10 consejos para aplicar BI de manera acertada

 El costo de un proyecto de Business Intelligence (BI) va mucho más allá del precio de compra. El tiempo dedicado a la investigación, la ejecución y el mantenimiento de una inversión de BI puede expandirse rápidamente y los errores son a menudo costosos. De modo que propongo 10 consejos y aspectos a tener en cuenta a la hora de implantar un sistema BI en un empresa:

1. **Dar prioridad a tus objetivos:** Algunas plataformas de BI son gratis, pero esto a costa de un gran esfuerzo y tiempo para la implementación. Sin embargo, otras plataformas de pago se instalan y ejecutan en una semana. Es importante saber cuáles son la prioridades.
2. **Reconocer los criterios de selección no negociables:** Incluso antes de empezar a buscar entre varias soluciones, decidir cuáles son los «must» de la solución y cuales los «deseados».
3. **Utilizar las herramientas de análisis integrados en la solución:** Optar por las aplicaciones de análisis integradas en vez de acumular varias aplicaciones ya que estos cuadros de mando proporcionan herramientas simples y datos procesables con una personalización mínima.
4. **La calidad de los datos:** Normalizar los datos antes de implementar ahorra tiempo porque en la fase de implementación se convertirá en una tarea mucho más pesada. Por otra parte, el nivel de confianza y la fidelidad de los datos utilizados para la toma de decisiones es un factor crítico de éxito del proyecto.
5. **Identificar los factores clave de antemano:** Antes de implementar BI, decidir qué datos se necesitan y en qué formato, en busca de una solución tecnológica que puede proporcionar datos coherentes con el análisis. Antes de empezar, es importante saber lo que se está buscando.
6. **Partir de pequeños proyectos piloto:** Enfocar su aplicación BI de uno o dos objetivos de negocio iniciales. Esto va a acelerar la implementación permitiendo al equipo trabajar concentrando sus esfuerzos, sin ser abrumados por conseguir los resultados de docenas de objetivos de negocio. Una vez que el despliegue inicial se ha completado se pueden agregar objetivos adicionales.
7. **No abandonar los procesos actualmente eficaces sin razón:** Evaluar qué herramientas y características son realmente importantes en su negocio y asegurarse de que todo el equipo de trabajo está utilizando sólo las que se han elegido. Esto es para evitar que algunos miembros del equipo

incluyan la información no pertinente en estos sistemas.

8. **La tecnología debe estar a su servicio, no al contrario:** Alinear las actividades de implementación con la estrategia de negocio: extraer sólo la información relevante para el negocio y sólo cuando sea necesario.
9. **Hacer la vida más sencilla para los usuarios finales:** Simplificar la herramientas y la infraestructura: proporcionar a los usuarios la capacidad de crear, editar y filtrar la información para cumplir con las necesidades. Los instrumentos muy complejos privan al usuario la capacidad de ser autosuficiente.
10. **Busque siempre un negocio más inteligente:** Tratar de profundizar en una mejor toma de decisiones en la empresa. Este paso sin ninguna inversión en BI es probable que tenga un impacto muy limitado.

ISO 27018: Cloud Computing

La certificación ISO 27018 publicada el 29 de Julio de 2014 , es un código de buenas prácticas en controles de protección de datos para servicios de computación en la nube. Esta norma se une a la anterior ISO / IEC 27001 e ISO / IEC 27002 en el ámbito de gestión de la seguridad de la información y que se dirige específicamente a los proveedores de servicios de nube.

El objetivo abiertamente perseguido por la norma es crear un conjunto de normas, procedimientos y controles a través de los cuales los proveedores de servicios en la nube que, en conformidad con la normativa europea en materia de privacidad, actúan como «procesadores de datos», puedan garantizar el cumplimiento de las obligaciones legales en materia de tratamiento de los datos personales. Al mismo tiempo proporciona a los consumidores potenciales de servicios cloud una herramienta comparativa útil para ejercer su derecho de verificar y auditar a los niveles de cumplimiento de las regulaciones establecidas por el proveedor.

Entre las medidas innovadoras recogidas por la norma ISO 27018 señalaría las siguientes:

- El proveedor, como responsable del tratamiento, tendrá que proporcionar las herramientas adecuadas para permitir y facilitar el

ejercicio por el interesado, de los derechos de acceso, rectificación y cancelación en relación con el tratamiento de los datos.

