La Seguridad Informática. Planes de Contingencia

JOSE A. SOLER DE ARESPACOCHAGA

Confederación Española de Cajas de Ahorros

En la actualidad el funcionamiento de una empresa, así como la consecución de sus objetivos depende en gran parte del correcto funcionamiento de sus equipos informáticos. Cualquier componente del entramado informático, que por cualquier motivo se viera afectado en su desarrollo normal, tendrá una influencia negativa en el conjunto de la empresa.

El Plan de Contingencia Informática aporta la infraestructura necesaria para la puesta en marcha de la recuperación del sistema, en caso de producirse un desastre.

Hoy podemos asegurar que la Seguridad Informática es una necesidad impuesta a toda Entidad o Empresa de cualquier rango. La evolución de las tecnologías, de los servicios y de los entornos empresariales en general, han hecho de la «Información» quizás el primer patrimonio de las Empresas.

Esta misma evolución fuerza a la adaptación de normas y de procedimientos de seguridad, que protejan al patrimonio aludido. En tiempos atrás la protección física de las instalaciones contra las agresiones internas, externas, naturales, etc... era suficiente para salvaguardar de una forma eficaz los diferentes patrimonios de la época.

Pronto, una serie de acontecimientos determinantes, como por ejemplo la guerra del Vietnam o los fraudes en los incipientes sistemas informáticos, alertaron a las ejecutivas empresariales, para desarrollar nuevas medidas que cubrieran estas parcelas.

La situación se fue agravando al diversificarse de forma notable y continua los usuarios y las instalaciones de los Centros de Procesos de Datos. La proliferación de los terminales en lugares remotos con toda la diversidad conocida de servicios y sobre todo con una ingente cantidad de usuarios provocó la alarma respecto a la adopción de una seguridad diferente, no necesaria hasta ese momento.

No se concibe en nuestra sociedad empresarial una seguridad integral que no esté formada por una Seguridad física y una Seguridad lógica. Mucho se ha escrito sobre la Seguridad física, de su transformación y de sus constantes mejoras; pero

si hacemos una reflexión veremos que las mejoras, espectaculares incluso, pasan por la utilización de sistemas de control informatizados. La informática ha propiciado este avance notable, pero a su vez incrementa las medidas de protección a tomar para su propia Seguridad.

Centrándo el análisis en la Seguridad Lógica o Seguridad Informática, es oportuno dar una visión general de los aspectos que debe cubrir y de su entroncamiento dentro de la Seguridad Integral de las Empresas.

El riesgo que implica la informatización a la empresa no se diferencia fundamentalmente de los introducidos por los otros medios de producción, pero algunas de sus características imponen que se les preste una atención particular.

— La concentración de información vital en un sistema único agrava la vulnerabilidad. El hecho de que ese sistema tenga una organización descentralizada no modifica esta constante desde el momento que existen relaciones lógicas y lazos físicos entre las diferentes informaciones y tratamientos.

— La característica inmaterial de las informaciones tratadas facilita las operaciones de copia, manipulaciones diversas o robo, y hace extremadamente difícil su descubrimiento y la constitución de pruebas contra sus autores.

— La persecución judicial de los autores de violación de sistemas, de robo de información, de sabotaje de ficheros o programas es muy delicada, por la inadaptación de las leyes existentes a este nuevo fenómeno.

— El control del riesgo informático hace necesaria la puesta en marcha de métodos y sistemas de prevención nuevos, la mayor parte de los cuales están aún sin desarrollar: procedimientos fiables de autenticidad de documentos, medios de identificación de los individuos, soportes informáticos seguros.

— El riesgo generado por la informática puede alcanzar igualmente a la colectividad en su conjunto, en caso de acciones de sabotaje o terrorismo sobre centros de tratamiento esenciales o sobre las redes de pago electrónicas.

Toda empresa debe hoy, pues, considerar la seguridad de los Sistemas de Información como parte integrante de su política general y tenerla en cuenta en la elaboración de los planes informáticos.

La seguridad es a menudo percibida como una idea abstracta, centrada esencialmente en los aspectos tecnológicos, cuando debería ser en realidad un conjunto de políticas acerca del personal, procedimientos, métodos, materiales utilizados para proteger los bienes de una organización. Es igualmente un estado de espíritu para todos los empleados de la empresa. Este mensaje debe ser difundido en el seno de esta última, utilizando los medios de comunicación y de formación más modernos y presentando la seguridad no como un fin en si, que no lo es claramente, sino como un paso obligado hacia la realización de ciertos objetivos, propios de cada empresa, tales como: la salvaguardia del empleo, el mantenimiento del avance tecnológico, conservación de su cuota del mercado, crecimiento de la productividad, mejora de la calidad de los productos y servicios prestados, etc.

