Unidad III: Seguridad de la Información
3.2 Administración de respaldos
3.3 Almacenamiento Masivo de Información
3.4 Alta Disponibilidad
3.5 Resguardo de Medios
3.6 Bóvedad Electronica de Datos

SEGURIDAD LÓGICA

Luego de ver como nuestro sistema puede verse afectado por la falta de seguridad física, es importante recalcar que la mayoría de los daños que puede sufrir un centro de cómputo no será sobre los medios físicos sino contra información por él almacenada y procesada; esta es el activo más importante que se posee, y por lo tanto deben existir técnicas, más allá de la seguridad física que la aseguren.
La Seguridad Lógica consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo".

Los objetivos que se plantean serán:

1. Restringir el acceso a los programas y archivos
2. Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
3. Asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto.
4. Que la información transmitida sea recibida por el destinatario al cual ha sido enviada y no a otro.
5. Que la información recibida sea la misma que ha sido transmitida.
6. Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
7. Que se disponga de pasos alternativos de emergencia para la transmisión de información.

Administración de respaldos

Un respaldo o backup es el resguardo final contra cualquier falla del sistema o pérdida de la información. Como sabemos, un respaldo de archivos permite tener disponible e íntegra la información para cuando sucedan los accidentes. Sin un backup es imposible volver la información al estado anterior al desastre.

No sólo es necesario respaldar, se necesita llevar a cabo toda una administración de respaldos que ayudaría a disminuir costos y a llevar un mejor control de nuestra información. Para manejar los respaldos se deben considerar los siguientes puntos:

- Ante que nada es recomendable hacer un escaneo de vulnerabilidades internas y externas para conocer los puntos débiles de la organización en cuanto a software y poder ofrecer soluciones integras de seguridad.

- Se debe hacer un análisis de riesgo; el cual implica:
    - Determinar que es lo que se necesita proteger, así como el nivel de riesgo de cada elemento.
    - Se debe identificar la fuente de amenazas de las cuales se está protegiendo la información (las verdaderas pérdidas son causadas por los usuarios internos).
    - Determinar la forma de proteger nuestra información.

- Se debe establecer una política de seguridad con la finalidad de asegurar que los esfuerzos dedicados a la seguridad impliquen un costo razonable. Esta política establecerá la continuidad con la que se harán los respaldos, los medios y el procedimiento para llevarlos a cabo.

- Por último se debe llevar un control de los respaldos hechos.

Riesgos

Los riesgos deben clasificarse por nivel de importancia y gravedad de la perdida. No debe terminar en una situación en la que se gaste más en proteger algo que es de menor valor para el centro.

Algunos de los componentes estudiados en una Análisis de Riesgos son:

- ***Riesgo:*** es el potencial que tiene una amenaza de explotar las vulnerabilidades asociadas con un activo, comprometiendo la seguridad de éste.
- ***Activo:*** es un componente relacionado con la información, el cual tiene un valor asignado por la entidad directamente relacionada con éste. Dicho valor representa el nivel de importancia que tiene el activo en el "proceso del negocio".
- ***Vulnerabilidad:*** es una debilidad en las Tecnologías de Información que hace susceptible un activo a una amenaza.
- ***Amenaza:*** es un evento, acción o agente que puede comprometer a un activo
- ***Impacto:*** es la magnitud en que afecta la materialización de un riesgo.

Partiendo de estos principios, se obtiene la siguiente relación:
Riesgo = Valor Información x Amenaza x Vulnerabilidad

TIPO DE RIESGO	FACTOR DE RIESGO
Equivocaciones	Medio
Virus	Medio-Alto
Fallas en equipos	Medio
Variaciones de fluido eléctrico	Medio
Accesos	Bajo
Robo de datos	Bajo
Vandalismo	Bajo
Robo común	Bajo
Al fuego	Medio-Bajo
Terremotos	Bajo

Respaldo de la información

Un respaldo regular requiere tomar este tipo de precauciones al menos una vez cada jornada laboral, o con mayor frecuencia si se trata de información crítica, como durante el desarrollo de una jornada electoral. La información puede ser respaldada en muy distintos formatos: discos removibles de diverso tipo, discos duros múltiples o cintas magnéticas, por ejemplo.

La estrategia integral de tecnología informativa de la organización puede estructurar un régimen formal de respaldo. Lo ideal es que el respaldo funcione de manera automática para asegurar que los errores humanos no causen problemas. Sin embargo, seguirá siendo necesaria una revisión periódica de los respaldos automáticos para asegurar que los errores de la computadora no causen problemas.

