áreas funcionales, por ejemplo, para el área de Instalaciones (edificios), un requerimiento de recuperación puede ser un espacio alterno para las oficinas o un centro de comando para gestionar la crisis y las comunicaciones.

Proceso de mitigación de riesgos

- Opciones de recuperación
  - Para desarrollar una variedad de opciones de recuperación se debe tomar en cuenta el impacto en la organización, dependencias con otras funciones, dependencias de TI, puestos clave, las habilidades y los conocimientos necesarios, el tiempo necesario de recuperación y cualquier otra información que haya identificado en el BIA.
  - Estas opciones tendrán distintos plazos, costos y capacidades, por lo que, en este punto, solo debe preocuparse de desarrollar la lista de **opciones viables** en función de los datos obtenidos.
  - Por ejemplo, si necesita un sitio alterno podría listar una nube pública, nube privada, co-location, sitio alterno propio, sitio alterno alquilado, después se deberá evaluar cada opción.

Proceso de mitigación de riesgos

- Opciones de recuperación
  - Existen 3 opciones básicas de recuperación:
    - **Según sea necesario:** generalmente toma más tiempo para implementar después de un evento y cuesta más, pero puede tener un costo menor si se toma en cuenta los costos acumulados durante un tiempo largo.
    - **Con antelación:** suelen ser de un costo intermedio e implementarse en menor costo pues ya está pactado, para estas opciones debe evaluar de forma exhaustiva a sus proveedores para asegurarse que podrán cumplir con lo ofrecido.
    - **Preestablecida:** se podrá implementar de forma casi inmediata, pero suelen tener un costo mayor, recurrente e irrecuperable antes del evento. En algunos casos se busca minimizar el impacto de estos costos aprovechando de alguna forma, por ejemplo, un sitio alterno puede ser frío, tibio o caliente.



Proceso de mitigación de riesgos

- Tiempo de recuperación de las opciones
  - Una vez listados los requerimientos y las opciones de recuperación se deberán observar los tiempos de recuperación de cada opción.
  - Dado que ya está definido el MTD puede compararlo con estos tiempos, las opciones que no cumplen con esto deberán ser eliminadas del listado.
- Costo vs capacidad de las opciones de recuperación
  - Ahora cuenta con una lista reducida de opciones de recuperación en función de las que cumplen con los requisitos de recuperación y el MTD.
  - A esta lista debe agregar la evaluación del costo y las capacidades de cada una, el listado de atributos a considerar es:
    - Costo: Costo de la opción de mitigación o recuperación.
    - Capacidad: las capacidades de la opción (características vs necesidades).
    - Esfuerzo: la cantidad de esfuerzo que tomará implementar y administrar la opción.
    - Calidad: atributos de calidad del producto, servicio o datos asociados con la opción.
    - Control: cantidad de control que retendrá la empresa sobre el proceso crítico.
    - Seguridad física (safety): en los casos que aplique, se debe indicar una calificación de la seguridad física que esta opción ofrece para luego poder hacer una comparación con otras opciones (seguridad para las personas y equipos en las instalaciones).
    - Seguridad (security): se refiere a la seguridad de los datos y recursos (que no sean robados, eliminados, etc.).
    - Conveniencia: suele ser un atributo cualitativo basado, de preferencia, en datos cuantitativos, se debe documentar los datos y razones para calificar la conveniencia, por ejemplo, como alta, neutra o baja.

Proceso de mitigación de riesgos

- Costo vs capacidad de las opciones de recuperación
  - Puede crear una matriz para evaluar estos atributos y poder tomar una decisión, por ejemplo:
  - Opciones para adquirir un sistema crítico de TI

Opción	Costo	Capacidad	Esfuerzo	Calidad	Control	Seguridad física	Seguridad	Deseabilidad
Según sea necesario	Alto	Desconocido	Alto	Bajo	Bajo	N/A	N/A	Bajo
Con antelación	Medio	Cumple requisitos	Medio	Medio	Medio	N/A	N/A	Medio
Preestablecida	Bajo	Cumple requisitos	Bajo	Alta	Alta	N/A	N/A	Medio