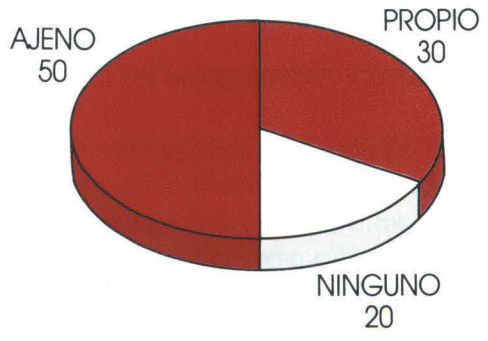

Fig. 1 Entidades que disponen de ordenadores alternativos

La puesta en marcha de un plan de seguridad informático coherente implica igualmente que se designe un responsable de la seguridad de los

Sistemas de Información, cuya función es la de aconsejar a la Dirección de Informática en la elección de sus inversiones, de diseñar y controlar el plan de seguridad, de elaborar el reglamento o las consignas de seguridad, de asegurar la puesta en marcha de los mecanismos de protección y de seguir su mantenimiento y su eficacia, de designar y formar a sus delegados en las correspondientes unidades operativas, de asignar la sensibilización y la formación del conjunto del personal y de dar cuenta del estado de la seguridad a la Dirección General.

Está claro que la responsabilidad final sobre la magnitud de las inversiones y sobre la política de seguridad debe ser de la Dirección General, único árbitro entre los inevitables conflictos entre usuarios, diseñadores y responsables financieros.

Estructura Primaria de la Seguridad Lógica

Una vez sentadas las particularidades y expuestos una serie de comentarios, se puede proponer como Estructura Primaria de una Seguridad Lógica:

— Seguridad Física de las instalaciones informáticas.
— Seguridad en el almacenamiento de la Información.
— Seguridad en los procedimientos de acceso a la Información.
— Seguridad de la información al salir de los ordenadores.

1. Seguridad física de las instalaciones informáticas

El análisis de la protección física, sería redundar sobre los conocidos procedimientos de Seguridad Física de cualquier tipo de instalación. El C.P.D. es una instalación como otra de la empresa, la cual habrá que sensorizarla contra la agresión del fuego, dotarla de extinción del mismo, controlar el acceso al recinto, etc... como otra instalación del entorno de cualquier empresa.

Por consiguiente, el análisis debe dirigirse a las protecciones inherentes a la Informática, incidiendo en los elementos autenticamente diferenciadores de otros entornos.

2. Seguridad en el almacenamiento de la información

El principal y básico componente para lograr una seguridad en el almacenamiento de la información son las copias de salvaguarda (Backups), estas deberán ser periódicas atendiendo al ciclo que tengan de actualización. Asimismo, estarán depositadas en cámaras ignífugas y con todo tipo de protecciones físicas; se harán por duplicado depositándose en lugar diferente (otro edificio) unas de otras. Si el ciclo de actualización fuera de más de un mes, se comprobará si la información copiada sigue en perfecto estado de recuperación.

Se catalogarán las identificaciones externas de los soportes controlando su coincidencia con los procesos que los generan. En caso de bandotecas o instalaciones de soportes de copia que estén robotizadas, se controlarán los accesos a los mismos con procedimientos de paswords, identificándose de esta forma a la persona que utiliza la información.

Se procederá a clasificar los diferentes tipos de información en una división lógica; como ejemplo se puede citar:

— Información pública.
— Información confidencial.
— Información secreta.

Dependiendo del grupo donde esté clasificada la información, se estructurarán los niveles de usuarios de la misma.

3. Seguridad en los accesos a la información

Los accesos controlados a la información residente en los Centros de Proceso de Datos, es sin lugar a dudas uno de los puntos vitales a proteger. Lógicamente, en tiempo de proceso es el momento idoneo para la utilización de las denominadas técnicas activas o lo que es igual técnicas de alteración de datos encaminadas a usos de tipo fraudulento o de puro sabotaje. Por consiguiente, se contempla un apartado sobre:

3.1. La intrusión y la usurpación de identidad

La intrusión

La intrusión electrónica se puede hacer sobre un sistema en tiempo real, donde los utilizadores tienen terminales y donde su identidad es verificada automáticamente por el sistema. Cuando un terminal se pone en funcionamiento, el ordenador autoriza el acceso, habitualmente después de la recepción de una señal enviada mediante el giro de una llave, introduciendo una contraseña o mediante un procedimiento similar, previamente definido. Si se conecta un terminal a la línea después de la identificación del mismo terminal, podría accederse a información sin que el ordenador sea capaz de reconocer ambos terminales. La intrusión puede igualmente producirse cuando un usuario se desconecta de una manera incorrecta, dejando el terminal en estado de funcionamiento o dejando al ordenador en un estado tal que funciona como si el utilizado estuviese todavía conectado.

