Decisiones en proyectos TI
aspectos claves para tener en cuenta

Gentileza Alfredo Cofré E.

Este artículo aborda en detalle tres aspectos relevantes al momento de tomar decisiones en proyectos TI, que en general son subestimados o simplemente descartados.

Jens Hardings
Profesor Asistente del Departamento de Ciencia de la Computación, P. Universidad Católica de Chile. Ingeniero Civil en Computación, Universidad de Chile. Doctor en Ciencias mención Computación, Universidad de Chile.
jhp@ing.puc.cl

EVALUACIÓN CUANTITATIVA VS CUALITATIVA

En muchas ocasiones las decisiones estratégicas en proyectos TI son tomadas por razones comerciales. Abarcar mayor mercado, tener mayor cantidad de público lo más cautivo posible o generar economías importantes en la implantación de un proyecto son aspectos que justifican decisiones que afectan significativamente el impacto que puede tener éste. En la mayor parte de los casos está bien que se tomen esas decisiones, porque apuntan a cumplir con el objetivo que se ha impuesto para el proyecto.

Sin embargo, la cantidad de veces que una cualidad técnica puede justificar decisiones comparables es mucho más baja, sobre todo cuando no es directamente traducible a una característica comercial tal como precio, aumento de productividad, porción de mercado o algún otro indicador objetivo y cuantificable. Es ahí donde creo que hay un punto importante: preferimos tener datos cuantificables que se puedan comparar directamente y las características comerciales de los proyectos tienden a entregarnos ese tipo de datos. En cambio, aquellas características técnicas que nos entregan datos cualitativos nos generan problemas porque no los podemos comparar directamente.

Lo anterior no quiere decir que siempre tenga sentido comparar datos cuantitativos de orígenes diversos, pero al menos podemos comparar un número con otro, tomar una decisión (buena o mala) y continuar. En cambio, al tener datos cualitativos que no podemos traducir directamente a números, o vectores de números, sobre los cuales comparar y decidir si un costo X es justificado por la posibilidad de contar con la característica Y, se vuelve más complejo.

En ese punto, hay dos posibles caminos para tomar:

1. **Intentar realizar una traducción de los valores cualitativos a cuantitativos.**

2. **Aceptar que se debe realizar una apuesta, ya sea a favor o en contra, de la característica cualitativa y asumir los beneficios y costos que surjan a futuro.**

Asumiendo que se actúa de buena fe, la calidad de la decisión que se puede tomar por la vía de cualquiera de estos dos caminos es muy similar. Tenemos una tendencia de seguir el primero en desmedro del segundo, porque nos parece más riguroso y de menor incertidumbre.

Al seguir el primer camino, usamos herramientas como el Costo Total de Propiedad (Total Cost of Ownership, TCO), Retorno sobre la Inversión (Return on Investment, ROI) o para casos más específicos como la seguridad, el Retorno sobre la Inversión de Seguridad (Return on Security Investment, ROSI). Sin embargo, en algún momento debemos tomar decisiones subjetivas, inventar o asumir cifras a falta de información objetiva o simplificar el problema obviando aspectos que pueden luego demostrar ser muy relevantes. Por ejemplo, en el caso del ROSI es necesario estimar la efectividad de mitigación de un riesgo, frente a un futuro en el cual no podemos predecir el comportamiento de potenciales atacantes, cambios tecnológicos y otros elementos relevantes.

Al tomar estas decisiones y cuantificar en base a presunciones o predicciones, aumenta la incertidumbre de la evaluación. Sin embargo, esa incertidumbre no forma parte del resultado, que queremos sea un número limpio y puro, sin que nada nos moleste al momento de compararlo con otros.

Al final, podríamos acabar con una falsa sensación de objetividad, que aparenta ser mejor que el otro camino, el de la apuesta, que evidencia nuestra incertidumbre. Sería un error. Es mejor conocer las limitaciones de la evaluación que esconderla al interior de herramientas que pueden encapsular decisiones estratégicas relevantes. La incertidumbre debe quedar declarada, de lo contrario tenemos la tentación de asumir que la decisión se basa solamente en comparar dos valores numéricos.

> Es mejor conocer las limitaciones de la evaluación que esconderla al interior de herramientas que pueden encapsular decisiones estratégicas relevantes.

Es por ello que la propuesta es tomar lo mejor de ambos caminos. Intentar realizar una evaluación cuantitativa cuando ello tiene sentido y los datos son confiables, pero aceptando las incertidumbres y por ende la necesidad de realizar apuestas. Estas apuestas no deben quedar escondidas dentro de las herramientas de evaluación utilizadas, sino hacerse explícitas y tener un lugar de honor en el resumen ejecutivo que se haga sobre el resultado de la evaluación.

