Realización del plan de contingencia

Toda red debe de tener un plan de contingencia por cualquier siniestro o desastre que puede ocurrir por lo tanto no propusimos a elaborar el nuestro para estar prevenidos de cualquier circunstancia que se puede presentar.

Como con cualquier proyecto de diseño, un método estructurado ayuda a asegurar de que se toman en cuenta todos estos factores y de que se les trata adecuadamente.

A continuación se muestran las principales actividades requeridas para la planificación e implementación de una capacidad de recuperación de desastres.

1. Identificación de riesgos
2. Evaluación de riesgos
3. Asignación de prioridades a las aplicaciones
4. Establecimiento de los requerimientos de recuperación
5. Elaboración de la documentación
6. Verificación e implementación del plan
7. Distribución y mantenimiento del plan

1. Identificación de riesgos

La primera fase del plan de contingencia, el análisis de riesgos, nos sitúa en el lugar de un asesor de una compañía de seguros. En esta fase, la preocupación está relacionada con tres simples preguntas: ¿qué está bajo riesgo?, ¿qué puede ir mal? y ¿cuál es la probabilidad de que suceda?

1.1. ¿Qué está bajo riesgo?

La primera de estas preguntas, ¿qué está bajo riesgo?, necesita incorporar todos los componentes del sistema susceptibles de ser dañados, dando lugar a la pérdida de conectividad, computadoras o datos. Un diagrama de la arquitectura de todos los componentes del sistema facilitará la realización de un inventario de los elementos que pueden necesitar ser restituidos tras un desastre. No hay que olvidar que también el software necesita ser reemplazado, y que todos los productos software relevantes han de ser identificados. Esto incluye cosas como las utilidades del sistema de archivos empleados para facilitar las operaciones de red.

Un inventario completo de una red muestra de manera clara la complejidad de ésta. Cualquiera que realice inventarios de componentes para redes, comprende los problemas en el seguimiento del hardware y software utilizado por los usuarios finales.

Afortunadamente, existen algunos productos disponibles, como los de las compañías Seagate Software, McAfee y otros, que facilitan la construcción de un inventario de los sistemas.

Una omisión en el inventario fácilmente puede dar lugar a una recuperación fallida tras un desastre. El sistema de aplicación puede no encontrarse preparado para su uso si alguno de sus componentes no está disponible; en tal caso, es aconsejable estar constantemente a la expectativa de los nuevos elementos que pueden haberse olvidado. Por ejemplo, una aplicación para acceso remoto no funcionaría si los cables no están disponibles para conectar los módem.

Uno de los aspectos menos agradables a tener en cuenta, y que a menudo se pasa por alto, es que las personas esenciales se vean afectadas por el desastre y sea necesario recurrir a otras para realizar sus labores. Una formación diversificada en los sistemas dentro de la organización pude ayudar a reducir el impacto de la indisponibilidad de uno de los colaboradores. Al menos, los manuales de las aplicaciones más importantes para la empresa deberían encontrarse disponibles en un sitio externo.

1.2. ¿Qué puede ir mal?

Lo más difícil en el plan de contingencia es responder a la pregunta, ¿qué posiblemente pueda ir mal? La respuesta a tal cuestión varía desde lo evidente hasta lo casi increíble. La ley de Murphy nos proporciona una colección de extraños e inesperados desastres. Por ejemplo, las inundaciones son bastante frecuentes, pero pocos podían haber predicho la inundación de un sistema de túneles del metro en la ciudad de Chicago, en 1992, provocada por la rotura de una tubería a raíz de las obras de reparación de un puente.

Las clases más obvias de desastres son los desastres naturales que conllevan tormentas de todo tipo o los acontecimientos geológicos como terremotos o volcanes. En cada localidad existe la posibilidad de tener mal tiempo. En los últimos años se han visto huracanes destrozar instalaciones a lo largo Florida, islas del Caribe y el Golfo de México. Los tornados y vientos de elevadas velocidades han destruido edificios cada año en el interior de los Estados Unidos y Canadá.