La usurpación de identidad

El acceso electrónico al ordenador necesita la identificación indiscutible de un usuario autorizado. La verificación de la identidad está basada en la combinación de un cierto número de informaciones conocidas por el usuario, como una palabra clave o cualquier característica fisiológica del mismo como la huella digital, una característica de la vista, la geometría de la mano o la voz u otro elemento que el usuario posee, como una tarjeta magnética o una llave de acceso. Cualquiera que posea la combinación correcta de las características de identificación podría usurpar la identidad de otro individuo.

Las palabras clave (PASWORDS)

Un sistema informático, dotado de un mecanismo de palabras clave razonablemente seguro, debe poseer las características siguientes:

1. Deben ser suficientemente largas, para resistir una investigación exhaustiva de todas las combinaciones.
2. Deben estar compuestas por caracteres elegidos al azar.
3. No deben ser visibles para otras personas cuando se teclea en el terminal.
4. No deberían aparecer en claro en el ordenador o durante la transmisión. En caso de existir un fichero de palabras clave, estas deben estar cifradas.
5. Descubrir las palabras clave mediante ensayos debe ser difícil. No deberán permitirse más de tres reintentos de introducción del número secreto. Para acceder al sistema, deberían estar definidos un tiempo máximo y mínimo.
6. El ordenador debe registrar y memorizar las informaciones que en cada tentativa de acceso se acompañen, con fines de auditoría. Debe inmediatamente dispararse una alarma e imprimirse un informe de excepción cuando se produzca una actividad no habitual, que podría indicar una tentativa de abuso del sistema informático.
7. Los sistemas informáticos de alto riesgo, para los cuales sea necesaria una gran seguridad, deberían estar equipados con una alarma que se dispare en caso de violencia. Si un usuario es obligado por la fuerza a acceder al sistema, debería ser capaz de introducir discretamente un código en el terminal que alertase al operador del ordenador.
8. Debe existir un plan de acción de salvaguardia cuando las palabras clave sean violadas.

9. La gestión de las palabras clave debe ser confiada únicamente a empleados de confianza, utilizando medidas de protección y reglas muy estrictas.

10. Las palabras clave deben ser cambiadas periódicamente sobre todo si hay alguna posibilidad de que el sistema pueda ser violado.

11. Los usuarios de palabras clave deben ser periódicamente alertados, sensibilizándose en los problemas de seguridad, y deben estar advertidos sobre las penalizaciones si no respetan las reglas. La dirección debe afirmar su intención de imponer sanciones en caso de no respetarse las reglas, siendo los primeros en cumplir las normas de seguridad.

12. El procedimiento de entrada de las palabras clave y la respuesta del ordenador no debe ser tedioso y frustante, que haga que los usuarios intenten descubrir procedimientos alternativos.

La concepción de los procedimientos de conexión y de gestión de las palabras clave, es compleja: debe ser realizada con una gran minuciosidad y debe tener en cuenta el comportamiento humano y en particular los problemas de interacción hombre-máquina.

4. Seguridad de la información al salir de los ordenadores

La Seguridad de la información al viajar por las líneas telefónicas, sea en redes públicas o en redes privadas, pasa indefectiblemente por la utilización de **encriptadores** o por técnicas de comprobación de inviolabilidad. En primer lugar, se aporta lo suficiente para su comprensión:

a) Criptoanálisis.

Es la ciencia que se encarga del descifrado y análisis de los mensajes. Hasta hace bien poco eran solo personas expertas, profesionales, los que intentaban descifrar los mensajes secretos. El método que utilizaban era basándose en las pruebas y sobre todo empleando mucho tiempo.

Hoy día esos métodos han sido suplantados por la velocidad analítica de los ordenadores. Métodos de análisis matemáticos unidos a analizadores de semántica han obligado a la creación de nuevos sistemas de cifrado, inviolables por los ordenadores. Con esto se lucha primordialmente contra el tiempo ya que se trata de crear mensajes con tanta dificultad que el ordenador tarde en buscar el significado del mensaje.

