

10 lecciones aprendidas en DRP

Fuente: http://bsecure.com.mx/articulos.php?id_sec=53&id_art=6609

¿Puede alguien presumir que ha llevado a la práctica un Plan de Recuperación en Caso de Desastres (DRP) sin contratiempos? Lo más probable es que no. La diferencia es que algunas empresas han tenido problemas menores y otras han sufrido fallas importantes que les han impedido, incluso, arrancar el plan en el momento necesario. Involucrados en este tipo de fallas mayores hay muchos: instituciones bancarias, empresas manufactureras, retails, farmacéuticas, y no de importancia menor, en muchos casos se trata de los principales jugadores de estos sectores.

Por supuesto, casi ninguna empresa está dispuesta a exponer públicamente que falló en su DRP y menos a hablar de cuáles fueron en concreto los errores cometidos. Pero se sabe de casos como el de una gran compañía nacional de manufactura de bebidas que no documentó punto a punto los procesos de su plan de contingencia y cuando se enfrentó a un siniestro, simplemente no lo pudo echar a andar.

En este caso en particular, el problema fue que los procesos estaban descritos en forma muy general, el DRP decía, por ejemplo, levantar el sistema X, pero no se documentó cómo hacer eso paso a paso. Así que en plena contingencia, el equipo de respuesta enfrentó serias dificultades para llevar el manual a la práctica.

Otro caso fue el de un conocido retail, que por falta de experiencia en su equipo interno tardó más de cinco años en implementar su DRP. Finalmente la empresa se dio cuenta que necesita asesoría externa, pero para entonces ya habían arriesgado bastante tiempo la operación del negocio.

La lista de ejemplos puede seguir, pero en resumen y como una forma de ofrecer una guía a los lectores de b:Secure respecto a lo que no dicen los manuales de DRP, he aquí lo que puede bautizarse como las lecciones aprendidas en diferentes implementaciones de un plan de contingencia.

1.- Cada quien debe poner su parte. Lo primero que se debe tener muy en cuenta en esto de desarrollar e implementar un DRP es si se está en sincronía con la alta directiva respecto a este tema y si se van a cubrir de forma adecuada las necesidades del negocio.

“Primero se debe definir qué entienden los responsables de la estrategia de contingencia por DRP y qué entienden los directivos de la organización. Ese es el primero dolor de cabeza, porque, muchas veces, se tiene la equivocada idea de que esto es un problema exclusivo del área de informática”, comenta Méndez.

Pero para que informática sepa cuál pie pone primero para levantarse, continúa, la alta directiva debe ayudarlo a definir qué sustenta a la empresa. “Si informática no sabe cual es el corazón del negocio, no sabrá

qué levantar primero. Los directivos deben ayudarlo a determinar cuál es la infraestructura y los procesos que requieren recuperarse primero y en qué tiempo, para minimizar las pérdidas. Informática lo que pone es el cómo se hace la recuperación.

2.- Hay que darle al plan “el mantenimiento adecuado”. Muchas organizaciones, asegura Alejandro Cerezo, de Integridata, se deciden a implementar un DRP por acatar la recomendación de los auditores (60%) o porque el corporativo se los pide (30%), pero pocas lo hacen por convicción propia (10%). “De manera que la mayoría se conforma con implementarlo y no lo actualiza, dicen ya cumplí, no le dan el mantenimiento necesario y luego vienen los fracasos”.

Ese mantenimiento del que habla Cerezo involucra, entre otras cosas, probar constantemente el DRP, para ver si algo falló en el desarrollo metodológico.

Puede ser que el personal no conozca bien la infraestructura del negocio, a la mejor la plataforma de recuperación no es la adecuada o los procedimientos técnicos no están bien desarrollados, y todo eso se mide en las pruebas posteriores a la implementación.

¿Cuántas pruebas deben hacerse y cada cuándo? Lo que recomienda el estándar BS25999 (que plantea el uso de sistemas de administración de la continuidad del negocio) es probar el DRP cada seis meses y luego proceder a las actualizaciones pertinentes, para asegurar su vigencia.