La información "viva" puede ser respaldada al mismo tiempo que es creada, utilizando un disco duro como espejo, que puede estar localizado en el mismo servidor o en uno distinto. Al utilizar discos espejo, la misma información es almacenada de manera simultánea en dos o más discos. Esto significa que si un disco falla, la información puede ser restaurada de otro. Es preferible utilizar servidores separados para los discos espejo, ya que el segundo se puede utilizar si el primero falla completamente.

Los programas, tanto los comerciales como los desarrollados internamente, también pueden ser respaldados para que se puedan recargar si las versiones originales se pierden o dañan. La

mayoría de los programas vienen cargados en discos. Sin embargo es cada vez más frecuente que los programas se puedan descargar de Internet. En este caso las copias de respaldo deben ser almacenadas localmente, ya que no existe garantía de que estarán disponibles en línea en el futuro. Los discos de programa que son almacenados en una biblioteca administrada por una unidad u oficial responsable pueden ser fácilmente ubicados y utilizados, de ser necesario.
Cuando se respalda la información de programas, se debe tener cuidado de no violar los permisos legales. La mayoría de las licencias o permisos legales permiten conservar copias de respaldo.

Clasificación de Respaldos

- **Copias** de Información, comúnmente llamados (**Backups**).
- Duplicados de Información **en línea** (Implementación **RAID**)

Copias de Información (Backups)

Estos respaldos son sólo duplicados de archivos que se guardan en "Tape Drives" de alta capacidad (30-40 GB aprox.). Los archivos que son respaldados pueden variar desde archivos del sistema operativo, bases de datos, hasta archivos de un usuario común. Existen varios tipos de Software que automatizan la ejecución de estos respaldos, pero el funcionamiento básico de estos paquetes depende del denominado *archive bit*.

Este *archive bit* indica un **punto de respaldo** y puede existir por archivo o al nivel de "Bloque de Información" (típicamente 4096 bytes), esto dependerá tanto del software que sea utilizado para los respaldos así como el archivo que sea respaldado.

Este mismo *archive bit* es activado en los archivos (o bloques) cada vez que estos sean modificados y es mediante este *bit* que se llevan acabo los tres tipos de respaldos comúnmente utilizados:

- **Respaldo Completo ("Full"):** Guarda todos los archivos que sean especificados al tiempo de ejecutarse el respaldo. El *archive bit* es eliminado de todos los archivos (o bloques), indicando que todos los archivos ya han sido respaldados.
- **Respaldo de Incremento ("Incremental"):** Cuando se lleva acabo un Respaldo de Incremento, sólo aquellos archivos que tengan el *archive bit* serán respaldados; estos archivos (o bloques) son los que han sido modificados después de un Respaldo Completo. Además cada Respaldo de Incremento que se lleve acabo también eliminará el *archive bit* de estos archivos (o bloques) respaldados.
- **Respaldo Diferencial ("Differential"):** Este respaldo es muy similar al "Respaldo de Incremento", la diferencia estriba en que el *archive bit* permanece intacto.

Respaldo	**Archivos en Respaldo**	***Archive Bit***	**Ventajas**	**Desventajas**
Completo ("Full")	Todos	Eliminado en todos los archivos	Con este respaldo únicamente es posible recuperar toda la información	Tiempo de Ejecución
De Incremento ("Incremental")	Archivos con *archive bit* activo.(Aquellos que hayan cambiado desde el último Respaldo Completo)	Eliminado en los archivos que se respaldan	Velocidad	Requiere del último Respaldo Completo y de todos los Respaldos de Incremento que le siguieron para recuperar el Sistema

Diferencial ("Differential")	Archivos con *archive bit* activo.(Aquellos que hayan cambiado desde el último Respaldo Completo)	Intacto	Sólo requiere del último Respaldo Completo y del último respaldo Diferencial	Ocupa mayor espacio en discos comparado con Respaldos de Incremento

Secuencia de Respaldo GFS (Grandfather-Father-Son)

Esta secuencia de respaldo es una de las más utilizadas y consiste en *Respaldos Completos* cada semana y *Respaldos de Incremento o Diferenciales* cada día de la semana.

Para una correcta realización y seguridad de backups se deberán tener en cuenta estos puntos:

Se debe contar con un procedimiento de respaldo de los sistemas operativos y de la información de los usuarios, para poder reinstalar fácilmente en caso de sufrir un accidente.

Se debe determinar el medio y las herramientas correctas para realizar las copias, basándose en análisis de espacios, tiempos de lectura/escritura, tipo de backup a realizar, etc.