Las inundaciones pueden acaecer en casi cualquier lugar donde el drenaje existente no sea capaz de absorber el volumen de lluvia o fango. Relacionado con las inundaciones se encuentra el perjuicio producido por el agua. Cada año los incendios en los edificios provocan importantes daños a los sistemas informáticos debido al agua, cuando los sistemas automáticos de irrigación (sprinklers) se activan para apagar el fuego.

Los propios incendios constituyen uno de los peores desastres posibles. El calor, el humo y el agua que rodea a los incendios son tremendamente perjudiciales para los sistemas informáticos. Los dispositivos de almacenamiento se deterioran fácilmente debido a las altas temperaturas y

el humo. La eliminación de los residuos tóxicos tras el incendio de una oficina puede llevar meses, incluso años. En los Estados Unidos, la agencia de protección ambiental (EPA), en ocasiones, ha tenido que cerrar edificios después de un incendio debido a la alta concentración de toxinas encontradas en el mismo. Esto implica que puede no ser posible disponer de lo sistemas y datos hasta bastante tiempo después del incendio. Existen compañía especializadas en preparar operaciones específicas de limpieza de instalaciones víctimas del incendio, que darán su aprobación para enviar especialistas con trajes protectores al edificio incendiado, recuperar el equipo de procesamiento de datos e intentar restaurar la información de los discos.

Deben considerarse mecanismos alternativos de acceso a la red en el caso de que, por alguna razón, sea imposible acceder al edificio, incluso aunque el edificio puede estar en pie y operacional. Ejemplos de sucesos que pueden impedir e acceso al interior del edificio son los accidentes químicos e industriales, así como los motines y disturbios callejeros.

El fuego no tiene por qué darse necesariamente en la propia instalación para que el problema sea devastador. Un incendio destruyó la oficina central de Ameritech, en Hinsdale, Illinois, en mayo de 1988, dejando a numerosos clientes sin servicio telefónico durante meses mientras la compañía reparaba la edificación dañada. Obviamente, las comunicaciones que empleaban las líneas telefónicas que habían sido enrutadas a través de esta instalación, se vieron seriamente afectadas.

Desgraciadamente, los ataques terroristas y otros actos deliberados de destrucción cometidos por personas pueden devastar sistemas e instalaciones. Este incluye actos violentos (por ejemplo, descargar armas sobre los equipos informáticos). Menos excitante, pero igual de perjudicial para la organización, es la pérdida de equipos debido al robo. Existen también ataques a los datos contra los que hay que estar prevenidos, en los que la gente destruye intencionadamente datos mediante su borrado o inutilizándolos. Los virus se encuentran en este campo.

Los errores humanos son una de las causas más probables de la pérdida o deterioro de los datos. Si un error de este tipo provoca la pérdida de un sistema en la red, tiene el mismo efecto que cualquier otro tipo de desastre, y como tal debe ser tratado.

1.3.¿Cuál es la probabilidad de que suceda?

Si se tuviera una cantidad ilimitada de recursos y fuera posible protegerse contra todas las calamidades, esta pregunta carecería de interés. Sin embargo, no se dispone de recursos infinitos; de hecho, los recursos son bastante escasos. Por lo tanto, se deben seleccionar los tipos de desastres contra los que uno intentará protegerse. Obviamente, estos preciados recursos se querrán gastar en aquellos desastres que tengan la mayor probabilidad de afectar a la organización.

Por ejemplo, se podría intentar proteger los sistemas de la improbable ocurrencia de la caída sobre el edifico de un meteorito procedente del espacio exterior. Esto no sería tan valioso como proteger los sistemas de las inundaciones.