En la primera prueba, realizada después de la implementación, se logra alcanzar apenas entre 45 y 50% de efectividad en el plan. “Eso es un rango normal, no hay por qué preocuparse. La experiencia dicta que es hasta la cuarta o quinta evaluación cuando el DRP está ya listo, cuando la empresa puede salir airoso de una contingencia”, asegura Cerezo.

Desafortunadamente, ni siquiera las empresas que implementan su DRP plenamente convencidos de su importancia le dan a éste el seguimiento adecuado. De hecho, muchas no pasan de la segunda prueba, así que de 10% que desarrolla un DRP por convicción, sólo 7% puede salir adelante de un evento catastrófico.

“De las empresas que estaban en las torres gemelas sólo 20 o 25% se recuperaron de ese evento, porque tenían un plan, pero no le dieron seguimiento, ni mantenimiento y nunca probaron con la frecuencia requerida, si no cada dos años y eso no es funcional”, enfatiza Cerezo.

Y agrega: “no se vale hacer la prueba dos años después, porque la gente cambia, la infraestructura cambia, los cambios en tecnología son muy rápidos y también en la operación del negocio, y si no le das mantenimiento al plan, ya no te puedes recuperar”, subraya el consultor.

3.- Contar con todo lo necesario para cubrirse bien las espaldas. El siguiente reto es la disponibilidad tecnológica y de elementos críticos: tener, por ejemplo, los suficientes respaldos para recuperar toda la información sensible.

“En el mundo de los respaldos hay una parte olvidada: no todos los usuarios tienen un plan para respaldar su información, por eso conviene elaborar una política en la cual se asiente que todo el personal debe almacenar en un servidor y no sólo en su computadora. Claro que para esto se requiere definir qué se respalda y cada cuándo”, puntualiza Méndez.

Además, cuando hablas de un proceso de recuperación, hay una parte importante que es la inversión en los equipos para el recovery. “A la dirección todo este gasto le parece excesivo, por ende se pronuncia por buscar esquemas baratos o asignan el presupuesto para implementar el plan, pero tres meses después lo retiran, eso provoca que el DRP se quede empantanado”, comenta Cerezo. Viene entonces la lección número...

4.- Hay que saber vender el DRP. En la mayoría de las empresas no se consigue el presupuesto necesario para preparar la recuperación de un desastre, porque el personal de IT o los encargados de esto no saben cómo vender el plan a la dirección general.

La alternativa más adecuada para esto es hacer un análisis de impacto, es decir, hay que dejarle bien claro a la alta dirección, cuánto pierde la organización por estar fuera de servicio en las horas más críticas para el negocio. Por ejemplo, si la empresa es una comercializadora, habrá que definir cuando perdería por no poder llevar sus productos a ciertas regiones.

Pero en lugar de hacer esto, se empieza al revés, generalmente el área de sistemas pretende implementar el plan y conseguir los recursos necesarios sin justificar cuánto pierde la organización si no puede recuperarse de forma efectiva y en el tiempo justo de un incidente.

5.- Integrar un buen equipo de respuesta. Un plan de recuperación debe involucrar no sólo al responsable de la recuperación, si no a un grupo compuesto por: un equipo directivo (encargado de hacer la declaración formal de contingencia), otro de respuesta (enfocado a evaluar todo el evento y determinar en qué momento “sube” la decisión de declarar la contingencia), uno más con la función de “ejecutar” el plan en la parte técnica y un grupo de usuarios, cuya misión es operar las aplicaciones y darle continuidad al negocio.

Las lecciones específicas aprendidas en esta parte, durante ciertas implementaciones, indican, de acuerdo a los entrevistados, que a veces el DRP o las pruebas fallan, porque al responsable del plan lo saturan con otras cosas y no le permiten dedicarle a esto el tiempo suficiente.