- El almacenamiento de los Backups debe realizarse en locales diferentes de donde reside la información primaria. De este modo se evita la pérdida si el desastre alcanza todo el edificio o local.
- Se debe verificar, periódicamente, la integridad de los respaldos que se están almacenando. No hay que esperar hasta el momento en que se necesitan para darse cuenta de que están incompletos, dañados, mal almacenados, etc.
- Se debe contar con un procedimiento para garantizar la integridad física de los respaldos, en previsión de robo o destrucción.
- Se debe contar con una política para garantizar la privacidad de la información que se respalda en medios de almacenamiento secundarios. Por ejemplo, la información se puede encriptar antes de respaldarse.
- Se debe contar con un procedimiento para borrar físicamente la información de los medios de almacenamiento, antes de desecharlos.
- Mantener equipos de hardware, de características similares a los utilizados para el proceso normal, en condiciones para comenzar a procesar en caso de desastres físicos. Puede optarse por:
    - Modalidad Externa: otra organización tiene los equipos similares que brindan la seguridad de poder procesar la información, al ocurrir una contingencia.
    - Modalidad Interna: se tiene más de un local, en donde uno es espejo del otro en cuanto a equipamiento, características técnicas y capacidades físicas. Ambos son susceptibles de ser usados como equipos de emergencia.

En todos los casos se debe asegurar reproducir toda la información necesaria para la posterior recuperación sin pasos secundarios ni operación que dificulte o imposibilite la recuperación.

Control

Se debe tener:

- Una forma de etiquetar los soportes
- Registro/Control del backup, uso de soportes
- Guarda de los soportes de backups en línea
  - Dónde se guardan
  - Ciclo diario de traslado a los lugares de guarda
  - Responsables del traslado
  - Por qué lugar deben ser retirados.
- Guarda de los soportes de backups históricos
  - Dónde se guardan
  - Ciclo mensual de traslado a los lugares de guarda
  - Responsables del traslado
  - Por qué lugar deben ser retirados.

- Autorización al personal encargado de los traslados
  - Quién debe mantener las listas actualizadas y cómo hacerlo.

Nro.0000	**Ficha de Backups** **Nombre:**	

Nivel de Seguridad	**Alto** ☐	**Medio** ☐	**Bajo** ☐	**Fecha de Creación:** / /

Unidad o Dpto:
Tipos de Archivos contenidos:
Medio de almacenamiento: **CD-R** ☐ **CD-RW** ☐ **ZIP** ☐ **OTRO:**
Aplicación o Sistema (que lo lee)**:**
Ordenado por:
INCIDENCIAS

Fecha	**Descripción**	**Responsable**	**MB**
/ /			
/ /			
/ /			
/ /			

ALMACENAMIENTO MASIVO DE INFORMACIÓN

En la actualidad las organizaciones son capaces de generar, almacenar y utilizar información ilimitada importante para sus operaciones. Una de las cosas que más preocupa a los usuarios de computadores, es la capacidad de los dispositivos de almacenamiento, con la finalidad de

conservar la integridad de los datos que se manejan en la organización. En la actualidad se tienen varios dispositivos para almacenamiento y protección de datos.

Dado el incremento de las necesidades de los usuarios, los fabricantes se han visto en la necesidad de realizar inversiones en tecnología para diseñar dispositivos de almacenamiento con mayores capacidades y más sofisticados. El mercado ofrece gran diversidad de equipos de almacenamiento entre los que destacan los discos duros, las cintas magnéticas, los discos de cartuchos removibles, disquetes, flash- cards, discos ópticos y DVD.

Los dispositivos de almacenamiento son unidades periféricas del sistema que se utilizan como medio de soporte para el almacenamiento de datos, archivos y programas, que son manejados por las aplicaciones que utilizan los sistemas. Estas unidades pueden ser internas al computador o externas en carcasas. También es bueno mencionar que dado a los grandes volúmenes de información que manejan algunas organizaciones, existen sistemas automatizados de gestión de archivos de unidades de almacenamiento.

Medios de almacenamiento magnético.

Entre los medios de almacenamiento magnético mas conocidos se encuentran los discos duros, los disquetes y las cintas magnéticas.

Consisten básicamente en varias láminas rígidas de forma circular. Estas láminas están recubiertas de un material que posibilita la grabación magnética de los datos. Las cabezas de lectura y escritura se mueven por esta superficie magnética "apoyadas" en una burbuja de aire.