Como ejemplo se puede tomar el caso del Algoritmo Des, del cual se dice que un millón de procesadores, encontrando un millón de claves por segundo, podría tardar 24 horas en descifrar un mensaje siendo el coste del sistema superior a 50 millones.

En el año 1977 fue aprobado el sistema DES (Data Encryption Standard) como un estandar federal. USA.

Este algoritmo utiliza 64 bits, de los cuales 8 son de paridad. Con respecto a una regla de trasposición se trasponen trozos de texto de 64 bits que se separan en dos partes de 32. La parte en cuestión se modifica mediante la utilización de una palabra de 48 bits, más tarde la parte que se encuentra a la derecha pasa a la izquierda y esta se suma a la de la derecha ya cifrada, quedando en la derecha.

Con este tipo de cifrado se produce un gran desorden, siendo la única forma de deshacerlo mediante la búsqueda exhaustiva de la clave, cuyos valores son 2 elevado a 64.

Este proceso es lento y caro y sólo podrá ser realizado por ordenadores con microchips. Del mismo modo las transmisiones deben criptografiarse a través de equipos cuyo hardware esté destinado a ésto. De esta forma es posible transmitir hasta 1,6 megabytes por segundo.

Aunque se ha demostrado como un algoritmo con un alto nivel de seguridad se está tendiendo a incrementar esa complejidad mediante el uso de vectores de control previos, que permiten comprobar si la clave que se usa es la correcta para el funcionamiento. Esto le va a permitir transformar un algoritmo que es clave única en clave múltiple.

b) Sistemas de claves.

Se utilizan dos sistemas: el simétrico y el asimétrico.

Simétrico

Se denomina simétrico porque la clave con la que se criptografía en un punto también se utiliza para traducirlo en el otro. El inconveniente que presenta este método es la dificultad de la transmisión de la clave mediante métodos seguros. Esta técnica se va perdiendo poco a poco.

Asimétrico

También denominado «clave pública» el método consiste en utilizar dos claves para más tarde traducir otras dos:

El operador A envía un mensaje al operador B. Para criptografiar utiliza su clave secreta más la clave del receptor B, que se encuentra en un directorio (público). El operador B, traduce el mensaje utilizando su clave secreta. Tanto las claves públicas como las secretas están relacionadas pudiendose canjear a voluntad, cambiando siempre el directorio.

La gestión de cualquier tipo de clave es muy complejo, por ello existe un amplio desarrollo de facilidades para la gestión como puedan ser:

- La instalación.
- El almacenamiento.
- La generación.
- La distribución (importación/exportación).

c) Criptografiadores.

Con respecto a los criptografiadores se distinguen dos sistemas:

- **Criptografiadores Software.**

La función de estos programas es la de leer y escribir información criptografiada. Normalmente utilizan al algoritmo Des y por tanto su mayor inconveniente es la lentitud.

- **Criptografiadores Hardware.**

Se usan para datos que se envían por líneas de teleproceso. Estos procesos son baratos y rápidos comparandolos con el nivel de seguridad que aportan. Utilizan como algoritmo el Des en sus chips y aparecen como clave pública. Por su gran resultado su uso se está haciendo más extenso.

d) Técnicas de comprobación de inviolabilidad.

Son técnicas empleadas para comprobar en destino que los mensajes no han sido alterados, de estas técnicas, la más conocida y de probada eficacia es la denominada MAC. Consiste en añadir un campo al mensaje que contendrá el número resultante de un cálculo definido entre el emisor y el receptor del mensaje. Como ejemplo se puede tomar el caso de sumar los campos de importe, D.N.I., y el día de la operación, el resultado se puede multiplicar por otra cifra y dividirla por el número del mes, el resultado se añadiría como campo al final del mensaje, siendo interpretado con la misma rutina en el ordenador de destino.

Se puede apreciar que las posibilidades de complicar el MAC son importantes y lógicamente iría en beneficio de la seguridad de la inviolabilidad del mensaje.

En la aplicación de la Seguridad Lógica es muy importante el reconocimiento de su necesidad y la imposibilidad del divorcio entre seguridad física y seguridad lógica y la cristalización de todos los métodos en un Plan de Contingencia, que por su importancia, se puede asegurar que es la parte principal de la Seguridad Informática.

Plan de Contingencia

Hoy día se puede afirmar que el funcionamiento de una empresa, así como la consecución de sus objetivos, depende en gran parte del correcto funcionamiento de sus equipos informáticos.

Cualquier componente del entramado informático, que por algún motivo se viera afectado en su desarrollo normal, tendría una influencia negativa en el conjunto de la empresa.

Esta influencia vendría dada en algún tipo de interrupción de mayor o menor grado, pero en cualquier caso afectaría a la empresa en sí.

