

## **ARTÍCULOS TÉCNICOS**

### **ESPECIAL CONTINUIDAD DE NEGOCIO**

#### **LA RECUPERACIÓN DE DATOS, EL ÚLTIMO ESLABÓN DE LA CADENA EN LOS PLANES DE CONTINUIDAD DE NEGOCIO**

**Hoy en día, sin lugar a dudas, la información es el activo más importante del que disponen las compañías. Cualquier error que suponga la pérdida de este activo puede resultar crítico para la supervivencia del negocio.**

**A raíz del incendio del edificio Windsor en Madrid, las empresas españolas y la sociedad en general, han comenzado a tener un mayor interés y a preocuparse por la seguridad informática y la continuidad de negocio. Hay empresas que han comenzado a tener conciencia del problema y otras muchas, que ya estaban concienciadas con la importancia que tienen los datos de su empresa, se han puesto manos a la obra y han rescatado esos planes que tenían dentro del cajón y que por falta de tiempo o presupuesto no se habían puesto en marcha.**

**Cualquier plan de continuidad del negocio y de recuperación frente a desastres busca establecer cómo una organización puede continuar sus operaciones en caso que se produzca una interrupción y a sobrevivir a un bloqueo desastroso de sus sistemas de información.**

**La responsabilidad de que este plan de continuidad exista, que esté bien dimensionado y que cuente con los recursos necesarios para llevarse a cabo recae en la gerencia de la empresa debido a que las consecuencias de una interrupción del servicio por un tiempo prolongado pueden llevar a un gran quebranto económico para la empresa y, en algunos casos, suponer la desaparición de la misma.**

**Los procesos que se deben llevar a cabo para la creación de un plan de continuidad se pueden dividir en varias fases. Primeramente se procede a la identificación y análisis de cuáles son aquellos puntos en el negocio que, en caso de fallo o interrupción, pueden provocar problemas a la organización. A continuación se desarrollan las estrategias de recuperación del negocio con las posibles alternativas existentes. Con las conclusiones anteriores, se procede a diseñar un plan detallado de las actuaciones a acometer. Se debe implementar dicho plan realizando las adquisiciones y la formación**



necesaria para que todo esté preparado si este desastre se produce. Y por último, y probablemente lo más importante, se debe realizar una prueba exhaustiva total de dicho plan. Tras esa prueba se deberán sacar las conclusiones de cuáles han sido los fallos y realizar las correcciones adecuadas para cumplir con los objetivos propuestos.



El problema que ocurre en muchos casos, es que ese plan se queda en eso, “un plan” y no se comprueba que han sido correctamente identificados los puntos críticos que, en caso de pérdida, pueden afectar a la productividad de la empresa. ¿Quién asume la responsabilidad de apagar el interruptor general para confirmar que en el plazo planeado volvemos a estar trabajando sin problema? Todo plan valora los gastos que, irremediamente, se producen tras un desastre, ¿asumimos los gastos para comprobar que estamos preparados?

Dentro de las actuaciones rutinarias que debe realizar la empresa y que están contempladas dentro del plan de continuidad, está la realización de copias de seguridad. Éstas son las que, en caso de fallo de los soportes de almacenamiento, servirán para restaurar la copia más reciente de los datos. El fallo se produce cuando, al ir a restaurar estas copias, no están disponibles o no se han realizado según lo planeado. En ese momento todo el plan, o parte de él, se empieza a desmontar.

Otro problema muy frecuente es el implementar sólo una parte del plan. Por ejemplo, se ha considerado necesario instalar un sistema RAID con redundancia como almacenamiento, implementando, además, un sistema de back-up periódico, pero sólo se instala el sistema RAID pensando que ya estamos a salvo pues “estos sistemas nunca fallan”.

En Recovery Labs recibimos asiduamente personas que se han llevado la desagradable sorpresa de que una mañana el sistema no arranca por un error en la estructura lógica del sistema de archivos y se tienen que enfrentar a un problema que se podría haber evitado implementando al completo las soluciones propuestas ya que, aunque no puedan acceder a los datos que se encuentran en la unidad de almacenamiento principal, sí podrían acudir al back-up de sus datos y, restaurándolos, continuar con el trabajo de forma normal en un tiempo más o menos corto en función de cómo se hubiera dimensionado el plan.

La realidad es que todo sistema informático es susceptible de fallar por uno u otro motivo. Formateos involuntarios, particionamiento erróneo, boicots, virus, bloqueos del sistema, averías mecánicas, picos de tensión, golpes o catástrofes naturales, sin la debida protección frente a ellos, producen la imposibilidad de acceso a los datos y por tanto la pérdida de información si no se tienen los medios y conocimientos para acceder a los mismos en caso de fallos de este estilo.

**Cuando todo parece perdido**

Las compañías de recuperación de datos dan respuesta a la necesidad, cada día mayor, de recuperar información perdida o inaccesible de la manera más rápida y

eficiente. Estas empresas son el último eslabón de la cadena en los planes de continuidad de negocio. Cuando todo parece perdido y han fallado todas las previsiones y sistemas de seguridad, la recuperación de datos informáticos es la vía más eficaz para acceder a la información. El servicio que proporcionan consiste en recuperar la información perdida directamente de cualquier tipo de dispositivo dañado.

Antes de contratar los servicios de una empresa de recuperación de datos es imprescindible asegurarse de que cumplen algunos requisitos básicos, que el tratamiento que van a utilizar para realizar la recuperación es el adecuado y por tanto nuestra información está en buenas manos. El primer requisito es la existencia de un laboratorio tecnológico con una cámara limpia —no confundir con cabina de flujo laminar, que permite abrir los discos pero nunca ofrece la misma garantía—. Esta cámara es el lugar óptimo para la apertura de los discos duros, ya que consigue el máximo nivel de limpieza y seguridad con un nivel mínimo garantizado clase 100.

Nuestra información es confidencial, en mayor o menor grado, y el factor diferencial de nuestro negocio. Poner estos datos en manos ajenas requiere de un ejercicio de máxima confianza. Por este motivo, otro de los puntos fundamentales a tratar y que se deben exigir son los protocolos de seguridad y confidencialidad. La posibilidad de tener un seguimiento telefónico de los diferentes estadios del proceso de recuperación, así como ver un listado de referencia de algunos clientes y partners, puede ser de ayuda a la hora de decidirnos por una u otra compañía

.

Si se trata de proteger nuestra información, nuestros datos, los que permiten que funcionemos todos los días y nos interrelacionemos con partners, proveedores y clientes, cualquier precaución que tomemos para salvaguardarlos puede resultar insuficiente. Resulta entonces evidente que lo ideal es tener un buen plan de contingencia que contemple la redundancia de sistemas, la copia casi diaria de los datos de una empresa y que estos se almacenen en lugares remotos a la ubicación de la empresa. Pero un plan de continuidad no estará completo si no se contempla la posibilidad de que algo falle. Tener identificada una buena empresa que pueda proceder a la recuperación de datos en caso que fuera necesario acudir a ella, debe ser una tarea obligada ya que, en momentos de crisis, no se pueden tomar decisiones a la ligera que puedan provocar la pérdida total de ese bien único en el mundo que es el contenido de nuestros dispositivos de almacenamiento.

*Miguel*  
*Director técnico de Recovery Labs*

*Ruiz*