Existen básicamente dos tipos de discos duros: los IDE y los SCSI. Las principales diferencias entre ellos son, para no entrar en muchos detalles, la velocidad de acceso a los datos grabados, la calidad en general y, sobre todo, el precio. En los tres aspectos los discos SCSI son ampliamente superiores a los IDE.

Las cintas han sido y todavía lo son, la manera más efectiva en costos para que las empresas respalden y recuperen sus datos. Con las necesidades de almacenamiento de datos duplicándose cada año para la mayoría de compañías, las cintas continuarán siendo una solución viable, ya que proveen a los usuarios finales la capacidad, confiabilidad y velocidad necesarias para almacenar y proteger la creciente cantidad de datos que se generan. Hoy en día, los cartuchos de cintas high-end tienen más de 500 carriles de datos que almacenan hasta 200,000 bits por pulgada. La velocidad de transferencia de datos se ha incrementado a 30 Megabytes por segundo (MB/sec) y la capacidad se ha incrementado a más de 200 Gigabytes en un solo cartucho con cartuchos de terabyte y multi-terabyte para el final de la década.

Duplicado de Información en Línea (RAID)

RAID ("Redundant Array of Inexpensive Disks") en términos sencillos es: un conjunto de 2 o más "Discos Duros" que operan como grupo y logran ofrecer una forma más avanzada de respaldo ya que:

- Es posible mantener copias *en línea* ("redundancia").
- Agiliza las operaciones del Sistema (sobre todo en bases de datos.)
- El sistema es capaz de recuperar información sin intervención de un Administrador.

Existen varias configuraciones de Tipo RAID, sin embargo, existen 4 tipos que prevalecen en muchas Arquitecturas:

- **RAID-0:** En esta configuración cada archivo es dividido ("Striped") y sus fracciones son colocadas en diferentes discos. Este tipo de implementación sólo agiliza el proceso de lectura de archivos, pero en ningún momento proporciona algún tipo de respaldo ("redundancia").

- **RAID-1:** En orden ascendente, este es el primer tipo de RAID que otorga cierto nivel de respaldo; cada vez que se vaya a guardar un archivo en el sistema éste se copiara *integro* a DOS discos (en línea), es por esto que RAID-1 también es llamado "Espejo".

Además de proporcionar un respaldo en caliente ("hot") en dado caso de fallar algún disco del grupo, *RAID-1* también agiliza la lectura de archivos (si se encuentran ocupadas las cabezas de un disco "I/O") ya que otro archivo puede ser leído del otro disco y no requiere esperar a finalizar el "I/O" del primer disco.

- **RAID-3:** Esta configuración al igual que RAID-0 divide la información de todos los archivos ("Striping") en varios discos, pero ofrece un nivel de respaldo que RAID-0 no ofrece. En *RAID-0* si falla un disco del grupo, la Información no puede ser recuperada fácilmente, ya que cada disco del grupo contiene una fracción del archivo, sin embargo *RAID-3* opera con un disco llamado "de paridad" ("parity disk").

  Este "disco de paridad" guarda fracciones de los archivos necesarias para recuperar toda su Información, con esto, es posible reproducir el archivo que se perdió a partir de esta información de paridad.

- **RAID-5:** El problema que presenta RAID-3 es que el "disco de paridad" es un punto crítico en el sistema; que ocurre si falla el disco de paridad.

  Para resolver este problema *RAID-5*, no solo distribuye todos los archivos en un grupo de discos ("Striping"), sino también la información de paridad es guardada en todos los discos del sistema ("Striping"). Este configuración RAID suele ser usada en sistemas que requieren un *"alto nivel"* de disponibilidad, inclusive con el uso de "Hot-Swappable Drives" es posible sustituir y recuperar la Información de un disco dañado, con mínima intervención del Administrador y sin la necesidad de configurar o dar "reboot" al sistema.

Observando la evolución de los discos de las unidades de almacenamiento externo, tenemos el IOMEGA ZIP con una capacidad de 100MB y 250MB, seguidas por la unidad JAZ con capacidad de hasta 2GB y el CASTLEWOOD que puede almacenar hasta 2,2 GB; estas unidades poseen gran capacidad de almacenamiento y facilidad de transporte, pero tiene en contra que no todas las maquinas poseen este tipo de unidades para leer la información. También tenemos entre los dispositivos de almacenamiento magnético a los disquetes utilizados como medios de almacenamiento secundario en microcomputadoras, cuyo uso ha sido generalizado por su facilidad de manejo y bajo costo, aunque su capacidad de almacenamiento es muy baja.