- En relación con los fines del tratamiento, el proveedor debe velar por el cumplimiento del tratamiento a los únicos usos descritos al cliente en el momento de la contratación del servicio, en particular garantizando que los datos no serán utilizados para fines distintos de los especificados por el cliente, ni para el propósito de marketing directo o publicitario, a menos que haya consentimiento explícito, consenso de que, en cualquier caso, nunca será un requisito establecido por el proveedor para la función del servicio.
- Salvo que exista una prohibición establecida por la ley, la solicitud de divulgación de los datos personales por parte de las autoridades administrativas o judiciales será notificada sin demora al consumidor de servicios de nube.
- En cuanto al tema de la subcontratación, la norma establece, de forma particularmente incisiva, el derecho del cliente a conocer, incluso antes de empezar a utilizar el servicio, toda la cadena de los subcontratistas, los países en los que se establecen, la ubicación de los data centers utilizados por ellos y sus obligaciones en relación con el tratamiento de los datos. También se reconoce el derecho del cliente a oponerse a eventuales cambios en la cadena de los subcontratistas, o de rescindir del contrato.
- El proveedor deberá notificar inmediatamente al cliente toda violación de los datos personales de los que derivan de una pérdida, destrucción, alteración, divulgación o acceso no autorizado, con el fin de permitir que el propietario y los interesados lo□□ notifiquen a las autoridades de control en los plazos establecidos por la ley.
- El acuerdo de servicio debe establecer una política de traslado que detalla el método de restitución, transferencia y / o cancelación de sus datos en poder del proveedor en el cese de los efectos de dicho contrato.
- En relación con las medidas de seguridad de la información, sería conveniente que todo el personal del proveedor y de los subcontratistas estuviese vinculado a un acuerdo de confidencialidad, recibiese una formación adecuada, accediesen a los datos mediante operaciones de autentificación y login.

Seguridad en la Nube. ¿Cómo mitigar

los riesgos?

Me gustaría empezar con la definición de la computación en la nube según el Instituto Nacional de Estándares y Tecnología: » La computación en nube es un modelo para permitir a conveniencia, acceso a la red bajo demanda a un conjunto compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente suministrados y liberados con un esfuerzo de gestión o interacción con el proveedor de servicios mínimo». Otras organizaciones adoptan un enfoque más simple y definen la computación en nube como servidores virtuales disponibles en Internet. Independientemente de la definición, la computación en la nube es un fenómeno que sigue creciendo en popularidad en el mundo de los negocios.

Considero que las ventajas de la computación en nube son innegables. La tecnología cloud ofrece una mayor flexibilidad, permitiendo a los usuarios disfrutar de una mayor movilidad, proporciona a las organizaciones un mayor almacenamiento y reduce la carga de los departamentos de TI que utilizan sistemas informáticos convencionales. Son estas necesidades y la conveniencia de subcontratar estos requisitos lo que sigue marcando el creciente uso de la computación en nube. Sin embargo, ninguna tecnología está libre de posibles complicaciones. Como las organizaciones están recurriendo cada vez más a la computación en la nube, los riesgos asociados con el uso de esta son cada vez más claros, de los cuales el más importante es la seguridad.

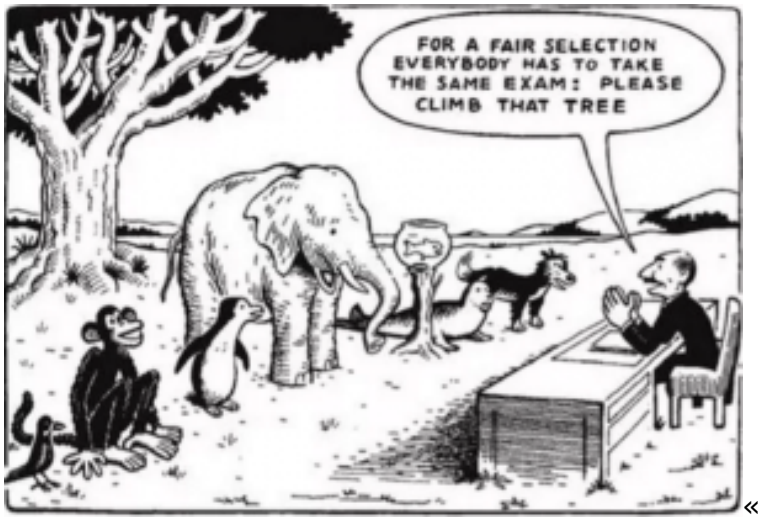
Los riesgos asociados con el uso de la computación en la nube dependen de varios factores tales como el tipo de actividad, la cantidad de datos en la subcontratación y el proveedor de servicio seleccionado. Sin embargo, siempre que se utilizan soluciones cloud el seguir estas estrategias permite mitigar el riesgo en cuanto a la seguridad:

- **Investigar y analizar las soluciones cloud:** Cuando tu empresa pretende migrar parte de su hardware y software a la nube, necesitas informarte sobre los potenciales proveedores. Esto incluye examinar el historial de seguridad del proveedor, la comprobación de referencias, la comprobación de vulnerabilidades de seguridad conocidas, y asegurarse de que el contrato con ellos incluye prácticas de seguridad proactivas por su

parte.

- **Utilizar una solución Single Sign-on(SSO) para añadir seguridad:** Dependiendo del tamaño de la organización, se podría dar el caso de estar creando muchas cuentas de usuario para diferentes servicios en la nube. Un usuario puede tener varias cuentas y contraseñas, lo que hace que sea más complicado para el usuario y el administrador. Reduciéndolo a un entorno de inicio de sesión único, se reduce el número de posibles debilidades de seguridad.
- **Trabajar con un tercero para asegurar seguridad en la nube de forma regular**: Por lo general, tener múltiples proveedores aumenta los riesgos de seguridad y las pequeñas y medianas empresas sin grandes departamentos de TI a veces necesitan ayuda para auditar y garantizar la seguridad en la nube. Es importante contratar las auditorias de terceros para asegurarse de que su proveedor de la nube está siguiendo las normas de seguridad.
- **Implementar el cifrado end-to-end:** El cifrado end-to-end, en particular para el almacenamiento en la nube, disminuye la probabilidad de que sus datos sean violados. La mayoría de las soluciones de almacenamiento en la nube han cifrado la carga y descarga de datos, pero no el almacenamiento. El método con menos riesgo requiere que sus datos sean encriptados antes de subir, mientras están almacenados por el proveedor, y que sólo se puedan descifrar con una clave de cifrado única.
- **Actualizar regularmente su software:** No hay que descuidar el software cuando se migre a la nube. Si se están ejecutando sistemas operativos obsoletos como Windows XP y navegadores obsoletos como IE 7, se podría estar en riesgo a pesar del cifrado y las auditorias de terceros.

Céntrate en tus fortalezas, no en tus debilidades



«Todos somos unos genios. Pero si juzgas a un pez por su habilidad de escalar un árbol, vivirá su vida entera creyendo que es estúpido.»

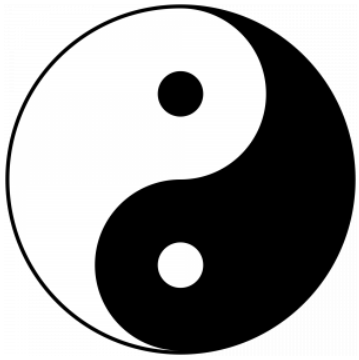
Es muy probable que ya hayáis oído esta frase de Einstein y visto la imagen de la izquierda antes en alguna parte, probablemente juntas. Esto es porque el mensaje que tienen detrás es el mismo.

Vivimos en una sociedad que está enfocada en penalizar las debilidades en lugar de premiar las fortalezas. Por ejemplo, sin un estudiante tiene malas notas en matemáticas y sobresalientes en música, ¿qué crees que le espera al chaval? Lo más seguro es que inmediatamente se le apunte a clases particulares de matemáticas para mejorar esas notas que no son lo suficientemente buenas. Sin embargo, si en vez de esto, a ese mismo chaval se le inscribe en una escuela de música, algún día podría llegar a ser un virtuoso de la música. Quién sabe cuántos Mozart nos habremos perdido así.

