X CONGRESO DE GERENCIA DE RIESGOS Y SEGUROS INDUSTRIALES

CEGERS´98

MADRID, 30-31 DE MARZO DE 1998

INESE
SCIENTIA SECURITAS ET OECONOMIA

AGERS
ASOCIACIÓN ESPAÑOLA DE GERENCIA DE RIESGOS Y SEGUROS

LA INFORMATICA UTILIZADA EN LA DISTRIBUCION Y COMERCIALIZACION

Por: **D. Juan Andrés Pro Dios**
Responsable de Soluciones y Servicios de
INFORMATICA EL CORTE INGLES, S.A.

RIESGOS INFORMÁTICOS: ASEGURANDO LA CONTINUIDAD DE LOS NEGOCIOS

Juan Andrés Pro Dios
Informática El Corte Inglés

RESUMEN DE LA PONENCIA

En el mundo cambiante en que vivimos, la informática se ha convertido en fuente de ventaja competitiva para las empresas, pero también en fuente de problemas. Desde el punto de vista de la gerencia de riesgos es lícito afirmar que hay causas de siniestros propias de la aplicación de las Tecnologías de la Información a la vida socio-económica; sin ellas no se hubiera producido o, al menos, no con la misma amplitud y repercusión.

En esta ponencia se describen los riesgos informáticos que amenazan la continuidad de los negocios, sus causas finales, su impacto sectorial y las soluciones de que disponen las organizaciones para prevenirlos.

A finales del siglo XX vivimos en un mundo caracterizado por la rápida aparición de nuevas tecnologías, con ciclos de vida cada vez más cortos tanto en su desarrollo y comercialización como en su aplicación a la vida social y económica.

Parece claro que una fuente de ventaja competitiva para todas las empresas es el conocimiento y el uso y aplicación que de él se hace. Estamos viviendo una nueva revolución en la historia de la humanidad; estamos ante una nueva Era, la Era del Conocimiento. Y las tecnologías de la Información no son ajenas a ello; más bien se han convertido en su instigador.

La Informática y las demás tecnologías afines han invadido tanto la vida económica como la privada.

La seguridad de la información, tanto desde el punto de vista de la confidencialidad como de la integridad, consistencia y disponibilidad de la misma, es una necesidad de primer orden; las implicaciones sobrepasan al plano socio económico y alcanzan a la propia ética.

Voy a centrar esta exposición en el mundo empresarial. Estamos asistiendo al nacimiento de un nuevo modelo de negocio, mucho más competitivo, que requiere una integración más estrecha entre las Tecnologías de la Información y los procesos de trabajo. Como consecuencia de ello, el papel de los departamentos de informática en las organizaciones está cambiando.

La informática ya no es una mera herramienta de soporte a los procesos administrativos y operaciones repetitivas, sino que se ha convertido en un mecanismo de transformación organizativa e, incluso, de rediseño del propio negocio.

La variedad creciente de sistemas de información, la distribución de los mismos y el uso intensivo que de ellos se hace en el mundo empresarial ha hecho de las Tecnologías de la Información una herramienta estratégica para la sostenibilidad del negocio. Y como tal, no sólo sujeta a los riesgos a los que cualquier bien empresarial está expuesto (daños materiales, robo, gastos suplantarios, ...) sino también a otros relacionados con las consecuencias que de un mal uso o funcionamiento de la misma se puedan derivar para la vida económica de la empresa.

Todos los profesionales del sector asegurador tienen una larga experiencia en medir las probabilidades de un siniestro y en el nivel de las consecuencias que se pueden derivar de éste, pero cuando estamos hablando de riesgos informáticos que pueden poner en serio peligro la continuidad de las actividades de la empresa es cuando el papel del Gestor de Riesgos cobra un protagonismo especial. El avance tecnológico supone para éste último la identificación constante de nuevos riesgos, su evolución previsible, la planificación del control de los mismos y los planes de monitorización de los sucesos potenciales. Y todo ello en unos escenarios de carácter multiforme, con una gran complejidad operativa, con multiplicidad de arquitecturas y sin gran base documental de mejores prácticas.

La emergencia de los riesgos informáticos, manifestada desde principios de esta década, tiene su origen en los siguientes hechos:

A. Los sistemas de información y control de las empresas están cada vez mas automatizados e integrados entre sí.

B. Las aplicaciones informáticas incorporan cada vez más inteligencia del negocio.

C. El desarrollo de las Tecnologías de las Comunicaciones hace que los sistemas informáticos tiendan a estar interconectados en tiempo real, tanto intrinseca como extrínsecamente a cada organización.

D. La evolución vertiginosa de las Tecnologías de la Información y su incorporación rápida al mercado para amortizar las costosas inversiones en I+D que se ven obligados a hacer todos los fabricantes, provoca el uso de técnicas poco maduras, no dominadas totalmente ni en el fondo ni en la forma. Además, este hecho se ve agravado porque la experiencia del pasado vale poco para el futuro.