  - Opciones para establecer un data center alterno

Opción	Costo	Capacidad	Esfuerzo	Calidad	Control	Seguridad física	Seguridad	Deseabilidad
Sitio frío pagado por la empresa	Medio	Cumple requisitos	Medio	Bajo	Alta	Media	Media	Media
Sitio caliente con proveedor externo	Alto	Cumple requisitos	Bajo	Alta	Baja	Alta	Alta	Media
Servicio de nube pública	Bajo	Cumple requisitos	Bajo	Media	Baja	Alta	Media	Media

Proceso de mitigación de riesgos

- SLA de recuperación
  - Cualquier acuerdo de servicio de recuperación debe incluir métricas específicas que lo definan, por ejemplo:
    - Tiempo de respuesta
    - Capacidades técnicas: espacio de almacenamiento, velocidades, etc.
    - Acceso a las áreas y equipos
    - Acceso a áreas de trabajo para el personal
    - Procedimientos y garantía de seguridad
    - Soporte técnico y funcional

Los SLA que tenga con servicios contratados le pueden servir de referencia para evaluar los de recuperación.

Proceso de mitigación de riesgos

- Revisión de controles existentes
  - En algunos casos ya tendrá implementadas algunas de las opciones de recuperación, es necesario revisar que cumplan con los requisitos correspondientes pues seguramente no fueron implementadas con estos en mente.
  - Además, el hecho de estar ya implementadas, pueden ser una ventaja vs otras opciones y hacer más fácil su aceptación o realizarle mejoras.

Proceso de mitigación de riesgos

- Desarrollo de la estrategia de mitigación de riesgos
  - Los pasos para desarrollar la estrategia de mitigación de riesgos son:
  1. Reunir los datos de recuperación
  2. Comparar costos, capacidades y SLAs de las opciones
  3. Determinar si las opciones restantes se clasifican en aceptar, evitar, limitar o transferir el riesgo y cuál es más deseable de estas.
  4. Seleccionar las opciones que mejor se adapten a las necesidades de la empresa.
  - Estos datos y el proceso realizado deben quedar documentados, el resultado final puede documentarlo utilizando tablas o cualquier formato que la empresa utilice siguiendo el mismo estilo que los pasos anteriores.

Proceso de mitigación de riesgos

- Ejemplo de opciones para la estrategia de mitigación de pérdida de datos críticos:

Categoría	Opción	Costo, Capacidad, SLAs	Mitigación de Riesgos	Implementar
Frecuencia de respaldo de datos	Continua	Costoso, ningún tiempo de inactividad, excede el MTD	Solución potencial, dependiendo del costo de implementación.	
	Diario	**Moderado, hasta 8 horas de pérdida potencial de datos, 3 horas para restaurar, cumple con MTD**	**Implementar un proceso de respaldo diario para reducir la probabilidad de pérdida significativa de datos y para reducir el tiempo de recuperación para cumplir con MTD.**	**X**
	Semanal	Moderado, hasta 5 días de pérdida potencial de datos, 12 horas para restaurar, puede cumplir con MTD		
	Mensual	Bajo, no cumple con MTD		
Tipo de Respaldo de Datos	Completo	Mayor tiempo de respaldo, menor tiempo de recuperación, cumple con MTD		
	Incremental	Tiempo de respaldo medio, mayor tiempo de recuperación, excede MTD		
	Diferencial	**Tiempo de respaldo medio, tiempo de recuperación medio, cumple con MTD**	**El respaldo diferencial cumple con MTD al menor costo.**	**X**

Proceso de mitigación de riesgos

- Ejemplo de opciones para la estrategia de mitigación de pérdida de datos críticos:

Categoría	Opción	Costo, Capacidad, SLAs	Mitigación de Riesgos	Implementar
Método de Respaldo de Datos	Cintas de respaldo	Mayor tiempo de recuperación, menos costoso, puede no cumplir con MTD		
	Vaulting electrónico	Tiempo de recuperación largo, algo costoso, puede no cumplir con MTD		
	Replicación de datos	Tiempo de recuperación medio, gasto medio, puede cumplir con MTD		
	Sombreado de discos	**Recuperación rápida, gasto medio, puede cumplir con MTD**	**Basado en restricciones de costo, esta opción puede cumplir con MTD. Este y el sombreado de discos serán explorados en términos de costo, tiempo y viabilidad.**	**X**
	Espejo de discos	**Recuperación rápida, gasto medio, puede cumplir con MTD**	**Basado en restricciones de costo, esta opción puede cumplir con MTD. Este y el sombreado de discos serán explorados en términos de costo, tiempo y viabilidad.**	**X**
	Virtualización de Almacenamiento	Tiempo de recuperación rápido, alto costo, elimina el riesgo de fallos localizados, cumple con MTD		
	Almacenamiento en Red	Tiempo de recuperación rápido, mayor costo, elimina el punto único de fallo, puede eliminar el riesgo de fallos localizados, cumple con MTD		
	Clúster de Alta Disponibilidad en Área Amplia	Tiempo de recuperación rápido, mayor costo, elimina el punto único de fallo, puede eliminar el riesgo de fallos localizados, cumple con MTD		
	Espejo Remoto	Disponibilidad continua, tiempo de recuperación cero, costo más alto, elimina el punto único de fallo y el riesgo de fallos localizados, excede MTD		

Mitigación de riesgos de TI

Mitigación de riesgos de TI

- Hasta el momento hemos hablado bastante sobre el análisis de impacto y la mitigación de riesgos a nivel empresa.
- Vamos a centrarnos en la mitigación de riesgos específicamente para TI.
- El riesgo con respecto a los datos incluye, además de los **desastres naturales** de los que hemos estado hablando, las **interrupciones en el centro de datos** (incendios, energía, humedad, etc.), **fallas de hardware** (por antigüedad, accidentes, etc.) o **software** (bugs), **violaciones de seguridad** que pueden incluir pérdida, robo o modificaciones de datos críticos, e interrupciones debido a que los **datos críticos no están disponibles** para los usuarios (DDoS, malware, etc.).
- Los análisis de riesgos y de impacto deben cubrir estos, por lo que es un bueno momento para revisarlos con más detalle.

Mitigación de riesgos de TI

- Datos y registros críticos
  - Al analizar el MTD y el costo de las interrupciones (pérdida de productividad, pérdida de ingresos, etc.), tendrá una sólida comprensión del impacto que tendría la pérdida de varios datos críticos en la organización.
    - Si no lo tiene claro, debe regresar a su análisis de riesgo, vulnerabilidad e impacto para obtener en **dónde se guarda sus datos críticos, quién los genera, qué se hace con ellos y qué harían sin ellos.**
  - Además, deberá analizar los requerimientos legales y regulatorios asociados con los datos críticos, por ejemplo, datos médicos, financieros, etc. que sean afectados de alguna forma por la ley.
    - Es necesario consultar con abogados sobre esto y que nos mantengan informados sobre cambios en las leyes y regulaciones que puedan afectarnos.
  - Finalmente debe revisar todos sus controles existentes, así como las soluciones propuestas a la luz de la recuperación ante desastres y continuidad del negocio.
  - Normalmente encontraremos que nuestros controles cubren partes de los posibles riesgos, pero seguramente no hayamos considerado todas las posibilidades al analizarlos contra estos.

