UNIVERSIDAD
DE ANTIOQUIA

1 8 0 3

Julio Mario Monterrosa Paternina

c.c 1038123206

Fundamentos de sistemas

Taller de gestión de riesgos en sistema de información

21. mayo de 2021

Caucasia – Antioquia.

Nota: este documento no sigue los estándares de los informes escritos como APA u otras, porque en pro de mejorar la visualización del cuadro, el tamaño de esta página será casi el límite de tamaño de hoja de Word lo cual no cumple con dichos estándares.

Id Riesgo	riesgo	causa	evento que dispara el riesgo	probabilidad de ocurrencia	impacto en caso de que se materializa el riesgo ¿Cuál es el daño?	clase de riesgo (muy alto, alto, medio, bajo)	plan de mitigación para evitar que se presente el riesgo	plan de contingencia en caso de que ya sea inminente el riesgo	rehabilitación y construcción
0	perdida de datos.	no existe un backup de respaldo del datacenter ni se usa cloud computing.	cualquier eventualidad que pueda dañar la integridad física del datacenter como un terremoto.	probabilidad nunca inexistente: (0,100]%	perdida de información y datos en general; perdida del trabajo realizado alojado en los servidores; pérdidas económicas a futuro; clientes descontentos.	muy alto	usar cloud computing para tener la información segura en la nube; invertir en servidores de backup que funcionen como respaldo de la información y tenerlos en un lugar alejado de los servidores principales; proteger físicamente al datacenter acogiéndose a estándares cuya finalidad sea proteger la integridad física del datacenter ante una subida de voltaje causada por un rayo o por sismos por ejemplo.	pocas amenazas son contenibles: si la amenaza es por alto voltaje ya sea por tormenta eléctrica inminente o daño en la red eléctrica inminente, entonces se pude apagar y/o desconectar el datacenter lo que significaría un funcionamiento parcial de los servicios ofrecidos; Otras amenazas que pongan en riesgo la integridad del datacenter son prácticamente incontenibles, un terremoto, una inundación por alguna razón, un incendio, etc.	dependiendo de qué tan valiosa sea la información alojada en los servidores afectados del datacenter, se puede plantear la recuperación de la información extrayéndola de los discos duros mediante métodos de recuperación de información si es que los servidores utilizan tal medio de almacenamiento u otros medios de recuperación dependiendo del hardware; se tiene que invertir en más servidores y/o equipo de cómputo para suplir a los que resultaron dañados; reparación de daños generales en el datacenter.
1	seguir con pobres resultados de negocio.	el nuevo jefe tecnológico no tiene experiencia en el sector de sistemas de información.	una mala decisión o un mal procedimiento de parte de dicho activo por falta de conocimientos y experiencia para ocupar tal cargo.	[50,100]%	baja tasa de proyectos entregados y terminados a tiempo, con el presupuesto estipulado y de acuerdo con las especificaciones de los clientes; pérdidas económicas a futuro; pérdida de clientes; baja reputación de la empresa.	alto	capacitar al activo es una opción que lleva tiempo y costo a la empresa también esfuerzo por parte de él, se puede buscar un reemplazo con la experiencia y el conocimiento pertinente y poner al activo en otra área o despedirlo.	si este riesgo es inminente es porque al activo no se le puede reemplazar por alguna razón. Personas interesadas en el buen resultado del negocio y la empresa podrían influir en las decisiones del activo y hacer costumbre reuniones con él en cada proyecto para intentar tomar las mejores decisiones y acciones.	si el daño está hecho, es decir, si el activo siguió en el cargo y llevó a la empresa a pobres resultados nuevamente, se puede hacer lo descrito en el plan de contingencia, que ya no sería para contener el riesgo pero si mejoraría los resultados, también con el tiempo al activo se le podría capacitar y mejoraría los resultados a futuro tras cada proyecto; pasarlo a otro cargo o despedirlo también es una medida para enmendar el daño.