Tarjetas PC-Card

Una de las mejores opciones que tienen los usuarios, en lo que se refiere a almacenamiento y transporte de datos haciendo intercambio de información en vivo son las PC-Card, dispositivos de almacenamiento de información, que se encuentran basados en discos duros diminutos del tamaño de una tarjeta de crédito, estas se utilizan generalmente para el almacenamiento de datos que manejan equipos portátiles y para la transferencia de información entre equipos portátiles y equipos de sobremesa. Su capacidad aproximada es de 720 MB.

Discos Ópticos

Los discos ópticos son dispositivos de almacenamiento para grandes sistemas electrónicos de archivos. Tiene como diferencia contra otros métodos de almacenamiento que este es no magnético. Estos dispositivos son utilizados para trabajar con grandes bases de datos, con aplicaciones que requieren almacenamiento de archivos de voz y vídeo, mediante el cual se pueda almacenar, localizar, transmitir, procesar y administrar documentos. Existen diferentes tipos de unidades de discos ópticos:

- de lectura
- de lectura y una sola escritura
- de lectura y escritura.

Las unidades de CD-RW, pueden grabar CD´s a una velocidad de 52x y leerlos a una velocidad de 52x, lo que significa que esta unidad puede ser capaz de sustituir la actual unidad de CD-ROM. La flexibilidad es otra de las cualidades que nos presentan estas unidades, ya que utilizándolas podemos leer CD-ROM y escribir tanto en medios CD-R y los CD-RW. Además existe un tipo de CD-RW, que han sido diseñadas para leer los DVD-ROM. También se debe hacer notar que solamente la última generación de CD-ROM, puede leer los CD-RW, otra ventaja es que la información que se escriba en uno de esos discos puede durar entre 70 y 200 años, lo cual los hace ideales para la conservación de archivos, también sobre uno de estos discos se puede rescribir hasta 1000 veces.

DVD

Los aspectos más impactantes del DVD son su capacidad, su interoperabilidad y su compatibilidad retroactiva. Los fabricantes han diseñado las unidades de DVD tal que puedan leer también los CD-ROM de modo que las personas no pierdan la inversión realizada en los CD.

Además el formato de datos y tecnología láser utilizados para el software DVD y para unidades PC, serán los mismos que se utilizan para los reproductores DVD y para los títulos que se distribuyen en el área de los equipos electrónicos para el hogar. Ademas están los DVD regrabables de 10 GB, para este año se esperan los DVD de 50 GB y para el 2006 los de 100GB.

Referencias:

Imation de Latinoamérica
http://latinamerica.imation.com

Avances en los sistemas de almacenamiento masivo de información.
http://neutron.ing.ucv.ve/revista-e/No7/Randy%20Miliani%5Carticulo3.htm.

Alta Disponibilidad

Concepto

Nos referimos a alta disponibilidad (en inglés High Availability) a los sistemas que nos permiten mantener nuestros sistemas funcionando las 24 horas del día, manteniéndolos a salvo de interrupciones.

Debemos diferenciar dos tipos de interrupciones en nuestros sistemas.

- **Las interrupciones previstas.**
  Las que se realizan cuando paralizamos el sistema para realizar cambios o mejoras en nuestro hardware o software.
- **Las interrupciones imprevistas**
  Las que suceden por acontecimientos imprevistos (como un apagón, un error del hardware o del software, problemas de seguridad, un desastre natural, virus, accidentes, caídas involuntarias del sistema)

Y distintos niveles de disponibilidad del sistema:

- **Los sistemas de la disponibilidad base:** El sistema está listo para el uso inmediato, pero experimentará tanto interrupciones planificadas como no planificadas.

- **Los sistemas de disponibilidad alta:** Incluyen tecnologías para reducir drásticamente el número y la duración de interrupciones imprevistas. Todavía existen interrupciones planificadas, pero los servidores incluyen herramientas que reducen su impacto.
- **Entornos de operaciones continuas**
  Utilizan tecnologías especiales para asegurarse de que no hay interrupciones planificadas para backups, actualizaciones, u otras tareas de mantenimiento que obliguen a no tener el sistema disponible.
- **Los sistemas de la disponibilidad continua**
  Van un paso más lejos para asegurarse de que no habrán interrupciones previstas o imprevistas que interrumpan los sistemas. Para alcanzar este nivel de la disponibilidad, las compañías deben utilizar servidores duales o los clusters de servidores redundantes donde un servidor asume el control automáticamente si el otro servidor cae.
- **Los sistemas de tolerancia al desastre**
  Requieren de sistemas alejados entre sí para asumir el control en cuanto pueda producirse una interrupción provocada por un desastre.