Responder a la pregunta: ¿cuál es la probabilidad de que suceda? también requiere de ciertas consideraciones presupuestarias. Ello puede ayudar a asumir distintos escenarios de presupuesto para comprender cuáles son los costos de compromiso para diferentes niveles de protección y preparación. Finalmente, se puede estar expuesto a ciertas amenazas cuya protección no está al alcance del presupuesto, pero, al menos, se es consciente de su existencia y, por lo tanto, es posible mejorar el plan en un futuro.

2. Evaluación de riesgos

Es el proceso de determinar el costo para la organización de sufrir un desastre que afecte su actividad. Si una inundación impidiera la actividad comercial durante cinco días, la compañía perdería cinco días de ventas, además del deterioro físico de los edificios e inventario. En el caso de los sistemas informáticos, la preocupación principal es comprender la cantidad de pérdida financiera que puede provocar la interrupción de los servicios, incluyendo los que se basan en las redes.

Por ejemplo, si la empresa se anuncia a través o realiza negocios en Internet, ¿cuál es el costo de tener el servidor web inhabilitado? Si la red a través de la cual se produce la solicitud de pedidos está caída, o si el sistema de control de inventario utiliza la red, ¿cuál es el impacto sobre la productividad de la empresa?

Los costos de un desastre pueden clasificarse en las siguientes categorías:

- Costos reales de reemplazar el sistema informático
- Costos por falta de producción.
- Costos por negocio perdido
- Costos de reputación.

El costo real de los equipos y el software es fácil de calcular, y depende de si se dispone de un buen inventario de todos los componentes de la red necesarios.

Los costos de producción pueden determinarse midiendo la producción generada asociada a la red. La empresa tiene una correcta valoración de la cantidad de trabajo realizado diariamente y su valor relativo. La pérdida de producción, debida a la interrupción de la red, puede ser calculados utilizando esta información.

Los costos por negocio perdido son los ingresos perdidos por las organizaciones de ventas y marketing cuando la red no está disponible. Si el sistema de solicitud de pedidos no funciona y la empresa sólo es capaz de

procesar el 25% del volumen diario habitual de ventas, entonces se ha perdido el 75% de ese volumen de ventas.

Los costos de reputación son más difíciles de evaluar y, sin embargo, es conveniente incluirlos en la evaluación. Estos costos se producen cuando los clientes pierden la confianza en la empresa y se llevan su negocio a otro sitio. Los costos de reputación crecen cuando los retardos en el servicio a los clientes son más prolongados o frecuentes.

3. Asignación de prioridades en las aplicaciones

Después de que acontezca un desastre y se inicie la recuperación de los sistemas, debe conocerse qué aplicaciones recuperar en primer lugar. No hay que perder el tiempo restaurando los datos y sistemas equivocados cuando la actividad empresarial necesita primero sus aplicaciones esenciales.

Esto implica la necesidad de determinar por anticipado cuáles son las aplicaciones fundamentales del negocio. Si la empresa es como la mayoría, se tendrán aplicaciones "muy importantes" dependiendo de a quién se le pregunte. El departamento de recursos humanos afirmará que el sistema de nóminas es el más importante, el departamento de ventas dirá que es su sistema de entrada de pedidos, el departamento de producción insistirá en su control de inventario y el departamento de compras asignará el papel de más importante a su sistema de facturación. Desgraciadamente, no todos estos sistemas pueden ser el más importante; por lo tanto, es fundamental que la dirección ayude a determinar el orden en que los sistemas serán recuperados.

Es de esperar que esta información sea aceptada de buen grado por todos los jefes de departamento. Independientemente de ello, el plan de contingencia debería incluir la lista de los sistemas y su prioridad. Esta sección del plan debería ser firmada por la dirección para minimizar las desavenencias.