Para paliar estas consecuencias negativas, se crea el **Plan de Contingencia,** que se define como:

«El conjunto de procedimientos de tipo preventivo, cuya misión es aportar la infraestructura necesaria para la puesta en marcha de una recuperación del sistema, en caso de producirse un desastre.»

Las etapas que deben contemplarse en un Plan de Contingencia son:

— Gestión de Riesgos.
  - Análisis de Riesgos.
  - Medidas a Aplicar.
  - Financiación de los Riesgos.
— Sistemas de Protección Física.
— Sistemas de Protección Lógica.
— Sistemas de Recuperación.

1. Gestión de Riesgos

La gestión de Riesgos es la capacidad para llevar a cabo operaciones con un nivel aceptable de riesgos o de pérdidas. Ello implica una definición de medidas (coste/efectividad) que salvaguarden los bienes contra daños o pérdidas, alteración, trabas en su uso, etc... y que tiene como base éste análisis, del cual se derivarán las adecuadas medidas de Protección.

Análisis de Riesgos

Es la etapa del plan en la que se deberá:

— Identificar los componentes críticos a analizar.
— Identificar los aspectos críticos de estos componentes bajo el prisma directivo.
— Identificar las amenazas posibles.
— Estimar la frecuencia del suceso.
— Calcular el coste de la exposición.
— Evaluar la criticidad según la exposición.
— Ordenar los componentes críticos.

Medidas a Aplicar

Con estos datos en la mano se aborda la siguiente etapa, en la que se determinarán las Medidas a Aplicar. Estas deberán establecerse de acuerdo con:

— Diseño de objetivos de protección.
— Una selección de los modos de protección.
— Justificación económica.

En la justificación económica, se deberá tener en cuenta la cobertura, en algunos casos, con un seguro de riesgo. Esta medida en muchas aplicaciones de los sistemas sería salvaguarda suficiente para quedar cubiertos del riesgo puntual de dichos conjuntos de programas. Con ello se evitaría repercutir los cortes de contingencia y los de posterior recuperación para la empresa.

Financiación de los riesgos

Después de haber efectuado los análisis anteriores se presentarán a la dirección, quien deberá tomar las decisiones más adecuadas para la financiación de los riesgos.

2. Sistemas de protección física

Las medidas de Seguridad Física de un C.P.D., en forma resumida, tienen como base la utilización de los siguientes componentes:

— Sistemas de control de acceso físico.
— Sistemas de detección de incendio e inundación.
— Sistemas de extinción.

En el Plan de Contingencia cuentan como elementos a analizar su estado para una posible

entrada del plan de recuperación, los elementos físicos:

— Cámaras/Cajas fuertes de Seguridad.
— El Plan de Emergencia.
— El mismo Plan de Recuperación.

● Las cámaras/cajas fuertes de Seguridad, deberán estar en perfecto estado de funcionamiento, asegurada su confidencialidad de acceso y la manipulación de los elementos que contenga.

En éste elemento hacer solamente un comentario sobre cámaras ignífugas, donde se concentra la información en soportes magnéticos. Deberán ser revisadas y tener la certeza de su resistencia a las temperaturas así como los sistemas internos de detección y extinción. Deberán estar duplicadas para albergar la copia de seguridad de los sistemas, que en un momento de recuperación nos facilitaría poder tener la información necesaria para un arranque en el menor tiempo posible.

● El Plan de Emergencia es una parte importante y necesaria del entramado de Seguridad de una Empresa. Es uno de los apartados del Manual de Autoprotección y que la normativa obliga a tener implementado con sus partes de evacuación, normativa de edificación, salidas, entradas, etc...

● El mismo Plan de Recuperación será un elemento físico a analizar, con el fin de destacar sus cambios al ser una parte viva. No olvidemos que cada cambio en el Sistema Informático, cada implementación de una aplicación nueva, etc... se verá reflejada en el Plan de Recuperación. Por tanto será una de las partes donde se tendrá una mayor atención de actualización y análisis de sus situaciones.

Una recuperación efectuada sobre una parte obsoleta, dará como resultado una mayor interrupción en el caso de llegar a recuperar la novedad implementada o una pérdida de una parte de la información.

3. Sistemas de Protección lógica

Los diferentes componentes lógicos que se deben analizar son:

— Normas de Confidencialidad.
— Software de control de accesos.
— Copias de salvaguardia (operación).
— Copias de salvaguardia (recuperación).

a) Normas de Confidencialidad.