Por qué necesitamos la Alta Disponibilidad

Las razones para ello son básicamente dos:

- Las aplicaciones altamente críticas
- Los paros planificados.

Los sistemas informáticos como ya sabemos son vulnerables y están sometidos a una serie de peligros reales (virus informáticos, fallos de electricidad, errores de hardware y software, caídas de red, piratas informáticos, errores humanos, incendios, inundaciones ver tabla 1) y en cualquier momento nuestro sistema puede quedar total o parcialmente no operativo como consecuencia de cualquier incidencia.

Existen empresas que pueden permitirse estar no operativas durante horas, aunque existen sectores de negocios que no pueden permitirse la más mínima interrupción (banca, hospitales, logística, transporte, comercio electrónico…).

Si tu empresa está en el grupo de las que se puede permitir estar no operativas durante horas, no olvides diseñar un plan de recuperación o contingencia que te garantice que las pérdidas de datos y consecuentemente el coste de la interrupción van a ser mínimas. Asegúrate de disponer de copias de seguridad de tus ficheros, seguridad, configuraciones, programas y sus fuentes, por lo menos diarias y evidentemente un SAVSYS. Mantén las copias de seguridad en lugar seguro y a ser posible en una ubicación distinta del ordenador de producción.

El cálculo de los costes de los tiempos muertos requiere estimar las pérdidas de los ingresos, los costes del personal y los costes intangibles, causados por un fallo del sistema y sumar las tres partidas.

Paso 1. Calcular las pérdidas de ingresos.
Existe un método simple y otro método más complejo para calcular las pérdidas. La fórmula simple calcula primero el ingreso por una hora de funcionamiento del negocio:
Ingresos = Ingreso anual total / Horas hábiles de negocio al año
dónde ingresos son calculados en Ptas. por hora y las horas hábiles al año se calculan con la siguiente fórmula:

Horas de negocio al año = horas de negocio al día
* días de negocio al mes
* meses de negocio al año

Después, para obtener la cifra de perdida de ingresos, multiplicamos los ingresos por

hora por el número de horas de tiempo muerto.

Un ejemplo: Un negocio funciona de 8 a.m. a 8 p.m., de lunes a sábado, todas las semanas del año. Los ingresos por ventas del año pasado fueron de 6.000 millones de Ptas. Si procesamos estos datos con nuestra ecuación obtenemos:
Ingresos = Ptas. 6.000.000.000
/ (12 horas al día * 22 días al mes * 12 meses al año)
= Ptas. 6.000.000.000 / 3.168 horas
= Ptas. 1.893.939
El ingreso por hora asciende a Ptas. 1.893.939. De acuerdo con éste cálculo, una incidencia de 12 horas de tiempo muerto, implica una pérdida de ingresos que asciende a Ptas. 22.727.268 (12 horas por 1.893.939 Ptas.)
El considerar que el negocio no genera ingresos, mientras el sistema no esté disponible, es indudablemente una suposición importante. Pero como mínimo, este enfoque nos da un punto de partida y unos datos estadísticos, para comprender el valor de cada hora disponible de la organización.

<!--[if !supportLineBreakNewLine]-->
<!--[endif]-->

- **Paso 2. Calculo de costes de personal.**
  Otro factor a considerar, cuando calculamos los costes de los tiempos muertos, son los costes de personal generados mientras el sistema no estaba disponible. Puede insertar sus datos en la fórmula presentada a continuación, para computar la pérdida laboral:

  Pérdida laboral = numero de personas * % de horas afectado * numero de horas * Ptas./hora/empleado
  dónde Ptas./hora/empleado es el coste por hora de empleado, definido cómo:
  Ptas./hora/empleado = paga por hora + beneficios soc. + imputación gtos. fijos