E. Tanto el hardware como el software siguen siendo costosos y, además, su complejidad técnica aumenta.

F. La información es uno de los activos más importantes de todas las organizaciones. Para un gran porcentaje de ellas tiene, incluso, un valor monetario precisamente tasado.

G. Debido a su carácter estratégico dentro de todas las compañías, la informática puede se objeto de hechos vandálicos y terroristas como medio de perjudicar los intereses empresariales. Estos pueden ser cometidos por agentes internos o externos a la organización en beneficio de individuos aislados o de colectividades.

H. En muchas organizaciones la informática todavía es, por desgracia, un mundo aparte en donde los intereses de sus profesionales pueden no estar alineados con los objetivos del negocio. Este hecho puede provocar diferencias en el análisis multidisciplinar preciso para evaluar las consecuencias que toda acción, tanto originada por los técnicos como por los usuarios, puede tener de cara a prever los riesgos que conlleva.

I. El aseguramiento de la calidad en los procesos de desarrollo y de producción de sistemas de información es todavía muy incipiente. En una actividad con un alto componente tecnológico, las labores de diseño y construcción de software son, aún hoy, muy artesanales. La calidad del sistema sigue estando directamente relacionada con la calidad de sus diseñadores y usuarios; el riesgo de error todavía es grande...¡ Y sus consecuencias no bien analizadas!

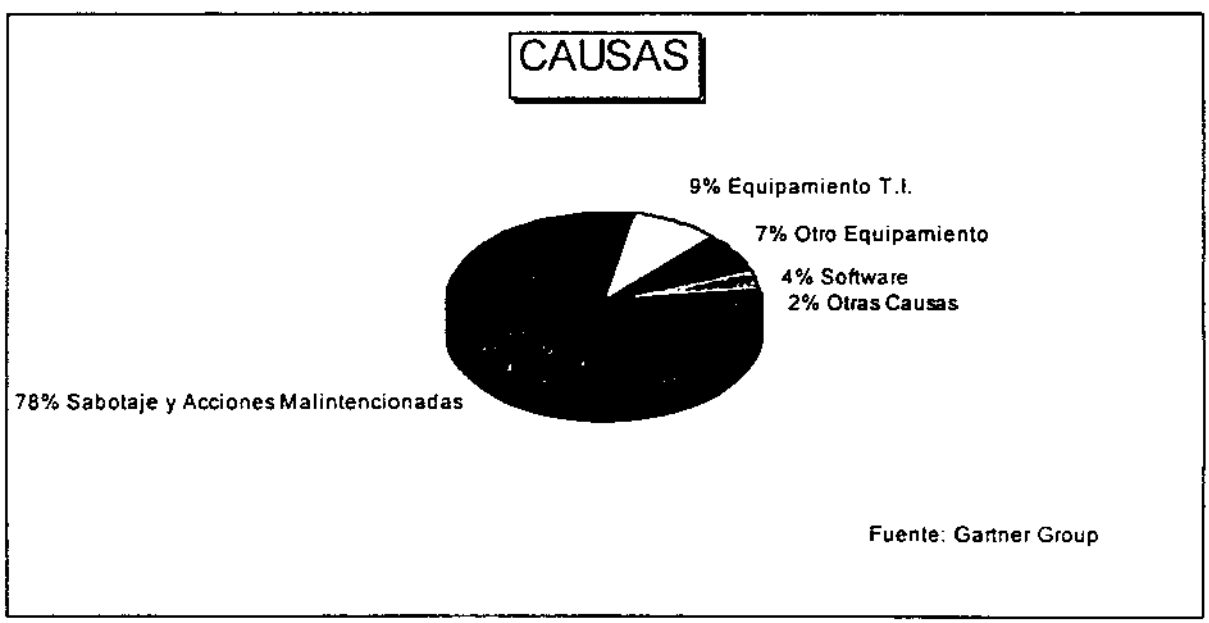
Seguramente hay algunos hechos más, no detallados aquí, que agravan el problema. Pero hay uno que, sin lugar a dudas, puede interesar a los gestores de riesgos: la informática desempeña el papel de amplificador de los siniestros. Cualquier organización, cualquier proceso de trabajo ve modificados sus mecanismos de prevención y de protección cuando se aplican las Tecnologías de la Información a los mismos. A día de hoy es lícito afirmar que hay causas de siniestros propias de la aplicación de la Informática a la vida socio económica; sin ella no se hubiera producido o, al menos, no con la misma amplitud y repercusión.