Dentro de las normas de Confidencialidad se distinguen dos apartados. Primero, la clasificación de la información y segundo, el manejo de la misma.

El principal problema que surge a la hora de proteger o definir la protección de la información, es el saber qué grado de confidencialidad tiene.

La Información corporativa, será aquella que, revelada sin autorización, puede ser perjudicial para los intereses de la entidad.

Será, por consiguiente, responsabilidad de todos los empleados, aplicar y hacer aplicar las «Normas de Clasificación de la Información» que dicte la Dirección al respecto.

Se pueden distinguir en una clasificación estandar:

— Información confidencial.
— Información confidencial y personal.
— Información legal y confidencial.

1. Marcado

Deberá llevar estampado un sello con la categoría apropiada. No es válido un literal escrito a mano, máquina o impreso.

El estampado debe hacerse en la parte superior e inferior del documento.

2. Reproduccción

El acceso a los departamentos de reprografía debe estar restringido.

El personal de éstos departamentos cuidará que los documentos clasificados como confidenciales no estén expuestos a la vista de cualquiera.

De forma ocasional o habitual, puede ser necesario entregar los documentos a servicios o empresas externas para su reproducción. Estas empresas deben de garantizar la confidencialidad de la documentación entregada mediante:

— Medidas de seguridad operativa.
— Protocolo ante Notario donde consten las medidas a aplicar y la responsabilidad en la que se incurriría en el caso de no guardarlas.

Además debe controlarse:

— Devolución del material sobrante.
— Borradores. Páginas estropeadas.
— Planchas. Hojas de papel carbón. Negativos.

3. Envíos

Los envíos de información confidencial se harán en dos sobres opacos.

El primero irá destinado a la persona o servicio receptor, sin advertir de la confidencialidad del contenido.

El segundo irá en sobre de tipo especial (confidencial) con la clasificación correspondiente.

4. Archivo

El archivado de la información confidencial puede hacerse en:

— Archivo propio (Armarios ignífugos, Cajas fuertes, Cámaras de seguridad).
— Archivo ajeno (Servicios de custodia, Cámaras alquiladas).

5. Destrucción

La destrucción de la información confidencial puede ser efectuada por los servicios propios o ajenos. En cualquier caso, por personal enterado de sus responsabilidades y normas de actuación y, además, en el caso de servicios ajenos, con las garantías mencionadas para la Reproducción.

Puede hacerse ésta destrucción:

— Por triturado y reducción a pulpa.
— Por cremación.
— Por borrado (soportes magnéticos).

b) Software de control de accesos.

El Software de control de accesos al que se refiere es el que controla la seguridad contra intrusión en las Bases de Datos, Aplicaciones informáticas, Teleprocesos, etc...

Se pueden enumerar como elementos a considerar:

— Normas y elementos de protección.
— Propietario.
— Depositario.
— Usuario.
— El dato.
— El registro.
— El fichero.
— El job.
— La aplicación.
— El terminal.
— Acceso interactivo.
— Acceso batch.

El control mantenido sobre estos elementos con el auxilio de herramientas apropiadas, análisis y seguimiento de los informes log y una dinamicidad en los circuitos de control, nos dará la certeza de tener acotado en gran medida la seguridad lógica de nuestra instalación Informática.

Los problemas principales suelen aparecer por la falta de responsables de estos seguimientos; el propio seguimiento no se hace en la profundidad y periodicidad correctas; la falta de normas una vez instalado el software de control; falta de sanciones en momentos de negligencia; etc...

c) Copias de salvaguardia (Backups de Operación)

Se denomina Backups de Operación, a las copias de seguridad que con periodicidad constante según se altere la información, se deben de tener con el fin de poder iniciar una recuperación de información, ante cualquier deterioro de la que se utiliza normalmente.

Esta operación de salvaguardar la información cuando sufre cambio o actualización, debe ser uno de los componentes cotidianos de toda po-

lítica de seguridad informática. La recuperación desde copias antiguas hace penosa la puesta al día de la información añadiendo tiempos seriamente altos en las interrupciones y en la consecución de objetivos en general.

Podemos decir que los elementos a considerar son:

— Las copias de los ficheros.
— Las copias de los programas.
— El transporte de estas copias.
— El almacenaje de las copias.

d) Copias de salvaguardia (Backups de recuperación).

Denominamos Backups de Recuperación a las copias que se deben depositar en otro sitio diferente a las de Operación y que servirán para retomar la situación normal, después de producirse un desastre. Estas copias son las utilizadas en los Planes de Recuperación de Desastre y consiguientemente no se encontrarán en la misma ubicación que el C.P.D.