Una vez conocido lo que se va a restaurar, debería disponerse de todo lo necesario para la disponibilidad de tales aplicaciones. Un sistema de aplicación en una red está compuesto por los sistemas servidores, donde las aplicaciones almacenan sus datos, los sistemas de estaciones de trabajo que los procesan, las impresoras o fax empleados para entrada/salida, la red que interconecta todo, y el software de las aplicaciones. Las aplicaciones cliente/servidor o distribuidas añaden un nivel extra de complejidad al requerir que distintas partes de la aplicación residan en máquinas separadas.

Puede caerse en la tentación de construir una infraestructura superior a la necesaria para las aplicaciones de mayor prioridad. Por ejemplo, si actualmente la red tiene 50 estaciones de trabajo, se puede comenzar a trabajar inmediatamente en la reconstrucción de las 50 estaciones de trabajo. Sin embargo, si las aplicaciones más prioritarias sólo necesitan cinco estaciones de trabajo, se debería detener la reconstrucción de las estaciones de trabajo una vez alcanzado el número de cinco y concentrar los esfuerzos en lograr que la aplicación funcione. Es mucho mejor intentar lograr que un

sistema pequeño funcione, que no uno más grande, y de esta manera se ahorrara gran cantidad de tiempo en el proceso. De hecho, cuando se está asignando las prioridades a las aplicaciones junto con la dirección, también es posible beneficiarse de la determinación del número mínimo de estaciones de trabajo necesarias para tener el sistema accesible. El tamaño de la red siempre puede incrementarse a posteriori una vez el sistema esté en funcionamiento. Una de las ventajas del enfoque basado en el sistema de aplicaciones es la cantidad de tiempo necesaria para recuperar una aplicación comparada con la cantidad de tiempo requerida para restaurar un servidor en su totalidad. Si la aplicación tiene sólo 500 MB de datos y el servidor 4 GB, es obvio que se ahorra una gran cantidad de tiempo recuperando únicamente la aplicación.

Sin embargo este enfoque requiere un conocimiento algo más detallado sobre los sistemas que actualmente se tienen. En primer lugar, es necesario saber dónde se encuentra toda la información que emplean las aplicaciones y qué dependencias entre sistemas de archivos pueden existir. Si existen archivos del sistema que contienen información sobre la aplicación, como es el caso de los archivos .ini de Windows, es necesario asegurarse de que esos archivos también se recuperan junto a la aplicación. En segundo lugar, es preciso conocer cómo funciona el sistema de copias de seguridad para realizar este tipo de recuperación selectiva. Aunque esto no supone necesariamente una dificultad, no obstante esta operación debería ser familiar.

4. Establecimiento de requisitos de recuperación

La clave de esta fase del proceso de elaboración del plan de migración es definir un periodo de tiempo aceptable y viable para lograr que la red esté de nuevo activa. Tal y como se ha planteado en la sección anterior, la preocupación básica debería ser disponer de las aplicaciones más importantes en primer lugar.

El personal directivo de la organización deseará saber cuándo estarán sus aplicaciones funcionando para planificar las actividades de la compañía.

Es muy importante concederse una cantidad de tiempo adecuada y no realizar estimaciones poco realistas sobre las propias posibilidades. No es el deseo de nadie tener a un montón de gente alrededor esperando la finalización de las operaciones de recuperación; una distracción de este tipo probablemente perturbe las labores. El término para este tiempo es tiempo de recuperación objetivo o en inglés TRO (Recovery Time Objective). El TRO definido debe ser verificado para comprobar que es realista y factible, no sólo por uno mismo, sino por el resto de la organización, que puede ser requerido para realizar el trabajo.

La dirección de la empresa debería colaborar íntimamente con el personal de administración de redes para determinar el TRO de las aplicaciones. Aplicaciones diferentes tendrán TRO diferentes.

Es necesario asegurarse de que se dispone de tiempo para recuperar las cintas localizadas en la instalación de almacenamiento exterior y para

adquirir los sistemas necesarios. Por cierto, debería conocerse por anticipado cómo realizar las órdenes de compra de los equipos cuando la empresa se encuentra en un estado de total desorganización.