CAUSAS FINALES DE LOS RIESGOS INFORMÁTICOS

Si analizamos las causas que han originado los siniestros habidos a nivel mundial y, pese a la dificultad que entraña obtener estadísticas de este tipo, podemos aventurar que:

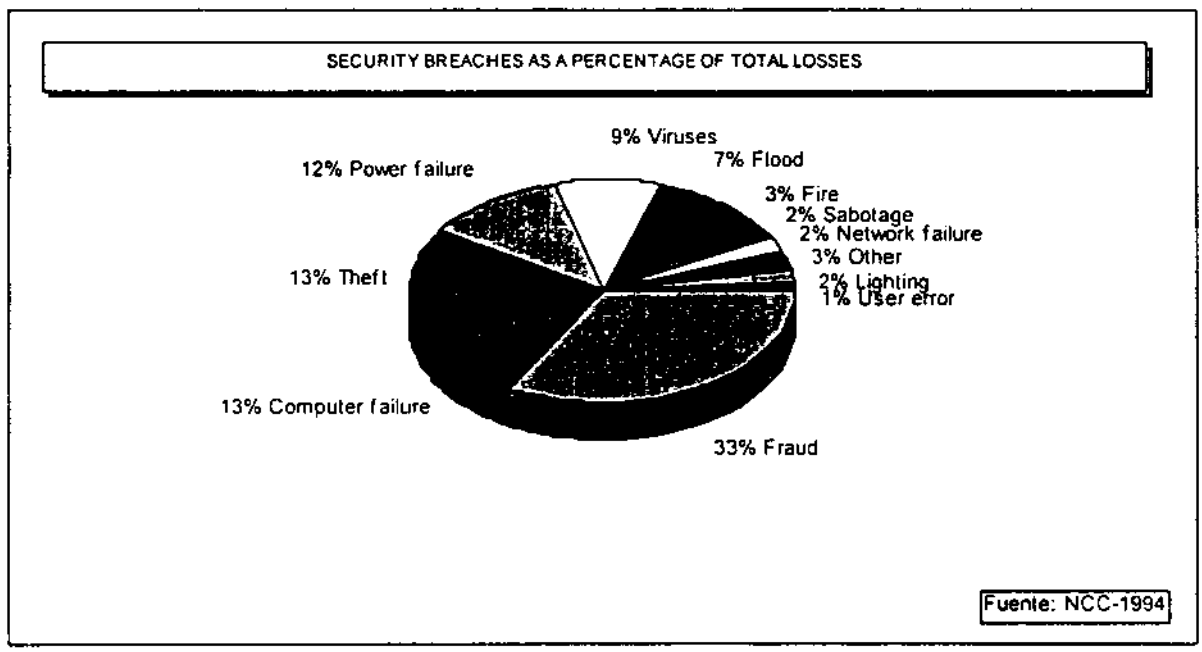
- Solamente un 13 por cien están originados por equipos (9%) y software (4%).
- Un 78 por cien tienen su origen en acciones malintencionadas y sabotajes cometidos tanto por elementos ajenos a las organizaciones como por personal de las mismas.

- El 9 por cien restante tiene su origen en fallos habidos en otro equipamiento de la empresa (7%) y en otras causas no clasificables dentro de los puntos anteriores.



TIPOS DE SINIESTROS, PÉRDIDAS ECONÓMICAS Y FRECUENCIAS

A partir de las conclusiones derivadas de la encuesta realizadas en 1994 en el Reino Unido por el National Computing Center (NCC) puede construirse el siguiente gráfico:



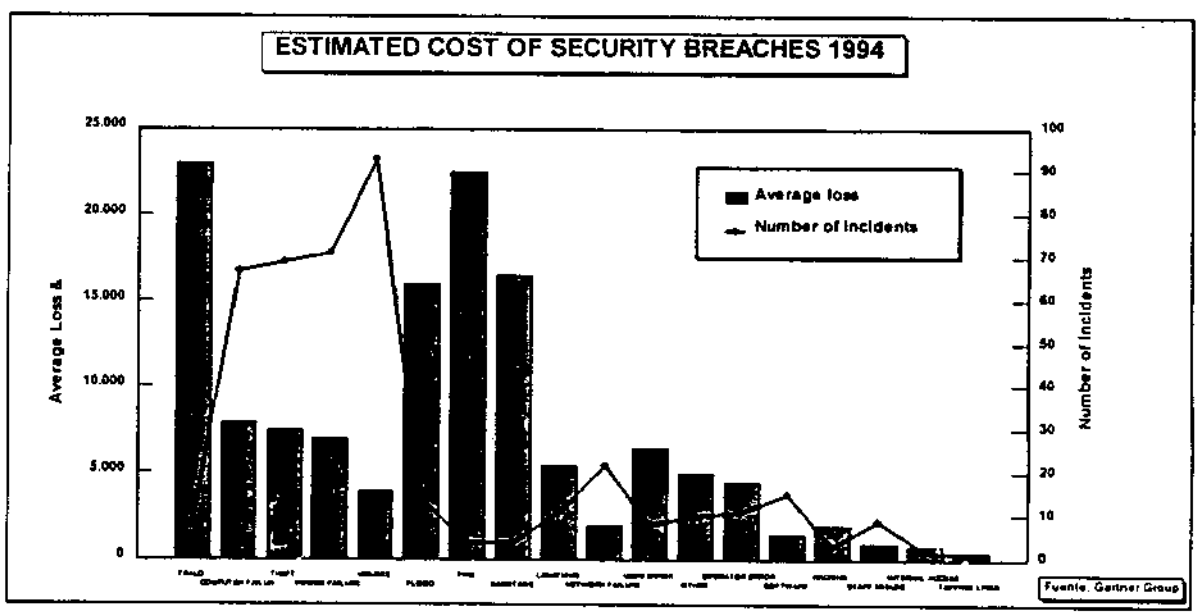
Siempre con la precaución de que la estadística que mostramos está basada en la información que, voluntariamente, los damnificados por los siniestros han reportado al NCC y que puede haber hechos no registrados en el cómputo, se concluye que del total de pérdidas por siniestros informáticos:

- el 33 por cien son debidas a acciones fraudulentas.
- el 13 por cien de las pérdidas son debidas a fallos en los sistemas de ordenador.
- el 13 por cien a robos.
- el 12 por cien a fallos en el suministro de corriente eléctrica.
- el 9 por cien a la contaminación por algún tipo de virus de los sistemas microinformáticos.
- el 7 por cien de las pérdidas es imputable a siniestros provocados por inundaciones y/o avenidas de agua.
- el 3 por cien a incendios.
- el 2 por cien es imputable a los daños ocasionados por sabotaje.
- Otro 2 por cien es imputable a fallos en la red de comunicaciones.
- Una cantidad de pérdidas similar, en porcentaje, a las anteriores es imputable a las descargas eléctricas provocadas por fenómenos atmosféricos de carácter tormentoso.
- ¡Solamente, por fortuna, un 1 por cien de las pérdidas es imputable a causas relacionadas con el mal uso del sistema!
- Y el 3 por cien restante de las pérdidas se pueden clasificar en el apartado de otras causas no contempladas en las anteriores.

Si consideramos sobre las misma base estadística el número de casos registrados, podemos concluir que no existe una relación directa entre el número de siniestros y el valor medio al que asciende la pérdida económica que de ellos se deriva.

Así, por ejemplo, los casos existentes de contaminación por virus son muy elevados y, sin embargo, su repercusión económica es francamente pequeña. En el polo opuesto se encuentran casos como el fuego o el sabotaje, con pocas ocurrencias pero con una repercusión económica elevadísima.

En el siguiente gráfico puede consultarse el número de siniestros habidos frente a la perdida económica media que se deriva de ellos, siempre según el estudio realizado por el NCC



No obstante, esta estadística puede ser significativamente distinta entre unas zonas geográficas y otras.

Es evidente que un factor importante a considerar es el riesgo de exposición a desastres naturales - terremotos, huracanes y tornados, ... - de la región donde se ubica el Centro de Proceso de Datos de cada empresa. También deben considerarse otros factores mas relacionados con la situación política y de clima social, a la hora de evaluar los riesgos potenciales.

LA DISPONIBILIDAD DE LOS SISTEMAS DE INFORMACIÓN

La gran cuestión a la que deben dar respuesta los departamentos de informática de todas las organizaciones ante los riesgos que, como hemos expuesto anteriormente, el uso y aplicación de Tecnologías de la Información al mundo empresarial conlleva es ¿Cómo garantizo el cumplimiento del nivel de servicio a toda mi organización?

El nivel de servicio es la medida, universal y objetiva, por la que se valora la función informática en cualquier compañía. El departamento de informática es, no sólo el garante de la consistencia, integridad y confidencialidad de la información, sino también del rendimiento de los sistemas de información y de la disponibilidad de ésta última para el usuario.

Y todos estos aspectos influyen decisivamente en el nivel de riesgos que una instalación informática presenta.

Los aspectos de seguridad, tanto física como lógica, de una instalación y de la confidencialidad de la información en ella contenida y manipulada son aspectos muy trillados -incluso alguno de ellos sometidos a la legislación - , comprendidos y soportados por lo que no haremos más que mención de ellos en esta exposición.

Otro tanto ocurre con los aspectos relacionados con el rendimiento de los sistemas de información. Los diseñadores y programadores de éstos cada día están más concienciados de que sus trabajos no solamente deben ir orientados a conseguir la funcionalidad requerida por el usuario, sino que también deben contemplar las características de la instalación en donde las aplicaciones que construyen deben ejecutarse, con el fin de que los diseños físicos de las mismas aprovechen al máximo sus capacidades, pero siempre minimizando los recursos requeridos. Los técnicos de sistemas, por otra parte, siempre han orientado sus esfuerzos a gestionar de manera óptima los recursos físicos disponibles en la instalación en relación con el uso que de ellos se demanda.

Ahora bien, el concepto de disponibilidad, y la problemática que le rodea, es mucho más disperso, menos conocido y menos comprendido, incluso por los profesionales del sector.

La disponibilidad absoluta de cualquier sistema de información no existe, de la misma manera que el ser humano no puede controlar la naturaleza o las acciones de otros semejantes suyos; lo que si puede hacer es prever los riesgos que le acechan y dotarse de los medios necesarios para alcanzar ciertos niveles de seguridad en relación a esos riesgos y amenazas. Y en el mundo de la tecnología pasa exactamente igual.