Desde mi punto de vista, es necesario centrarse y potenciar las fortalezas y dejar las debilidades en un segundo plano. Eso sí, los extremos nunca son buenos (demasiado al Este es Oeste) y cuando digo que hay que dejar las debilidades en un segundo plano no me refiero a que haya que olvidarse de ellas. Es necesario tener unos mínimos y si se tiene la oportunidad de mejorar uno de tus puntos débiles siempre va a ser algo positivo. Pero no considero que ese sea el objetivo a perseguir. Si mejoras tus debilidades a lo máximo que podrás aspirar es a ser mediocre en todo, mientras que potenciando tus fortalezas puedes alcanzar la excelencia en esos ámbitos.

Se me ocurren tres razones por las que apostar por tus fortalezas pero seguro que hay muchas más. Las razones son la siguientes:

- Trabajar en cosas en las que no eres bueno resulta frustrante y te roba la energía. Por el contrario, trabajar en lo que se es bueno te motiva y te llena de energía.
- Tienes recursos limitados. El tiempo que dedicas a mejorar una debilidad va a ser elevado para lograr un escaso resultado, mientras que el mismo tiempo invertido en una fortaleza multiplicará esos resultados.
- Mejorarás en las tareas que te gustan hacer y podrán verte como un experto en una de tus facetas clave y como una persona que aporta nuevas ideas.



Esto sirve tanto en el mundo de la empresa como en la vida en general y no hay que tener miedo a ser débil en ciertas cosas, siempre y cuando analicemos y conozcamos bien estos puntos débiles. Por ejemplo, en el caso de una empresa, si se conoce un punto en el que es débil se puede contratar personas que cubran estas debilidades. Aunque suene un poco a frase de maestro de

artes marciales, siempre se debe buscar un Yin para tu Yang, alguien que supla tus debilidades con sus fortalezas. Lo mejor para sacar el máximo rendimiento de un equipo es que cada uno 'juegue sus cartas', que hagan lo que saben hacer.

Para ello lo primero de todo es conocernos bien y tener claro cuáles son nuestras fortalezas, aquello que nos gusta hacer y en lo que somos buenos. Una manera para saber cuáles son nuestras fortalezas innatas es haciéndonos preguntas a nosotros mismos:

- ¿Cuál ha sido el mayor éxito que he tenido?
- ¿Cuál ha sido el mejor día de mi vida?¿Qué estaba haciendo?
- ¿Cuál era mi asignatura favorita en la escuela?¿Qué parte era la que más me gustaba?
- ¿Qué es por lo que me suelen alabar los demás?
- ¿Qué actividades me dan energía?¿Con qué actividad pierdo la noción del tiempo?

Estas son algunas preguntas que te ayudarán a conocer qué es lo que te gusta hacer y en las que eres bueno. Una vez lo sabes, adelante, potencia estas fortalezas que te hacen destacar, nadie mejor que tú sabe cuáles son y llena tu vida de tareas que estén en línea con tus fortalezas, con tus conocimientos y tus gustos.

«Elige un trabajo que ames y no trabajarás un día más de tu vida»

El modelo híbrido

Tras leer un artículo que me recomendó Rebeca, que trata sobre cuáles son las principales ventajas que tiene el tener los datos en servidores propios frente a tenerlos en la nube, tengo más claro que nunca que la opción acertada es optar por un modelo híbrido.

El apostar por una tecnología cloud se puede hacer por muchas y diferentes razones y quienes la usan se benefician de sus ventajas, como tener mayor agilidad, menores costes o lograr un alcance global entre otras. Pero para muchos CIO lo que realmente permite es reducir los recursos de áreas que no aportan al negocio hacia otras que si lo hacen. Dicho de otra forma, dejar de lado el trabajo engorroso de mantener una infraestructura y que no diferencia a una empresa de su competencia, para centrarse en los productos y servicios por los que una empresa es conocida.

Esto es lógico ya que al dejar ciertos servicios en manos de terceros nos permite centrarnos en la actividades que más aportan a nuestro negocio. Pero esto genera un debate, ¿Están seguros mis datos en la nube?¿Estoy ganando efectividad a costa de perder seguridad?

Las principales preocupaciones de las empresas se centran en aspectos de la gestión de los datos, fundamentalmente en la propiedad de los mismos y la forma de operarlos y tratarlos por parte de los proveedores, así como en la identificación y control de acceso a los recursos. Esta preocupación es natural al no controlar uno todo y depender de terceras partes, más aún si cabe cuando se ven escándalos de miles de datos robados en la nube como fueron los casos de Dropbox y iCloud.