SEGURIDAD EN PROYECTOS TI

La seguridad en los proyectos TI, sean estos de infraestructura, desarrollo de software, integración o cualquier otro, sufren el mismo problema que los administradores de sistemas: cuando está bien hecho el trabajo, éste pasa desapercibido. La situación genera un estado permanente de disconformidad, porque cuando el trabajo pasa desapercibido produce molestia y desconfianza sobre el gasto que implica. Pero cuando es notorio, significa que no está funcionando adecuadamente.

Por lo mismo no es fácil vender proyectos de seguridad al interior de las organizaciones. Si bien existen herramientas que apuntan a cuantificar el beneficio de proyectos de seguridad, como el ROSI ya mencionado, estos no siempre terminan por convencer, salvo que se esté frente a un problema de seguridad serio, ya sea interno o de terceros. Y en muchos casos los costos de una seguridad mediocre no los sufre quien puede resolver el problema. El primer punto ha comenzado a cambiar lentamente, en principio por obligaciones legales o imponiendo certificaciones a proveedores.

Pero aún queda bastante camino por recorrer, para que la incorporación de los aspectos de seguridad en proyectos TI se masifique, más allá de las obligaciones externas y provenga de un análisis que arroje que es buen negocio invertir en seguridad.

Respecto del segundo punto, me parece que no se está haciendo lo suficiente, en particular por parte de las instituciones financieras que tienen bastante impacto en nuestra sociedad. Por ello, profundizo en dos ejemplos:

1. Seguridad en sitios web

Durante muchos años numerosos bancos en Chile han tenido la mala práctica, que algunos mantienen hasta hoy, que es publicar el formulario de autenticación donde se ingresan el RUT y la clave del cliente en páginas entregadas de manera no segura. Es decir, al momento de obtener el formulario, el cliente no tiene la certeza que éste procede efectivamente del banco y no de un impostor. Si efectivamente proviene del banco, la transacción que se genera al enviar las claves es segura y nunca son reveladas. Sin embargo, si el formulario es enviado por un impostor, éste puede generar una transacción hacia otro destino en lugar de una transacción segura con el banco. Y el usuario en el mejor de los casos se enteraría una vez enviada la información sensible y sólo si el impostor actúa de forma descuidada.

Como resultado de esta práctica, los usuarios finales han debido aprender a ignorar las buenas prácticas de seguridad, que dicen, entre otras, que no se deben ingresar informaciones secretas en formularios salvo que se pueda validar el origen. Habiendo aprendido esto, los usuarios cada vez son más proclives a caer en trampas de phishing (obtención de claves de acceso por parte de terceros).

2. Medios de pago con clave

En los últimos meses hemos visto iniciativas que buscan agregar el uso de claves a transacciones de compra con tarjetas de crédito (PinPass). Si bien el uso de clave frente a su no uso es una mejora de seguridad, es necesario hacer una lectura un poco más detallada sobre este tema. En primer lugar, es posible que se produzca una falsa sensación de certeza que genere comportamientos más riesgosos, tal como comprar en un lugar de dudosa reputación asumiendo que los medios de pago están protegidos contra todo tipo de ataque. Y en segundo lugar, la responsabilidad frente a un fraude puede traspasarse desde la institución financiera hacia el usuario final cuando hay un uso de clave, dado que la presunción es que si se realiza una operación se tuvo que haber tenido acceso a la clave y es responsabilidad del usuario final resguardarla. Por tanto, si un tercero tuvo acceso a la clave y la tarjeta (o una copia de ésta), la responsabilidad del usuario final sería, si no total, generalmente mayor.

El principal problema que se da en los sistemas de PinPass para tarjeta de crédito y/o RedCompra para tarjeta de débito radica irónicamente en su éxito: hoy en día en casi cualquier tienda, feria de artesanía y otros puntos de venta se puede encontrar una alta diversidad de máquinas que permiten este tipo de pago; donde el usuario ingresa una clave directamente en la máquina perteneciente a la institución financiera que valida los pagos, con lo cual desaparece el peligro de que el comerciante o un tercero pueda acceder a todos los datos necesarios para generar transacciones a su favor.

Sin embargo, no hay ninguna herramienta que permita al cliente validar que efectivamente la máquina que tiene en sus manos pertenece o está siendo controlada en exclusiva por la institución que la debe controlar. La única verificación que puede realizar el usuario final es revisar si la máquina tiene el logo correspondiente, que por lo demás es fácil de falsificar. Si tampoco se tiene incorporada 'tecnología de tarjeta inteligente' en las tarjetas, basta con una transacción para que cualquier vendedor malicioso pueda generar una copia de la tarjeta y obtener al mismo tiempo la clave, directamente de una máquina alterada o propia. Este problema se volverá más crítico a medida que aumente la disponibilidad de aparatos, lo cual por ley de Moore es muy pronto. Por el momento, se está repitiendo el mismo error de autenticidad mediante las páginas Web: hacer que la gente confíe en un sistema que tiene serios problemas de seguridad.