Entendemos por disponibilidad del sistema de información la cantidad de tiempo que éste está funcionando respecto del nivel de servicio comprometido con el usuario. Este término está mediatizado por dos conceptos:

- El mantenimiento preventivo y planificado de los recursos informáticos, a nivel de hardware, software y de datos.

- Los fallos o contingencias imprevistas en cualquiera de su componentes.

Una mala estrategia de mantenimiento puede derivar en un incremento del riesgo de contingencias para la instalación. Y, evidentemente, éstas últimas pueden ir desde el nivel de un pequeño problema que afecta a cualquiera de los componentes del sistema de información, subsanable en pocos minutos, hasta un desastre general en el Centro de Cálculo que lo inhabilite durante días, semanas o, incluso, meses.

¿Nos hemos preguntado que ocurriría en cualquier empresa con un alto grado de informatización de sus procesos si esto último ocurriera? Evidentemente repercutiría de una manera grave en su negocio y no sería extraño que, incluso, pudiera comprometer su supervivencia. Es evidente la necesidad que manifiestan todas las organizaciones de disponer de una estrategia de prevención y de recuperación ante desastres. Hablamos más adelante de ello.

La clase de eventos que pueden provocar falta de disponibilidad en un Centro de Cálculo se categorizan en tres grandes grupos:

- Mantenimiento preventivo.
- Contingencias resolubles a nivel local.
- Desastres.

En el grupo del mantenimiento preventivo se incluyen todas aquellas actividades necesarias para realizar pruebas, modificaciones u operaciones de salvaguarda de información, necesarias para evitar la rotura de componentes. Se pueden incluir aquí otro tipo de actividades encaminadas a dotar a la instalación de los medios y procedimientos necesarios para recuperar la información en caso de anomalía.

A día de hoy existen métodos y tecnología suficientes cómo para garantizar la disponibilidad del sistema, aun cuando estas operaciones se realicen en instalaciones con niveles de servicio comprometido 24 x 7 (veinticuatro horas durante los siete días de la semana; es decir, todo el año sin parar).

En el grupo de las contingencias resolubles a nivel local distinguimos, a su vez, dos subcategorías:

- Punto de fallo
- Frecuencia de fallo

Desde el punto de vista del punto de fallo, se consideran:

- Fallos en la infraestructura.
    - Cortes en el fluído eléctrico
    - Averías en elementos anejos al sistema
- Fallos del hardware, tanto del sistema de ordenador como de su periferia.
- Fallos de las comunicaciones.
- Fallos en el sistema operativo y en los subsistemas.

- Fallos en las aplicaciones, bien sean éstas de desarrollo propio, paquetes estándar o desarrolladas a medida por terceros.

Desde el punto de vista de la frecuencia de fallo podemos considerar los siguientes:

- Fallos recurrentes por error de un componente del sistema, cualquiera que sea éste.
- Fallos puntuales motivados por la baja calidad del componente afectado.

En el grupo de Desastres encuadramos todas aquellas contingencias no resolubles a nivel local. Este tipo de contingencia está relacionado con eventos de carácter violento e inesperado que inhabilitan los recursos informáticos de la organización durante un largo período de tiempo.

MEJORA DE LA DISPONIBILIDAD DE LOS SISTEMAS

¿Cómo podemos protegernos para minimizar los efectos de cualquiera de los siniestros anteriormente descritos?

Evidentemente diseñando los procedimientos y métodos de trabajo adecuados, las arquitecturas de sistemas idóneas e invirtiendo las cantidades económicas necesarias para dotar a la instalación de las tecnologías y recursos humanos requeridos para garantizar los niveles de disponibilidad objetivo.

Existen cuatro niveles de protección que mejoran la disponibilidad, minimizando el impacto de las contingencias resolubles a nivel local:

- Nivel básico.

Puede ser obtenido con un sistema único y unos procedimientos primarios de gestión. La selección de un software y hardware fiables puede ayudar a mejorar la disponibilidad.

- Nivel mejorado.

Basada, también, en un sistema único se dota de mayor robustez mediante la aplicación o redundancia de algún componente del mismo (discos espejados, discos sustituibles en caliente, fuentes de alimentación continua, log de datos/transacciones, etc...). Es evidente que para alcanzar este nivel es necesario disponer de una rigurosa gestión del sistema.