Desde mi punto de vista, estos robos masivos de datos se seguirán perpetuando pero cada vez con menor frecuencia. La razón por la que considero que la nube era más propensa a fallos de seguridad de lo que es ahora es por el hecho de que durante años la tecnología de cloud computing ha evolucionado más rápido de lo que la seguridad en la nube lo podía hacer. Sin embargo, creo que esta diferencia se está acortando con el tiempo. Cada vez son más las herramientas de seguridad y las arquitecturas que se desarrollan para proteger la nube y que se estandarizaran para todas las empresas. Puede que en muchos aspectos el nivel de seguridad que te puede proporcionar un proveedor de cloud supere al nivel de seguridad que la mayoría de empresas puede garantizar de sus datos. Y si no, tiempo al tiempo.

Sin embargo, hay varios aspectos en los que es necesario contar con servidores propios y las razones se explican claramente en el artículo que he mencionado al principio. Las razones son básicamente estas seis:

- **Reglamento:** Dependiendo del sector, del mercado o de la localización geográfica es posible que se tengan ciertas regulaciones por parte del

gobierno sobre cómo almacenar y hacer uso de datos sensibles. Esto en algunos casos obliga a tener los datos en centros de datos privados.

- **Seguridad:** A pesar de que la nube sea bastante segura, puede haber casos en los que la empresa necesite una seguridad más fuerte para unos determinados datos.
- **Visibilidad:** Saber donde se encuentran realmente los datos almacenados en la nube resulta complicado.
- **Accesibilidad:** En un mundo perfecto todas las empresas tendrían un ancho de banda lo suficientemente alto y un acceso sin restricciones en todo momento al proveedor de cloud, pero la realidad no es así.
- **Latencia:** Si lo que se necesita es que el acceso a los datos tenga una latencia baja y predecible, como en el caso de repositorios de audio y vídeo, es más fácil de manejar en servidores locales.
- **Falta de confianza:** Es necesario tener en cuenta que a lo largo de la relación con el proveedor de cloud se puede tener momentos en los que se pierda la confianza en este. Para esos momentos es importante contar con servidores privados.

Como conclusión me quedo con lo dicho al principio del post, la mejor opción pasa por el modelo híbrido. De este modo aprovechar al máximo las ventajas de uno y de otro. Para las aplicaciones e información crítica del negocio aprovechar la confianza y la consistencia que da el tener servidores propios y para los datos de bajo impacto y fácil transición hacer uso de las ventajas de la nube.

Unknown unknowns

«There are known knowns. There are things we know we know. We also know there are known unknowns. That is to

say, we know there are some things we do not know. But there are also unknown unknowns, the ones we don’t know we don’t know»

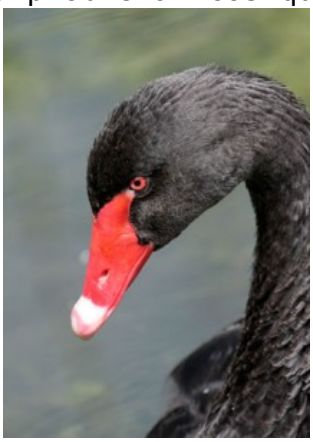
O dicho en castellano:

«Las informaciones que dicen que algo no ha pasado siempre me resultan interesantes. Hay cosas que sabemos que sabemos. También hay cosas desconocidas conocidas, es decir que sabemos que hay algunas cosas que no sabemos. Pero también hay cosas desconocidas que desconocemos, las que no sabemos que no sabemos»

Esta frase la dijo el secretario de defensa de los Estados Unidos Donald Rumsfeld. A pesar de que fue ridiculizado por esta especie de trabalenguas(a mí personalmente me gusta más en inglés ya que es aún más complicado de decir), yo no podría estar más de acuerdo con esta reflexión. Los que estamos en el mundo de la informática nos encontramos a diario con estos tres tipos de riesgos, pero los más peligrosos son sin duda los **«unknown unknowns».**

Cuando una tecnología lleva tiempo en el mercado y ,por tanto, es estable, por lo general, se conocen los riesgos que esta conlleva y los problemas que puede acarrear. Para evitar o al menos disminuir la probabilidad de estos riesgos, las empresas pueden tomar medidas y controles ya que estos riesgos están correctamente definidos y medidos.

