Caso Individual #1

A continuación, se presenta el siguiente caso:

Una empresa dedicada a la venta de seguros, cuya misión es "Brindar servicios de seguros en forma excelente, eficiente, competitiva, rentable y con responsabilidad social, atendiendo las demandas de los clientes, usuarios e intermediarios; tanto en el mercado local como regional; promoviendo la prevención en la ocurrencia de siniestros" cuenta con una estructura organizativa compuesta por una Junta Directiva formada por 5 personas, una Presidencia Ejecutiva, una Vicepresidencia Ejecutiva, una Gerencia General con tres Subgerencias Generales, dentro de una de las cuales se ubica la Dirección de Informática. En la empresa de seguros en mención las decisiones estratégicas en materia de TI son tomadas por la Subgerencia General a la que pertenece, cuyo líder no conoce absolutamente nada de tecnología, pero tiene mucho poder de decisión y convencimiento sobre su Gerente superior, por lo que no existen mecanismos para la rendición de cuentas adecuados. Otras decisiones de carácter más operativo son tomadas por el Director de Informática, sin embargo, algunas de esas decisiones no han sido las mejores y esto se ha traducido en pérdida y desaprovechamiento de recursos tecnológicos. Además, no existen mayores indicadores de desempeño que permitan tomar decisiones acertadas, no se ha pensado en la posibilidad de un plan de continuidad del negocio, ni mucho menos se tiene una hoja de ruta que señale hacia dónde enfocar los recursos tecnológicos de la empresa. El área de TI ejecuta una serie de procesos de negocio que, en teoría, deberían coadyuvar al negocio al cumplimiento de sus objetivos; sin embargo, las jerarquías de la empresa no tienen idea de lo que la palabra riesgo significa y nunca se han sentado a pensar en las posibles situaciones que podrían poner en peligro esos objetivos estratégicos del negocio en un mundo globalizado y competitivo como el nuestro. El Director de Informática alega que sus esfuerzos se concentran en darle mantenimiento a la plataforma actual, pero que "no puede estar en todo" y que, por lo tanto, no tiene tiempo de pensar más allá de esto. La empresa se mantiene en operación, pero con una bomba de tiempo en sus espaldas si continúa trabajando bajo la situación descrita anteriormente.

Con base en lo anterior:

Usted ha sido contratado como consultor en riesgos para esta empresa de seguros y debe responder claramente las siguientes interrogantes:

a) ¿Por qué es fundamental establecer un ERM dentro de esta empresa?

Establecer un ERM es importante ya que la empresa está tomando decisiones importantes sin pensar en los riesgos, especialmente en tecnología. Actualmente, las personas encargadas en tomar decisiones no tienen los conocimientos necesarios para evaluar los riesgos tecnológicos, y eso pone en peligro a la empresa. Si no controlan esos riesgos podrían causar pérdidas o incluso detener las operaciones en la empresa por lo tanto un ERM ayudaría a identificar esos riesgos antes de que se conviertan en un problema.

b) ¿De qué forma se deberían aplicar los seis principios de la gestión de riesgos de TI en esta empresa?

Para que la gestión de riesgos en TI funcione bien, es esencial que las decisiones tecnológicas estén en sintonía con los objetivos de la empresa. La tecnología no solo debe ser vista como un gasto, sino como una herramienta valiosa para alcanzar las metas de la empresa. También necesitamos estar evaluando los riesgos de manera constante, no solo cuando algo sale mal, y basar nuestras decisiones en datos concretos a través de indicadores de desempeño. Además, es clave que todos sepan quién se encarga de qué en el área de TI, para evitar que personas sin conocimientos técnicos tomen decisiones importantes. También debemos tener un plan de continuidad del negocio, así estaremos listos para enfrentar cualquier emergencia que pueda surgir. Por último, la comunicación sobre los riesgos es fundamental; todos en la empresa, desde los directores hasta el personal de TI, deben conocer los riesgos y cómo manejarlos, porque no se puede subestimar el impacto que la tecnología puede tener en nuestro negocio.

c) ¿Cuál estándar o sana práctica del mercado se debe usar en este caso que permita enfocarse en los objetivos de los procesos de TI? Señale cuáles actividades se deberán ejecutar según la sana práctica seleccionada.

El estándar más adecuado en este caso sería **COBIT** (Control Objectives for Information and Related Technologies), porque está enfocado en ayudar a que los procesos de TI se alineen con los objetivos del negocio.

Actividades clave que se deberían ejecutar:

1. **Definir los objetivos de TI**: Identificar qué se espera de la tecnología dentro de la empresa.
2. **Evaluar los riesgos tecnológicos**: Hacer un análisis detallado de los riesgos que existen actualmente.
3. **Monitorear y reportar el desempeño**: Establecer indicadores para saber si la tecnología está cumpliendo con su función.
4. **Establecer controles**: Crear procesos que aseguren que los recursos tecnológicos sean utilizados de forma eficiente y controlada.

d) Defina la escala para la evaluación, así como el apetito del riesgo que deberá usar esta empresa en su gestión. Justifique su respuesta.

La escala para evaluar los riesgos será de cinco niveles:

1. **Muy bajo**.
2. **Bajo**.
3. **Moderado**.
4. **Alto**.
5. **Muy alto.**

El apetito de riesgo tiene que ser moderado. Esto significa que la empresa no puede permitirse grandes riesgos, porque su funcionamiento depende de la tecnología, y los errores graves en TI pueden detener las operaciones o causar grandes pérdidas. Sin embargo, tampoco debe ser extremadamente conservadora, porque la tecnología avanza rápido y la empresa debe poder adaptarse.