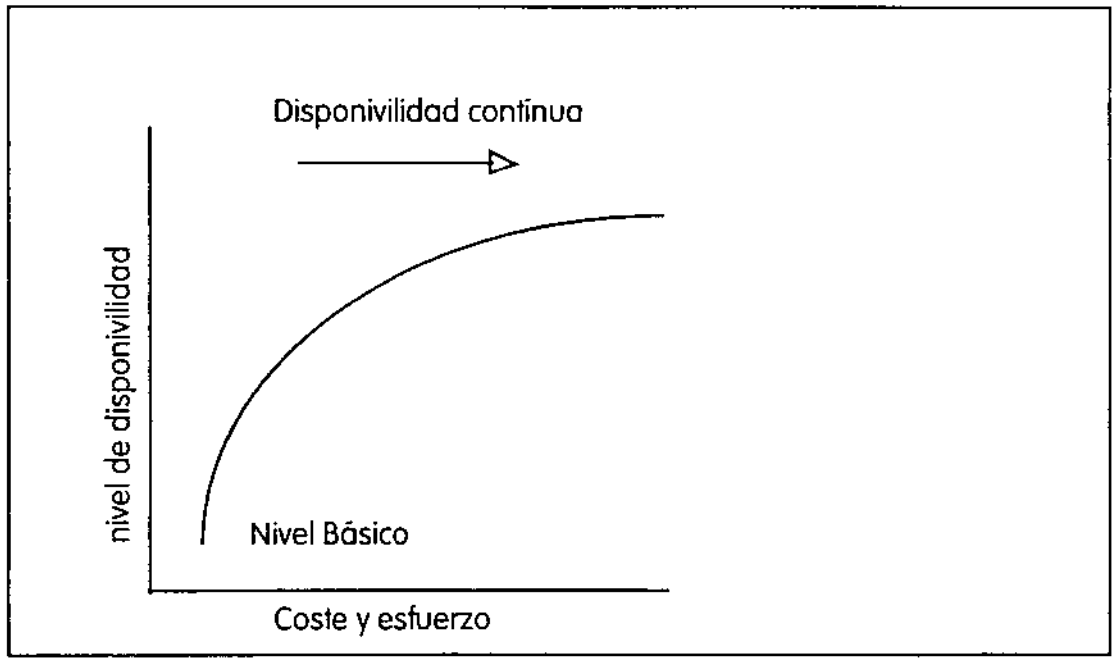
- Alta disponibilidad

En este nivel se intenta dotar a la instalación de los sistemas hardware y software necesarios para suministrar un servicio continuo dentro de una ventana temporal determinada. Generalmente se requiere un alto grado de redundancia en los componentes del sistema de cara a protegerlos de cualquier fallo. Deberá utilizarse una correcta tecnología para automatizar los procesos de recuperación y minimizar los requerimientos de tiempo necesario para ejecutarlos.

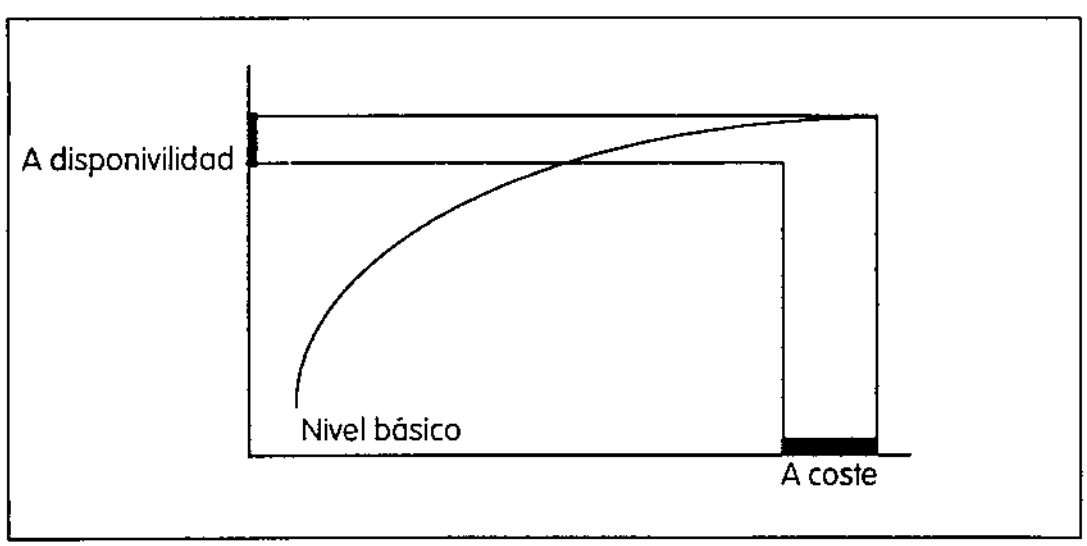
- Disponibilidad continua

En este nivel, el Sistema debe ofrecer servicios de forma permanente, incluso ante casos de cambio de procesos y de recuperación de errores. La redundancia de todos los componentes del sistema es vital para conseguir este nivel.

Ante todo este panorama, la disponibilidad se ve como una función contínua definida por los valores "coste y esfuerzo" (eje de abcisas) y su contraprestación del nivel de disponibilidad alcanzado (eje de ordenadas).



Con relativamente pocas inversiones pueden conseguirse mejoras importantes en la disponibilidad del sistema. A medida que tendemos a la disponibilidad continua el coste crece exponencialmente.