Por otra parte están los riesgos desconocidos que son conocidos, es decir, los riesgos que son conocidos pero no han sido o no pueden ser correctamente identificados o medidos. Un ejemplo claro de estos es que como desarrolladores sabemos que el cliente puede cambiar de idea, pero no sabemos cuándo y en qué casos. Estos riesgos son más problemáticos que los primeros pero se pueden controlar con ciertas medidas.

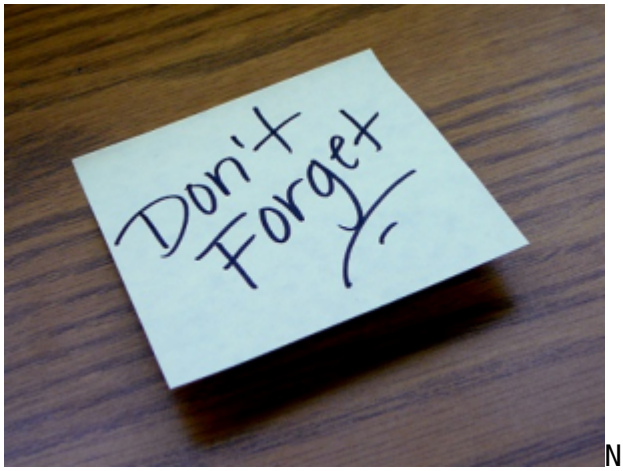


Sin embargo, hay riesgos que pueden ser desastrosos para nuestro negocio y ni siquiera sepamos de la existencia de estos riesgos. Y lo que es más, es posible incluso que nuestro negocio ya esté sufriendo las consecuencias de este riesgo y no seamos conscientes de ello. Podemos estar pensando que nada falla o puede fallar mientras ya está ocurriendo. Por alusión metafórica se les suele llamar **cisnes negros** a estos sucesos que reúnen tres atributos: constituyen una rareza, pueden generar consecuencias extremas y son imprevisibles.

Resulta inquietante el pensar que puede haber algo que pueda acabar con nuestro negocio y no pueda ser controlado. La pregunta que se me plantea es

¿Cómo te preparas para algo que ni siquiera sabes que te tienes que preparar?

Planificación a medio plazo, la gran olvidada



Normalmente asociamos la planificación estratégica al mundo de las empresas y de directivos con altos cargos y grandes despachos. La realidad es distinta. La planificación estratégica la debe emplear cualquier persona en su vida cotidiana. Puedes pensar que ya lo haces, y hasta cierto punto es así, pero probablemente no del modo correcto.

Desde mi punto de vista, las personas tendemos a planificar a corto y a largo plazo, es decir, lo que vamos a hacer los próximos días (ej. El martes me voy a apuntar a una academia de inglés) y lo que se pretende conseguir en un periodo de uno o dos años (ej. En dos años vivir en Estados Unidos). La planificación a medio plazo suele ser la gran olvidada en estos casos y, tal y como yo lo veo, es muy importante planificarse a medio plazo. ¿Por qué? si ya se los que hacer los próximos días y lo que quiero alcanzar en unos años, ¿para qué tengo que planificar a medio plazo?

Mi respuesta es que si uno no planifica en vista a dos, tres o hasta cinco meses corre el riesgo de ir en la dirección equivocada hacia sus objetivos a largo plazo o incluso estancarse. Es más, bajo mi punto de vista es muy complicado conseguir fijar objetivos de gran valor a corto plazo, mientras que a medio plazo se pueden fijar objetivos medibles de un alcance importante y dirigirlos hacia un objetivo mayor (ej. En cinco meses me voy a sacar el First Certificate). De este modo, los objetivos fijados a largo plazo que inicialmente parecían inalcanzables van cogiendo forma y cada vez se ve más posible el alcanzarlos y de este modo nos motivan a seguir adelante.

Como conclusión, es importante que planifiquemos en nuestra vida diaria, desde un plazo corto hasta un plazo largo, sin olvidarnos nunca del plazo medio. Este último nos marcará los objetivos para alcanzar metas mayores y nos proporcionará un contexto en el que actuar.