Una alternativa más segura sería generar un mecanismo mediante el cual el vendedor le entregara al comprador toda la información para realizar la transacción, el comprador instruyera a su banco el pago usando mecanismos bajo su propio control (vía PDA o teléfono celular por ejemplo) y el vendedor recibiera la notificación del pago en línea.

En algún momento debemos tomar la decisión de cuánta dependencia tecnológica aceptaremos. Y para eso necesitamos tener claro las consecuencias que nos genera esta dependencia, las cuales generalmente son futuras, versus los beneficios que suelen ser inmediatos o de corto plazo.

DEPENDENCIA TECNOLÓGICA

La dependencia es algo que un proveedor siempre busca y que el cliente rehúye. Ambos con justa razón. Si existe una dependencia, implica que el proveedor puede aumentar arbitrariamente el precio de lo que provee y el cliente está obligado a continuar pagando lo que le pidan o bien asumir el costo de cambiarse a otra alternativa, si es que ésta existe. En el caso de los proyectos TI casi siempre hay soluciones alternativas, pero con un costo asociado al cambio. Este será mayor en la medida que sea más grande o especializado el sistema. Y se puede decir sin temor a equivocarse que a medida que un sistema está en uso durante un período más prolongado, la tendencia es que el cambio a otro sistema se vuelva más costoso.

El usuario de tecnologías tiene dos opciones para enfrentar este problema: evitar proyectos que generen algún tipo de dependencia o bien intentar reducir el costo de la dependencia. Me atrevería a decir que lo primero es casi imposible y con certeza no siempre es deseable. En general se puede intentar reducir el costo de la dependencia y llegar a un equilibrio.

Debemos entender también que tenemos dependencias tecnológicas que pueden parecer poco obvias, pero existen y las aceptamos. Por ejemplo, las metodologías de gestión de tiempo que abundan hoy en día sugieren liberar el cerebro de tareas poco creativas como recordar datos y depender para ello de elementos externos y la escritura. En ese sentido, la dependencia incluso genera un resultado positivo porque libera a la mente de una actividad para abocarse a otra; siempre y cuando el subconsciente confíe en que los datos estarán ahí a futuro.

En algún momento debemos tomar la decisión de cuánta dependencia tecnológica aceptaremos. Y para eso necesitamos tener claro las consecuencias que nos genera esta dependencia, las cuales generalmente son futuras, versus los beneficios que suelen ser inmediatos o de corto plazo. Se condice con el incentivo que tiene el proveedor: entregar beneficios inmediatos a cambio de una relación duradera con el cliente, período en el cual recupera la inversión inicial y genera beneficios para sí. Es importante destacar que se debe tomar una decisión y no simplemente obviar el problema y su análisis, porque el impacto, por muy futuro que sea, es real.

Los estándares permiten en general algún nivel de interoperabilidad que admita reducir el costo de cambiar de una plataforma a otra, con lo cual un proveedor puede mostrarle a sus clientes que los costos futuros por causa de dependencia tecnológica son menores al reducir los de una potencial migración. Sin embargo, ese proveedor también pierde algo que le puede ser muy atractivo: clientes cautivos, razón por la cual solamente ofrecerá ese tipo de beneficios en la medida que los clientes lo demanden y tengan alternativas.

En esto hay dos aspectos que han sido claves en la industria TI en los últimos años, al proveer una alternativa o al menos la promesa de una alternativa, mejorando la posición negociadora de los clientes: el software libre, u open source, y los estándares abiertos. Si bien el hecho de que un software sea open source o que un estándar sea abierto no garantiza que nos libremos de la dependencia tecnológica. En muchos proyectos la tendencia es que se genere algún nivel de interoperabilidad que rompe la barrera del cambio, disminuyendo el costo de la dependencia de software. Sin embargo no basta con que existan alternativas para que el usuario de tecnologías esté a salvo de este problema; debe revisar no sólo el tipo de software y formatos que utiliza, sino también cómo lo utiliza. No da lo mismo un motor de base de datos con todas las optimizaciones específicas y no interoperables, que usar ese mismo motor de base de datos con solamente SQL standard. En un caso se puede tener un mejor rendimiento o facilidad de cambio interno a costa de mayor dependencia de esa solución, mientras que en el otro se puede aprovechar menos la solución actual, pero teniendo siempre la posibilidad de cambiarla por otra a un costo mínimo.

Como siempre, la decisión depende de las condiciones particulares en las cuales se evalúa. Lo importante es que sea una decisión y no una consecuencia casi azarosa de determinaciones que no consideraron estos elementos. Lo último sería una irresponsabilidad. BITS