2	negocio no rentable por costos de operación excesivamente altos.	la adición de nuevos y diferentes sistemas de información que requieren de más conocimientos, activos y mantenimiento.	el servicio que ofrecen es una mezcla entre S.I. de terceros y propios, cada sistema de información que poseen requiere personal experto, mantenimiento y conocimientos, y todo ello conlleva un costo y tiempo.	[90,100]%	pérdidas económicas, recorte de personal por daños económicos en la empresa, reducción del número de proyectos en desarrollo simultaneo y reducción del número de proyectos por año debido al recorte de personal.	muy alto	centrarse en uno o pocos S.I. para los servicios que ofrecen que requieren S.I. de terceros, buscando S.I. individuales que sean capaces de llevar a cabo las funciones de todos o varios de los S.I. que poseen actualmente y así minimizar en número de S.I. y proveedores que requieren para ofrecer sus servicios; para los S.I. propios, incluir las funciones de dichos S.I. como criterios de aceptación de las capacidades de los nuevos S.I. de terceros e integrar y/o adaptar el flujo de trabajo a estos últimos; si la empresa insiste en desarrollar S.I propios, podrían invertir tiempo, dinero y esfuerzo en mejorarlos y usar temporalmente S.I. para cubrir el trabajo de los S.I propios que están siendo mejorados de tal manera que los S.I propios funcionen de la manera más unificada posible con los de terceros que ahora serán pocos; identificar procesos repetitivos que sean automatizables para usar RPA y ahorrar en costos en los diferentes S.I.	cuando la empresa dependa de un gran número de S.I. para ofrecer sus servicios y los costos de operación sean excesivamente e 'irremediablemente' altos, también se puede empezar hacer lo descrito en el plan de mitigación mientras el negocio aún es rentable, una vez se pasa el límite en el que el negocio ya no es rentable, la solvencia económica pasaría a manos de las personas interesadas en la rentabilidad el negocio y tendrían que poner empeño en resolver los problemas económicos mientras el plan de mitigación que ahora se ha vuelto de contingencia se lleve a cabo, si estas personas no son capaces de solventar el problema económico la empresa quebraría irremediablemente.	nuevamente aplica el plan de contingencia en este punto ya que el problema es económico; también podrían reinventarse ofreciendo otros productos de S.I. evitando los errores que llevaron a la empresa a tal situación.
3	fallos y caídas frecuentes en los sistemas de información y la disponibilidad de los distintos servicios para los clientes tecnológicos.	la empresa tiene una arquitectura de red de almacenamiento no óptima para los servicios que ofrecen, desconocen el tema de las SAN, no se usa cloud computing.	cualquier fallo principalmente de software en los servidores del único datacenter de la empresa.	[50,100]%	descontento del cliente tecnológico por servicios mejorables; pérdida de clientes; pérdidas económicas; mala reputación en los servicios de la empresa; gasto continuo en solucionar errores en los servidores y el datacenter.	alto	optar por usar cloud computing para el total o parcial de datos alojados en su datacenter, lo cual ofrecería un plus en seguridad e integridad de la información; usar SAN como arquitectura de red de almacenamiento para blindarse contra errores, mejorar la latencia en los servicios y minimizar el desperdicio de tiempo y recursos en operaciones críticas como respaldo y restauración de datos de cada uno de los servidores.	además de empezar a integrar y usar las tecnologías descritas en el plan de mitigación, el personal de IT deberá solucionar los problemas en el datacenter que causan las frecuentes caídas y fallos de sistemas, la empresa deberá contratar más personal capacitado con experiencia para el equipo del personal de IT y así tener más personal para trabajar en más y más fallos y hacerle frente al riesgo materializado.	una vez este riesgo se halla materializado y el servicio ofrecido por la empresa dé qué desear, quedará en manos de la empresa y/o las personas interesadas en el funcionamiento óptimo de los servicios que se prestan en invertir para mejorar sus tecnologías y arquitectura de red nuevamente usando las tecnologías descritas en el plan de mitigación, disponer de más personal de IT mientras las nuevas tecnologías son adaptadas, acogidas y usadas para mitigar la gran cantidad de errores, fallos y caídas.

Recuerde que puede ver este documento y la versión en Excel del cuadro bajo el nombre de ‘taller gestion del riesgo JulioMonterrosa.pdf’ y ‘taller gestión del riesgo JulioMonterrosa.xlsx’ respectivamente en el siguiente repositorio en la carpeta documentos: https://github.com/JulioMarioUdeA/FundamentosDeSistemas