LA RECUPERACIÓN ANTE DESASTRES

A lo largo de la exposición anterior hemos visto como los Centros de Cálculo son en la actualidad componentes críticos para el funcionamiento de cualquier organización, sea cual sea el sector en el que desarrolla su actividad. En consecuencia, la recuperación de sus operaciones en caso de fallo no resoluble a nivel local, constituye una actividad crítica para el negocio.

La recuperación de desastres implica un conjunto de procedimientos, políticas y productos que permitan la reanudación en un tiempo limitado de los elementos informáticos asociados a los procesos de negocio de la empresa, tras una interrupción significativa del servicio.

La presunción fundamental que existe detrás de todo plan de recuperación de desastres es que el lugar físico donde residen los sistemas de ordenador ha sido destruido o no es posible su acceso. En este sentido hay que tener en cuenta no sólo los riesgos a los que está sometido el Centro de Cálculo, sino también los riesgos potenciales que amenazan la zona geográfica en donde éste está instalado.

La recuperación desde la situación de desastre hasta la reanudación de los procedimientos habituales de gestión implica tanto a las unidades de soporte al proceso de datos como a todas las unidades de la entidad que utilizan para su trabajo las aplicaciones informáticas que se procesan en la instalación siniestrada.

Estas últimas deben contar, en función de la previsiones de recuperación del servicio con:

- Los procedimientos de gestión alternativos que deberán emplear hasta que el servicio informático se restaure.
- Los procedimientos de recuperación de datos ante eventuales pérdidas de información, resultantes del intervalo de tiempo transcurrido desde el momento en que se obtuvo la última copia de seguridad válida para proceder a la recuperación del servicio, y el momento del siniestro.

Por otra parte, las unidades de soporte al proceso de datos deben disponer de un conjunto de procedimientos que permitan recuperar las bases de datos y que garanticen la posibilidad de reanudación de los procesos.

Hay varias soluciones para proteger los recursos informáticos críticos. Estas incluyen un rango muy amplio de costes y de tiempo necesarios para el proceso de recuperación.

* Espera caliente

El medio ambiente de esta solución es una instalación cuya utilización está exclusivamente dedicada a la recuperación después de un desastre. No tiene ningún otro uso. Esta instalación puede tener una imagen duplicada del sistema de información completo o, solamente, una parte de éste con la funcionalidad más crítica.

*Sombra de la base de datos

En este caso, la información nueva se manda sobre una red local a una copia remota tan pronto como sea posible. Esta acción es asíncrona respecto a la actualización en el sistema primario, por lo que puede haber inconsistencias entre las bases de datos en el momento del siniestro.

* Espejo de la base de datos

En un sistema con espejo de la base de datos, la información nueva se actualiza de manera síncrona en los sistemas primario y secundario. Puede , por tanto, tener un impacto significativo en el rendimiento del sistema principal, pero garantiza que su copia es exacta en caso de desastre.

* Almacenaje y edición del sistema operativo

En esta solución se mantiene una imagen del sistema operativo de producción en un disco del sitio remoto dedicado a la recuperación de desastresas. Después de un siniestro, se utiliza esta imagen para iniciar el sistema de la "espera caliente". Este método es más rápido que el proceso de restaurar la imagen de las cintas de reserva.

* Traslado electrónico de grandes paquetes de datos

Este traslado consiste en mandar, a través de la red de comunicaciones, las copias de los datos críticos de la instalación al sitio remoto. Evidentemente este proceso optimiza los tiempos necesarios para el transporte de la información y elimina el trasiego de cintas entre las instalaciones.

* Sitio caliente/Sitio frío

Los sitios calientes/fríos son facilidades de proceso de datos alternativas, donde se puede reconfigurar el medio ambiente del sistema primario si ocurre un desastre. El tiempo necesario para recuperar el sistema es variable, en función de la complejidad de la instalación siniestrada.

Ahora bien, ante tanta opción, el dilema que se plantea a los profesionales de las tecnologías de la información es escoger aquella solución que mejor se adapte a las necesidades de su empresa y que, garantizando la recuperación de los sistemas, minimice el coste total de propiedad de éstos últimos.

Para ello, lo primero que debe hacer es preguntarse:

1. ¿Qué características de servicio al cliente presenta mi negocio?
2. ¿Cuáles son los sistemas de información críticos en la organización?
3. ¿Cuánto tiempo es posible operar sin sistemas de información hasta que el servicio pueda ser restablecido?
4. Una vez restablecido el servicio, ¿Cuál es el tiempo máximo que la empresa puede soportar con una situación de contingencia en su proceso de datos?

Seguramente con estas respuestas en la mano y con el conocimiento profundo de las distintas soluciones que la tecnología ofrece a día de hoy, podrá aproximar su mejor opción. No obstante, antes de tomar una decisión definitiva, sobre la solución escogida debería constatar:

- La integridad de la información que provee.
- El nivel de automatización de los procesos de notificación de fallos y de toma de control por una segunda máquina en caso de que estos ocurran.
- El tiempo de demora necesario para la restauración del servicio.
- La distancia máxima admisible para la ubicación de un centro de respaldo.
- La escalabilidad del sistema.
- La relación coste del tiempo perdido a causa del siniestro, comparado con los costes de instalación y mantenimiento del sistema de salvaguarda.
- La eficacia y eficiencia de la solución en el proceso de restauración del servicio.