Es posible que sea necesario actualizar el sistema de copias de seguridad para satisfacer el TRO. Un sistema de cinta que recupera datos a 2 MB por segundo realizará la labor mucho más rápido que uno que lo ejecute a 500 KB por segundo. Hay que ser precavido y no suponer que se pueden hacer muchas cosas al mismo tiempo; uno se puede encontrar cometiendo desafortunados errores que frenan la labor si no se presta atención al trabajo que se tiene entre manos.

5. Elaboración de la documentación

Crear un documento que mucha gente pueda tener como referencia es quizás lo más difícil del plan de contingencia. No hay que engañarse: implicará un esfuerzo significativo para algunas personas, pero ayudará a aprender cosas sobre el sistema y puede que algún día salve la empresa.

Los recursos necesarios para escribir y mantener un plan de contingencia representan más de lo que puede realizarse en ratos libres y después de horas de oficina. La dirección de la organización debe apoyar la iniciativa para que sea un éxito. Uno de los problemas del plan de contingencia en un entorno de comunicaciones es que la tecnología de redes cambia tan rápidamente que resulta difícil permanecer al día. Esto incluye nuevos dispositivos, así como nuevos sistemas de aplicación que introducen su propio nivel de complejidad en este campo.

Como ejemplo, considérese la recuperación de un gran sistema de base de datos relacional Unix. Este tipo de trabajo requiere un conocimiento mucho más complejo del que corresponde a la instalación de la base de datos y del que un administrador de redes es probable que tenga; generalmente es necesario un administrador de base de datos, para el que también la labor será un desafío.

Dado el hecho de que la tecnología de red evoluciona tan rápidamente, debería planificarse la actualización del plan de contingencia periódicamente, por ejemplo una vez al año. Aunque la redacción del plan inicial supondrá una gran cantidad de trabajo, una vez que se dispone del plan, las actualizaciones son relativamente fáciles.

Contenido del plan de contingencia

El plan de contingencia debe intentar definir las cinco áreas siguientes:

1. Listas de notificación, números de teléfono, mapas y direcciones
2. Prioridades, responsabilidades, relaciones y procedimientos
3. Información sobre adquisiciones y compras
4. Diagramas de las instalaciones
5. Sistemas, configuraciones y copias de seguridad en cinta

Hay que cerciorarse de que se sabe a quién notificar en primer lugar cuándo ocurre un desastre. Por ejemplo, si hay un incendio, llamar primero a los bomberos y luego al director general. Pueden existir otras personas o organizaciones identificadas con características o conocimientos especiales que puedan ayudar a minimizar el daño. Si no se dispone de números de teléfono o direcciones actualizados, se puede pasar muy mal contactando con las personas afectadas.

Mapas mostrando las ubicaciones del centro de operaciones temporal y la instalación externa pueden ahorrar mucho tiempo. También puede ser útil mostrar itinerarios alternativos de acceso para el caso de que las rutas principales no se encuentren disponibles.

Cuando en primer lugar se comienza a reflexionar sobre cómo responder a un desastre, hay que centrarse en las prioridades establecidas. El tiempo pasa; el trabajo debe empezar por recuperar inmediatamente las aplicaciones de mayor prioridad. Las personas deberían disponer de instrucciones y responsabilidades precisas. La relación entre tareas debería hallarse documentada de manera que pueda identificarse cualquier cuello de botella que pudiera surgir. Por último, deberían incluirse, de manera detallada, las operaciones y tareas que muestren las labores de instalación y recuperación necesarias, debiendo ser fáciles de leer y seguir.

También habría que incluir aquí los números de teléfono de las organizaciones de asistencia que pudieran requerirse.