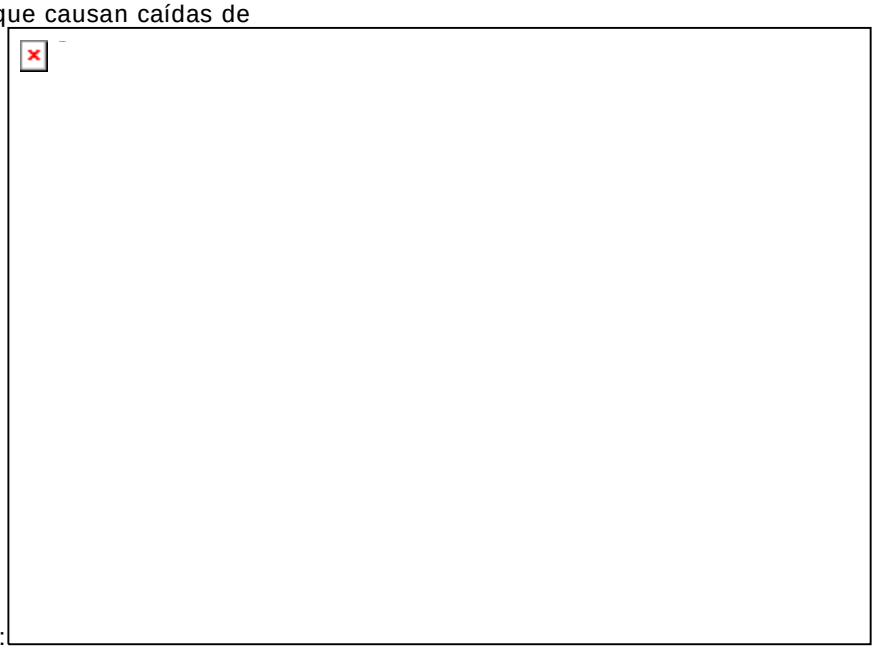
  Por ejemplo, supongamos que en la empresa, el coste total promedio por empleado por hora es de Ptas. 2.500. Si 50 empleados son afectados en un 50% durante las primeras 2 horas del fallo del sistema, 100 personas se ven afectadas en un 75% por las próximas 2 horas y 200 personas pierden todo su tiempo (100%), cuando el fallo dura más de 4 horas, un tiempo muerto de 12 horas costaría a la empresa Ptas. 4.500.000. Dividiendo este coste total de personal, entre el número de horas que duró la incidencia (12), obtenemos el coste promedio por hora: Ptas. 375.000. Esto quiere decir que cada hora de fallo de ordenador le cuesta a la empresa un promedio de 375.000 Ptas. en personal.
- **Paso 3. El calculo de costes intangibles**.
  Por más intangibles que sean, estos costes son algo que tiene que ser tomado en consideración, porque ponen de manifiesto algunos de los efectos a largo plazo de los fallos de disponibilidad de sistemas. Mencionaremos solo algunas cosas en las que hay que pensar:
  El ánimo dentro de la empresa. Si los empleados no pueden cumplir con su trabajo, debido a fallos del sistema, su ánimo afecta su modo de trabajar y prestar servicios.

  Las pérdidas de ingresos, los costes perdidos de personal y los costes intangibles se suman, para obtener el coste por hora de la no disponibilidad del sistema.

  Aunque los efectos de los tiempos muertos de sistemas no se pueden medir con facilidad, es muy necesario realizar estos cálculos de costes de los fallos de disponibilidad. Recuerde también, que el alcance de los efectos de un fallo, no depende solamente de su duración. Su cálculo supone también la evaluación de si durante todo el tiempo del fallo del sistema, los datos realmente necesitaban ser disponibles. Muchos tiempos muertos planificados, aprovechan el hecho que la duración de la falta de disponibilidad, muchas veces, no es tan importante como el cuándo el sistema no está disponible.

Sectores que sufren más interrupciones (fuente IBM)

Sector	Porcentaje
Banca y Finanzas	26%
Gobierno, Administraciones Públicas e Instituciones	19,1%
Educación	11,3%)
Industria	10,9%
Servicios	9,5%
Comunicaciones	8,2%

Motivos que causan caídas de sistemas:  <!--[if !vml]--> <!--[endif]-->

¿Qué debemos de tener en cuenta de una solución de alta disponibilidad?

1. La solución de clustering.
<!--[if !supportLineBreakNewLine]-->
<!--[endif]-->

Cada HABP (High Availability Business Partners) dispone de un conjunto de productos propio que constituye su solución de alta disponibilidad.

Cada solución propuesta debe ofrecer las siguientes funcionalidades:

- **¿Incorporan los productos las últimas tecnologías?**
  Cada ciclo de un producto debe incorporar mejoras diseñadas para que el entorno de alta disponibilidad y de clustering sea más robusto y eficiente. A medida que la tecnología avanza, es crucial que las soluciones de los HABP adopten y soporten estas tecnologías emergentes convenientemente. Tales tecnologías incluyen: Journaling Remoto, soporte e integración de MQ Series y el Sistema de Ficheros integrado (IFS).
- **Robustez**. Un entorno con clusters puede fallar de diversas formas. Un ejemplo puede ser la desincronización de objetos entre los sistemas primarios y secundarios. ¿Que herramientas proporciona el HABP para evitar o detectar problemas que puedan impedir la utilización de un nodo de respaldo en caso de caída no planificada?