UNA VISIÓN SECTORIAL

Los distintos sectores de actividad económica presentan diferentes grados de necesidad para adoptar una solución de recuperación ante desastres.

Pese a que no existe una legislación específica que regule tales salvaguardas, si existen ciertas características de los negocios que ejercen una presión considerable sobre la dirección de las empresas a la hora de diseñar, desarrollar, probar e implantar una solución de recuperación:

- La banca de negocios tiene la presión de los auditores y de los bancos centrales para operar de manera continua.
- Además de ello, la banca de particulares necesita de continuidad en las ventas, tanto directas como a través de medios electrónicos.
- El mundo del Seguro también necesita de continuidad en las ventas.
- Para el sector de fabricación es vital asegurar el control de los stocks para garantizar el "Just in Time" de su producción así como el asegurar la distribución de los bienes fabricados.
- Para el comercio, el aseguramiento de su cadena logística es vital para la continuidad de su negocio. Esto incluye desde el aprovisionamiento hasta la venta.
- El sector transporte necesita la continuidad en las operaciones de venta de billetaje y en la logística de materiales de mantenimiento, como parte fundamental de la seguridad de los viajeros.

Como consecuencia de las características y presiones anteriores, a nivel mundial, las distintas industrias presentan grados de necesidad diferentes a la hora de considerar la recuperación ante desastres:

- Banca, Seguros y Comercio encabezan el ranking de "sectores mas necesitados"
- Transportes y Fabricación presentan menores índices de necesidad.

Sin embargo, solamente la banca -tanto la de particulares como la de negocios- está preparada para la recuperación ante desastres en la misma que los requerimientos y características de su actividad empresarial manifiestan.

También hablando en términos generales, podemos tipificar las soluciones técnicas utilizadas en cada uno de los sectores:

- El mundo de la Banca de negocios necesita restaurar rápidamente sus operaciones, aunque no hasta el punto inmediatamente anterior al siniestro. Por lo general, aplican soluciones de sitio caliente/sitio frío.
- Tanto el mundo de la Banca de particulares como el Comercio necesitan restaurar rápidamente (en menos de 2 horas) sus operaciones hasta el punto inmediatamente anterior al siniestro. Por lo general, una solución mixta de segundo centro de proceso, con bases de datos espejo y sistema en "espera caliente" es la que típicamente aplican.

- El sector asegurador, por contra, no tiene especiales necesidades de velocidad de recuperación de la contingencia, aunque si de restaurar los sistemas hasta el momento en el que el siniestro se produce. Es usual la aplicación de técnicas de salvaguarda de los datos en cinta o disco para su restauración en caso de siniestro y de espejo de las bases de datos.

Este panorama tiene su correspondiente reflejo económico. Mientras, según datos de Giga Group, la media del gasto anual en recuperación de desastres de todos los sectores económicos es de un 3 ó 4 por cien del Total de gastos en informática, en la banca esta cantidad llega a elevarse hasta el 7 por cien.

Si analizamos en detalle estos datos, podemos concluir que el incremento de gastos viene motivado, entre otras cosas, por el uso intensivo que de los sistemas de telecomunicación ha de hacer la Banca para alcanzar sus garantías de respaldo ante desastres.

PLAN DE RECUPERACIÓN DEL NEGOCIO VERSUS RECUPERACIÓN DE DESASTRES

El Plan de Recuperación de Desastres encaja dentro de un Contexto más amplio de reanudación completa del negocio. Tradicionalmente, el primero de ellos se centra en la recuperación de los sistemas de información; el segundo se deriva de la conciencia, cada vez mayor, de la necesidad imperativa de continuar la operación de los negocios de empresa.

Este modelo de continuidad del negocio pretende asegurar que una interrupción inevitable del mismo sea transparente a los elementos clave de la compañía, incluyendo clientes, proveedores, accionistas y empleados.

Así, el modelo completo de continuidad del negocio, puede estructurarse de la siguiente manera:

Las diferencias entre la recuperación de desastres y la continuidad del negocio estriban, más que en el "Qué hay que hacer", en el "Quién es el responsable de hacerlo".

La continuidad del negocio afecta a toda la compañía, no sólo al Centro de Cálculo y a los responsables de los sistemas de información; pone énfasis en la capacidad de recuperar la funcionalidad, no sólo en las aplicaciones informáticas; implica un proceso para establecer prioridades de negocio, no de salvaguarda de los sistemas informáticos exclusivamente y, además, su planificación debe considerar a clientes, proveedores, aspectos económicos y de organización, no centrándose exclusivamente en los aspectos tecnológicos y de relación entre los técnicos y los usuarios finales.