Como se ha mencionado anteriormente, debe saberse cómo expedir una solicitud de compra y obtener los equipos para el centro de operaciones temporal. Esto significa proporcionar a los vendedores la dirección y cualquier instrucción necesaria para el transporte. No hay que suponer que todos los vendedores del mundo van a enterarse de la difícil situación y venir a nuestro rescate. Es aconsejable disponer de copias de las facturas, recibos y demás para mostrarlos como prueba de compra. También viene bien tener a mano una lista de los números de serie de los equipos hardware. No hay que olvidar que, actualmente, gran parte de los productos para el mercado de comunicaciones de LAN se vende a través de grandes sistemas de distribución, y que los fabricantes y desarrolladores de software de los productos utilizados puede que no tengan ni idea de quién es su cliente. No espere recibir los repuestos de manera gratuita; en su lugar, debería ser capaz

de llegar a acuerdos especiales de compra y provisión para sustituir los bienes perdidos.

Los diagramas de red simplifican cu gran medida la labor de construir una red. Un diagrama detallado de la red, necesaria para las primeras aplicaciones, facilita y agiliza la reanudación de las actividades. La asignación de etiquetas a los cables y su almacenamiento en un lugar reservado, probablemente no llevará mucho tiempo y evitará muchas confusiones con posterioridad. La otra ventaja de un diagrama de conexiones es la posibilidad de emplear contratistas para realizar las instalaciones. Alguien experimentado en la instalación del cableado y otros dispositivos de red, y que se dedica a ello, puede ser capaz de realizarlo mejor y más eficientemente que uno mismo.

Es posible ahorrarse horas o incluso días en el proceso de recuperación si existe la posibilidad de almacenar algunos sistemas de repuesto con la capacidad de gestionar tareas diferentes. Planifíquese instalar una configuración genérica que, como mínimo, permita ejecutar las aplicaciones de mayor prioridad sin problemas. Si se desconoce los productos que la gente tiene en sus PC, un producto para inventario de LAN puede ayudar en la recopilación de esta información. Después de que la red alternativa se encuentre funcionando, y se disponga de un momento de respiro, será posible restaurar los PC con sus configuraciones anteriores utilizando la información de configuración extraída de los informes de inventario.
Hay que asegurarse la disponibilidad de un sistema de copias de seguridad de cinta en funcionamiento. Si es posible, debe mantenerse un sistema de reserva, incluyendo adaptadores SCSI, cables y software de unidades de dispositivo, en un sitio alterno. No es inusual encontrarse con que los vendedores locales no disponen de existencias de los productos necesarios, obligando, por tanto, a esperar el envío de los repuestos antes de poder empezar la recuperación de los datos.

Si se sigue este consejo, no hay que olvidar actualizar este sistema cuando se actualicen los sistemas de copias de seguridad de producción; en caso contrario, uno se puede encontrar con formatos de cinta o bases de datos incompatibles u otros problemas que impedirán la restauración de la información.

Verificación e implementación del plan

Una vez redactado el plan, hay que probarlo. Hay que estar seguro de que el plan va a funcionar. Para ello, se debe ser escéptico sobre el propio trabajo, de manera que pueda uno probarse a sí mismo que funciona. Psicológicamente, esto no es fácil porque con toda probabilidad se ha invertido una gran cantidad de tiempo y energía personal en este proceso, aunque lo mejor sería, si es posible, situarse de manera imparcial ante la confiabilidad del plan. Por consiguiente, han de realizarse las pruebas para encontrar problemas, no para verificar que el plan funciona. Si existen errores en la información, tómese nota de ellos y corríjase el plan.