El principal problema que se encuentra es concerniente a su inexistencia, de igual modo a que cuando existen son antiguas y no se han actualizado con la periodicidad correcta. En algunos casos la falta de idoneidad del lugar de almacenaje originando la poca fiabilidad del soporte,...

Los elementos a considerar son los mismos que en las copias de operación debiendo incidir más sobre los aspectos de transporte y almacenaje al ser probable que se efectúe por personal externo a la Entidad y en lugares en muchos casos también fuera de jurisdicción propia.

Una vez tratado de forma general un Plan de Contingencia, procede la recomendación de que se cree un Comité de Seguridad lógica, integrado por personal de Seguridad, Informática y Auditoría. Dicho Comité tendría la clara misión de efectuar un seguimiento sistemático del cumplimiento del Plan, lo que en la mayoría de los casos ahorraría mucho dinero a la empresa y exposiciones innecesarias.

4. Sistema de recuperación

Lo más importante es no tener que usar un plan de recuperación, no obstante al ser posible su utilización, toma especial relevancia el tener resuelta la incidencia en caso de producirse la emergencia.

El plan de recuperación debe ser efectivo, entrenado y probado. De esta forma tendrá una un impacto menor en la marcha de la empresa, aunque, que duda cabe, un impacto al fin.

Los componentes de seguridad pueden funcionar mal o incluso no funcionar, se puede deber a obsolescencia, mal diseño, abandono, etc... Es por consiguiente imprescindible para tener a punto un plan de recuperación efectivo, tener controlados los diferentes componentes que intervienen en el mismo.

a) Medidas de recuperación.

Para realizar la recuperación es necesario disponer de Equipos de Recuperación, cuyos miembros tendrán procedimientos de actuación y guías de recuperación escritas en forma concisa.

Igualmente, es importante que haya procedimientos alternativos a las tareas que normalmente se realizan.

b) Centro de proceso de datos alternativo.

El C.P.D. alternativo es una instalación en la que se pueden seguir realizando las operaciones imprescindibles que necesita la Empresa para sobrevivir, en el caso que nuestro Centro primario no sea operativo.

Para poder funcionar en un C.P.D. Alternativo es necesario tener:

— Procedimientos alternativos escritos.
— Equipos de proceso alternativo.
— Guía de actuación.

Una vez asumida como estrategia de respaldo la existencia de dos Centros de Proceso de Datos (el propio o primario y el alternativo), se distinguen estas dos alternativas:

1. Centro propio

El elevadísimo coste que lleva asociado la construcción de un centro alternativo propio hace de un centro alternativo propio hace altamente compleja la decisión de adoptar esta solución de backup frente a las alternativas pooling.

Paralelamente a este grave inconveniente aparecen aspectos positivos y ventajas proporcionadas por un centro propio:

— Posibilidad de plantear una informática distribuida.
— Mayor fiabilidad.
— Generalmente mayor cobertura de servicios.
— Menor «Timer Frame».
— Mayor facilidad de mantenimiento del plan de contingencia.
— Mayor flexibilidad en la realización de pruebas.
— Mayor flexibilidad ante el crecimiento o modificación de la estrategia informática.
— Al contrario que en las estrategias pooling, los casos de contingencia simultánea con otras entidades suponen, antes que un grave inconveniente, una potencial ventaja de negocio.

Fig. 2 Entidades que disponen de «Software» de Seguridad

La decisión en un sentido u otro deberá salir de la ponderación de los aspectos positivos frente a los costes.

En algunas ocasiones, la toma de postura se facilita debido a la especial situación en que se encuentra la organización implicada. Así:

— Muchas organizaciones consideran sus recursos de proceso de datos inadecuados para dar respuesta al crecimiento de la institución. Una solución a este problema consiste en la construcción de un segundo CPD, de tal manera que paralelamente al objetivo citado se consigue respaldo recíproco entre ambos centros.
— Las fusiones entre entidades que cuentan con centros de procesos de datos facilita y abarata la posibilidad de contar con centros alternativos.

Los parámetros de grado de cobertura de servicio y «Time Frame» permiten establecer los siguientes tipos de centros de respaldo:

- Centro caliente (Hot backup).
  Este tipo de respaldo consiste en la coexistencia del CPD actual y de un segundo centro de proceso ya operacional y listo para, mediante una conmutación automática, hacer prácticamente instantánea la continuidad operativa.

- Centro templado (Warm backup).
  Se basa en la utilización de un segundo centro, posiblemente operacional, listo para asumir con sus recursos la continuidad del proceso operativo con un retardo que puede ir desde varias horas hasta uno o más días.