En la mayoría de las empresas, reconoce Cerezo, ya existe un responsable de recuperación, encargado de coordinar toda la parte del recovery. Generalmente este personaje está integrado al área de sistemas. Pero muchas veces cumple otras funciones que le impiden concentrarse en el DRP.

6.- Tener todo documentado a detalle. Como se mencionó en el caso de la empresa de manufactura de bebidas, no tener bien documentados los procesos puede causar severos problemas. Los procedimientos para lograr la recuperación después de un desastre

deben escribirse a detalle e involucrar toda la parte técnica en cuanto a bases de datos, aplicaciones, sistemas operativos, pero también en lo relativo a procesos de identificación y declaración de contingencia, entre otros.

7.- Si no se actualiza el inventario de IT, el plan no sirve. El DRP necesita estar bien actualizado, esto implica: tener un inventario al día de todos los recursos de IT, porque a veces pasa que se cambia una PC o los sistemas operativos, pero no se hacen las actualizaciones pertinentes para saber con que infraestructura se cuenta y al menos los cambios en los equipos importantes para la operación del negocio, deben estar reflejados en el inventario. “Esa es la otra parte de la vida real que a veces resulta complicada”, admite Guadarrama.

8.- No se valen los ensayos de laboratorio. Claro que hacer las pruebas cada seis meses no es nada sencillo. “Hay que ver cómo se van a realizar, si se va a probar el plan de principio a fin y qué involucra hacerlo de esta forma”, comenta Manuel Méndez, oficial de seguridad de la información de una importante compañía de transporte.

Al respecto, Luis Guadarrama, consultor independiente y experto en el tema de DRP, asegura que las pruebas se vuelven un verdadero problema, porque requieren una buena cantidad de recursos, tanto monetarios como de tiempo y compromiso por parte del personal, sobre todo cuando se toma la acertada decisión de ejecutarlas tratando de acercarse lo más posible a la realidad.

Esa es precisamente otra de las lecciones aprendidas en la implementación del DRP, mientras más real sea el ambiente y la escena de prueba, mejor se ubicarán las posibles fallas del plan y los flancos descubiertos.

Sin embargo, lo cierto es que muchas empresas hacen pruebas de escritorio, hay ensayos de un DRP hechos en una sala de juntas. El equipo se reúne y actúa toda la prueba, alguien declara la contingencia y luego cada miembro del equipo va diciendo lo que le toca hacer, pero todo simulado en el escritorio. Eso no es una prueba real.

Evidentemente, tampoco se puede bajar el swith, pero se deben encontrar un punto medio, entre la prueba de escritorio y esto. “No se puede tirar toda la infraestructura, pero si se debe prever la descompostura de un servidor crítico y dejarlo fuera o tirar funciones críticas”, recomienda Guadarrama.

Para convencer a la directiva de la necesidad de proceder así, habrá que plantear que en efecto la prueba puede tener cierto costo, pero esto se debe balancear contra el impacto de no estar preparados.

9.- La importancia del factor psicológico. Con todo y por muy real que sean las pruebas, existen factores imposibles de evaluar hasta que realmente sucede un incidente, “cuando se presenta un siniestro tienes encima a todos los usuarios; está, además, la presión de los ejecutivos; de la carencia de sistema y la necesidad de levantarlo lo más rápido posible para no afectar los procesos del negocio, todo eso involucra una respuesta

psicológica por parte de los involucrados en la respuesta que es difícil de simular”, subraya Guadarrama.

Lo forma de responder a este hecho es extrapolar los resultados de la prueba e intentar deducir cómo se comportarían los principales involucrados.

10.- Se vale pedir ayuda. El caso del retail, mencionado al principio de este artículo, resulta bastante ilustrativo para dejar claro que a veces el equipo interno requiere la ayuda de algún especialista externo.

Pero no sólo eso, también es posible que se requiera el soporte de partners o socios de negocio para implementar y llevar a la práctica un DRP. Involucrarlos no sólo es valido si no acertado.