Comprobación del plan por partes

No se puede tumbar el sistema algún día para ver si se es capaz de recuperarlo. Existen muchas y mejores formas de verificar un plan de contingencia sin causar mayores interrupciones en el trabajo de la organización. Algunas de las cosas en las que habitualmente no se piensa a la hora de comprobar pueden ahorrar mucho tiempo posteriormente. Por ejemplo, llamar a los números telefónicos de los colaboradores incluidos en las listas telefónicas del plan para confirmar si son actuales; llamar a los vendedores y comprobar si disponen de existencias de productos, ya que puede que hayan modificado su política de inventario. Algún día, viajar hasta la instalación alterna para saber dónde está y cómo reconocer el edificio.
Por supuesto, también es necesario verificar los procedimientos que se emplearán para recuperar los datos. Compruébese el software para la realización de las copias de seguridad para confirmar si pueden recuperarse las aplicaciones de mayor prioridad de la manera esperada. Esto debería hacerse en una red aislada para evitar problemas con el servidor de licencias. Por ejemplo, si la idea es unificar dos servidores mediante la recuperación completa de uno de ellos en el servidor de repuesto y a continuación restaurar sólo los archivos de datos de usuario procedentes del otro, finalmente se tendrá dos servidores con la misma licencia de software de servidor en la red, lo que podría dar lugar a la difusión por toda la red de mensajes de aviso sobre la licencia. Incluso aunque se utilice una nueva licencia de sistema operativo de red, todavía existen otros conflictos como nombres de servidores duplicados y cualquier otro problema de duplicación que podría causar problemas en los sistemas de producción.

Una vez recuperada la información, verifíquese si el usuario puede acceder a ella. Esto requiere de algunas estaciones de trabajo conectadas a la red para simular auténticos usuarios finales con cuentas en los servidos originales. En este punto, puede ser necesario actualizar el plan para incluir información sobre el establecimiento de cuentas de usuario. Compruébese cada una de las operaciones del plan individualmente y examínese entonces si, como resultado, se tiene un sistema de red en funcionamiento. No está de más verificar el plan con otras personas de la organización que se encuentren tan familiarizadas con los productos o procedimientos empleados.

Revísese cada día la parte del plan relacionada con las operaciones de copias de seguridad verificando la finalización correcta de las mismas. Además, supervise esto asegurándose de que algunas personas de la organización saben realizar copias de seguridad adecuadamente, y comprobar su finalización.

Distribución y mantenimiento del plan

Por último, cuando se disponga de un plan definitivo ya verificado, es necesario distribuirlo a las personas que necesitan tenerlo. Inténtese controlar las versiones del plan, de manera que no exista confusión con múltiples versiones. Así mismo, es necesario asegurar la disponibilidad de copias extra del plan para su depósito en la instalación exterior a en cualquier otro lugar

además del lugar de trabajo. Manténgase una lista de todas las personas y ubicaciones que tienen una copia del plan. Cuando se actualice el plan, sustituya todas las copias y recoja las versiones previas.

El mantenimiento del plan es un proceso sencillo. Se comienza con una revisión del plan existente y se examina en su totalidad, realizando cambios a cualquier información que pueda haber variado. En ese instante, se debe volver a evaluar los sistemas de aplicación y determinar cuáles son los más importantes para la organización. Las modificaciones a esta parte del plan causarán modificaciones consecutivas a los procedimientos de recuperación. Sin embargo, esto no debería verse como un problema porque probablemente la sección de procedimientos tenga que actualizarse de todas formas debido a otros cambios. Si se han realizado modificaciones al sistema de copias de seguridad, hay que cerciorarse de incluir la información sobre el funcionamiento del nuevo o actualizado sistema.

Este proceso llevará tiempo, pero posee algunos valiosos beneficios que se percibirán aunque nunca tengan que utilizarse. Más gente conocerá la red. Esto proporcionará a la organización una base técnica más amplia para mantener correctamente la red. También facilitará el crecimiento de una perspectiva global sobre la red dentro del núcleo de administradores de sistemas de información y puede ayudar a identificar las futuras o actuales áreas conflictivas. Uno de los aspectos más difíciles en cualquier labor distribuida, como es la gestión y administración de LAN, es dar a conocer la situación actual.

El mantenimiento y verificación de un plan de migración ayudará a que se produzca dicha comunicación dentro de la organización.