Mitigación de riesgos de TI

- Sistemas e infraestructura críticos
  - A partir de las necesidades de protección y administración de datos dentro del alcance del proceso de planificación de BC/DR, puede comenzar a evaluar soluciones de hardware y software, proveedores y costos.
  - No existe una fórmula única para solucionar esto, deberá utilizar los conocimientos y experiencia propia y de su equipo, así como proveedores que puedan asesorarlo.
    - Las convenciones, visitas de o a proveedores, desayunos y demás invitaciones son buena fuente de actualización para estar enterados de los últimos avances y servicios ofrecidos por los diferentes fabricantes.
  - A partir de analizar los controles actuales vs los que necesita, podrá determinar si puede **complementar o debe cambiar por completo algunos de ellos**.
  - A partir de este proceso se dará cuenta que debe tener proveedores, hardware y software que le **solucionen a mediano plazo**, 3 a 5 años, y no simplemente buscar las soluciones más baratas, imagine una solución de backup de la que no tenga seguridad que estará vigente y funcionando un año después.
  - Además, se recomienda que **no se enfoque en soluciones a largo plazo**, más de 10 años, pues seguramente tendrá que invertir mucho tiempo y recursos en buscar la solución perfecta y, dado que la tecnología y los requerimientos cambian, podría malgastar estos recursos.
    - Esto depende mucho de la solución y situación específicas, debe analizar todas las aristas antes de tomar decisiones.
  - Debe evaluar el **costo de adquisición, implementación y administración de la solución**. Tendrá que hacer algunas concesiones, pero si tiene en cuenta las **limitaciones de datos y el presupuesto, podrá diseñar una solución aceptable (o incluso óptima)** que se ajuste a esos parámetros.

Mitigación de riesgos de TI

- Revisión de las prioridades críticas del sistema
  - A través de su análisis de impacto empresarial, debería haber desarrollado una **evaluación de los sistemas de TI críticos que incluya una priorización** de los activos.
  - Debería tener un listado de los activos y sus prioridades, por ejemplo:
    - Cluster de servidores virtuales: Alto
    - Acceso a Internet: Alto
    - Acceso a correo electrónico: Bajo
    - NAS: Alto
    - CRM: Alto
    - Aplicación de administración de inventario: Medio
    - Sistema financiero: Medio
  - Basado en este análisis debe revisar sus estrategias de mitigación de riesgo para asegurarse que cumplen o exceden los requerimientos de recuperación en función de estas prioridades.
  - No se olvide de las dependencias, algunas veces nos centramos en los sistemas principales y nos olvidamos de que estos pueden depender de componentes que no estén clasificados como prioritarios.
    - Por ejemplo, podemos tener un servidor clasificado como importancia alta, tener un reemplazo, pero no tomar en cuenta el switch al que este se conecta, de forma que, al momento de la recuperación, no cumpliríamos con lo establecido debido a una dependencia.
  - Debemos documentar el orden de recuperación, algunos pueden ser intuitivos, como recuperar el servidor antes de instalar el SO, pero en algunos casos este orden podrá no ser tan obvio, por ejemplo, que un sistema deba acceder a Internet para verificar una licencia o un sistema que dependa del Active Directory para identificar a los usuarios.

Consideraciones sobre backups y recuperación

Consideraciones sobre backups y recuperación

- Como profesionales de TI estamos conscientes de la importancia de los backups y su respectiva recuperación, esto suele asociarse únicamente a datos, pero es aplicable a toda la infraestructura y software.
- Existen varias opciones y la idea es que revisemos algunas de ellas para tenerlas en mente en el momento de desarrollar nuestra estrategia.

Consideraciones sobre backups y recuperación

- Procesos de negocio alternos
  - En el análisis realizado hasta el momento usted tendrá los procesos de negocio clave y métodos alternativos para manejar estos procesos durante una interrupción, ya sea de los sistemas de TI, el edificio, el área en donde este se encuentra, etc.
  - En base a este análisis debe revisar cada proceso para determinar si existe un método alternativo para proveer los datos necesarios para que estos procesos funcionen de forma correcta.
    - Datos de órdenes de producción
    - Datos de clientes para atenderles en caso de dudas
    - Datos financieros
    - Nómina

Consideraciones sobre backups y recuperación

- Sistemas de recuperación de TI
  - Analice si tiene algún sistema de recuperación y si estos están actualizados, podría ser el momento adecuado de cambiarlos o mejorarlos.
  - Este proceso de análisis debe realizarlo de forma periódica, no puede depender de sistemas con una antigüedad de 5 años sin haberlos revisado previamente.
- Sitios Alternos
  - Esta es una de las decisiones más importantes, debe considerar que estos sitios suelen tener un costo alto, ya sea al inicio o como un gasto recurrente (o ambos).
  - Una clasificación de los sitios alternos puede ser:

Consideraciones sobre backups y recuperación

- Una clasificación de los sitios alternos puede ser:
  - Sitio alterno espejo: es un sitio alterno que tiene exactamente las mismas características y datos que el sitio primario, es el más costoso, aunque puede utilizarse como sitio de acceso rápido según donde estén localizados sus usuarios.
  - Sitio caliente: similar a un sitio espejo, pero no tiene una configuración idéntica siendo capaz de replicar los servicios más importantes.
  - Sitio tibio: un sitio alterno que está equipado para soportar algunos servicios se puede utilizar en el día a día como un sitio para servicios de menor importancia y en el momento de una interrupción tomarse para montar los servicios más importantes.
  - Sitio móvil: son datacenters que pueden transportarse a un lugar alterno y operar desde cualquier sitio.
  - Sitio frío: un sitio que no está en funcionamiento normal, pero existen los procesos necesarios para ponerlo en funcionamiento en el momento de una interrupción, es posible que se deba complementar parte de la infraestructura antes de que pueda funcionar completamente; en este sitio se podría guardar una copia física de los backups.
  - Sitio recíproco: es un acuerdo con algún proveedor o empresa que de alguna forma tenga relación con la suya para establecer un sitio temporal en caso de una disrupción, se le llama recíproco pues el acuerdo es en ambas vías.

Consideraciones sobre backups y recuperación

- Sistemas de almacenamiento
  - Considere opciones de almacenamiento que tengan capacidad para mitigar riesgos y procedimientos de recuperación entre sus características.
  - Por ejemplo:
    - Servidores con sistema de arreglo de discos
    - Discos de repuesto (instalados y no instalados)
    - SAN
    - NAS
    - Protocoles de datos distribuidos
    - Backup automático
    - Contrato de reemplazo de partes

Consideraciones sobre backups y recuperación

- Soluciones para desktops
  - Normalmente se suele no tomar en cuenta los equipos de usuarios, en parte porque puede ser más costoso tener soluciones de mitigación de pérdida de datos y recuperación.
  - Sin embargo, algunos usuarios podrían tener información incluso más sensible que la almacenada en un servidor.
  - Idealmente debería tener una réplica de todos los datos almacenados en un equipo de escritorio, pero los usuarios suelen realizar acciones fuera de lo establecido que hacen de esto una tarea muy complicada.
  - Algunas opciones pueden ser:
    - Apuntar el directorio My Documents a un servidor
    - Utilizar soluciones de nube que repliquen archivos automáticamente
    - Soluciones de backup para sistemas de usuario
    - Equipos virtuales
  - En todo caso deberá identificar los equipos más importantes según la criticidad de los datos que se manejan en ellos.
  - No olvide que estos equipos pueden ser robados por lo que debe preocuparse por asegurar los datos para que estos no puedan ser leídos por personas no autorizadas.

Consideraciones sobre backups y recuperación

- Licenciamiento y software
  - También debe considerar tener un backup de los instaladores del software (SO, Office, servidor de base de datos, CRM, etc.) así como sus respectivas licencias.
  - Aunque hoy en día las licencias suelen estar en línea, aún existen licencias físicas ya sea por medio de códigos o dispositivos de hardware.
  - Tome en cuenta también las contraseñas asociadas a los servicios que se van a instalar, así como de las licencias si estas se encuentran en línea.
  - Además, cuando se habla de licenciamiento no olvide que tendrá que mantener tanto las licencias del sitio primario como el o los sitios alternos.
  - Por último, la configuración necesaria para que los servicios funcionen correctamente también deben mantenerse seguros, en algunos casos es necesario guardar un archivo de configuración o identificar settins específicos que deben cambiarse para que algún servicio funcione correctamente.
    - La configuración de seguridad puede pasarse por alto en el proceso de recuperación así que no olvide, no solo tener la configuración respaldada, sino establecer procesos que eviten el olvidarse de esto.