- **Disciplina de proyecto**. ¿Es capaz el HABP de demostrar un nivel sofisticado de gestión de proyecto? ¿Comprende el HABP la solución total, incluyendo el entorno de la aplicación? ¿Se están ofreciendo servicios de análisis del entorno de sistema, incluyendo la aplicación? Incluso cuando los servicios de consultoría los proporciona IBM Integrated Technology Services, la disciplina de proyecto debe ser una parte de la discusión del diseño y una fase más dentro del proceso de consecución de los objetivos finales.
- **Replicación rápida**. Los cambios realizados en la máquina de producción tienen que reflejarse en la máquina de respaldo de manera oportuna. La solución debe ser capaz de manejar la carga de trabajo calculada que se va a generar, abarcando diferentes entornos de proceso tales como el interactivo de día y los procesos por lotes nocturnos. También debería haber la posibilidad de asignar prioridades a las cargas de trabajo de replicación en el sistema.
- **Secuenciamiento transaccional**. Los cambios realizados en la máquina de producción tienen que reflejarse en la máquina de respaldo en la misma secuencia en que fueron generadas. La solución debe garantizar que esto ocurra así incorporando controles de integridad internos y, en caso de producirse cualquier problema, avisar a los operadores inmediatamente (por ejemplo, cola de mensajes, buscapersonas, etc.).
- **Cambio de rol**. Debe ser posible invertir el sentido de la replicación utilizando herramientas que formen parte de la solución.
- **Replicación completa del entorno**. La solución tiene que ser capaz de replicar cualquier cambio realizado a cualquier objeto en el entorno de producción al entorno de respaldo.
- **Herramientas de generación de informes y de rastreo**. La solución debería ser capaz de rastrear y documentar el estado de los servidores de producción y de respaldo. Debería ser capaz de reportar cuantos cambios se han generado en la máquina de producción, cuantos se han recibido en la máquina de respaldo y cuantos se han aplicado en la máquina de respaldo. Debería haber también un registro histórico de esta información.
- **Manejo de errores**. La solución debería ser capaz de garantizar la entrega desde la máquina de producción a la de respaldo. Si se están enviando datos de una máquina a otra y el enlace de comunicaciones falla, la solución debe ser capaz de reenviar los datos que no han sido recibidos correctamente en la máquina de respaldo.

2. ¿Qué referencias existen?

Deberían existir referencias correspondientes a entornos con requisitos similares. Si además se están usando aplicaciones especificas procedentes de otros proveedores de software, siempre que sea posible, las referencias deberían corresponder a las mismas aplicaciones.

3. ¿Qué soporte se va a dar durante la implementación? ¿Qué soporte se va a dar para implementar la solución?

Implementar una solución de un HABP no consiste solamente en instalar y configurar software. Hay muchas más fases a realizar que, dependiendo de los niveles de conocimiento y experiencia del personal de su empresa, requieren diferentes niveles de soporte.

4. ¿Qué formación del producto se va a dar?

Para la solución propuesta debería darse una formación exhaustiva. Ésta debería cubrir la implementación del entorno, el cambio de la configuración del entorno (conmutación), procedimientos para la determinación de problemas y los procesos de recuperación requeridos en el caso de que se haga una conmutación manual.

Lo ideal sería que esta formación estuviera adaptada al entorno operativo y de negocio de su empresa.

5. ¿Cuál es la estructura de soporte después de la puesta en marcha?

Una vez la solución se ha puesto en marcha, se ha de proporcionar un soporte continuo. En el caso de que se tenga una pregunta urgente o se encuentre un problema, no es deseable tener que esperar hasta el comienzo de la siguiente jornada laboral para poder preguntar a alguien o para que el problema sea resuelto.

6. ¿Son los productos fáciles de usar?

¿Es intuitivo?
¿Es sencillo moverse por sus pantallas?
¿Es posible incluir funciones en trabajos por lotes o sólo se dispone de la interfase de línea de comandos?
¿Presenta una interfase parecida a la que está acostumbrado el personal de su empresa?

7. ¿Cuál es el coste total?

Obviamente, un factor en el proceso de selección es el coste de la solución. Sin embargo, el coste inicial aislado no debería ser el factor decisivo principal. Deben considerarse también los costes de mantenimiento del producto, los costes de actualizaciones a futuras versiones y los costes de soporte.