- Centro frío (Cold backup).
  En este caso, el segundo centro de proceso de datos cuento con un equipamiento escaso o no está equipado, con lo que la demora en la continuidad operativa es bastante más elevada que en los casos anteriores.

Paralelamente a la estrategia de equipamiento se plantea una estrategia de utilización de dicho equipamiento. Desde este punto de vista, se pueden enumerar las siguientes alternativas:

— Centros espejo.
En esta estrategia, las aplicaciones del CPD principal están replicadas en el centro de respaldo

de tal manera que las bases de datos están actualizadas en ambos centros, pudiéndose realizar la conmutación con un retardo mínimo.

Esta estrategia implica la existencia de un centro primario (CPD principal) y uno secundario (centro respaldo).

La consecuencia inmediata de todo ello es que el respaldo es unidireccional y no mutuo o bidireccional.

— Centros en espera (Standby).

Esta estrategia se basa en la idea de que el proceso de datos no se realiza en el centro de respaldo, estando la base de datos almacenada en disco y siendo actualizada de manera periódica. De igual manera que en la alternativa anterior el backup es unidireccional.

— Centros con producción distribuida.

Es la estrategia más común. Dos CPD, generalmente especiales, se organizan de tal manera que la carga de trabajo se reparte entre ambos. Esta estrategia de respaldo es bidireccional, pues cada centro proporciona backup al otro (por lo que ambos deben estar sobredimensionados).

2. Centro compartido (Pooling)

Esta estrategia contempla la existencia de un centro de respaldo (hot, warm o cold backup) ofrecido por una entidad de servicios y compartido por varias instituciones.

La selección del servicio debe hacerse de acuerdo a las necesidades de cobertura y teniendo en cuenta la compatibilidad de los equipos.

Esta opción presenta el riesgo de que sólo uno de los suscriptores puede hacer uso del mismo en un momento dado, por lo que de ocurrir simultáneamente en dos de las entidades la paralización de su proceso de datos se plantearía una situación altamente conflictiva si, como es normal, el centro no tiene capacidad suficiente para dar respaldo a ambas.

Para evitar esto pueden plantearse cláusulas contractuales que concedan prioridad a la entidad suscriptora del servicio en caso de que necesite los recursos a la vez que otro(s) de los contratantes del servicio compartido.

Sin embargo, los costes, al compartirse entre los distintos usuarios, son considerablemente inferiores a la opción de centro propio.

Uno de los principales problemas que existen con esta opción es que los recursos necesarios a contratar no los dan los suministradores de este servicio en el mercado. Si este punto se consigue resolver, esta opción tiene una relación calidad/precio muy buena.

La existencia de una situación de contingencia no evita la necesidad de medidas de seguridad física y lógica. El centro compartido deberá garantizar el control de acceso, así como la seguridad de equipos y datos. Ya que en la situación de contingencia se debe mantener el mismo nivel de seguridad de la información.

Otros aspectos a considerar deben ser:

— Vías rápidas de acceso al centro (aeropuertos, autopistas...).
— Facilidades de almacenamiento de soporte.
— Capacidades de líneas de comunicaciones (RTC, punto a punto, X.25, RSAN).
— Servicios de consultoría proporcionados por el suministrador del servicio.
— Personal de soporte y mantenimiento proporcionados por el suministrador del servicio.
— Salas para el personal de la propia entidad contratante.
— La superficie disponible en el CPD.
— La cobertura horaria.
— La fecha de puesta en marcha del centro.
— Situación económica y laboral de la empresa suministradora del servicio pooling.
— Periodicidad de las pruebas, duración máxima de las mismas y exigencia de plan de contingencias.
— Posibilidad de uso en situaciones de no contingencia.

Parámetros para la selección de la estrategia de centro de respaldo

Los principales factores a definir a la hora de realizar la selección de alternativas en un estudio de viabilidad de centro de respaldo son los siguientes:

- Grado de Cobertura.
  Definición de los servicios críticos. Servicios críticos son aquellos cuya discontinuidad produciría pérdidas a la entidad.

- Time Frame.
  Período de tiempo máximo admisible sin reanudación del procesamiento.
- Arquitectura de sistemas.
  Hardware, comunicaciones, software de base y aplicaciones.

- Infraestructura del centro.

Ubicación y características generales del local.

— Zona segura:

  * Escasa actividad sísmica.
  * Alejada de aeropuertos.
  * Baja probabilidad de inundaciones.

— Facilidad de acceso aéreo y/o por carretera.
— Con acceso para carga y descarga.
— Espacio suficiente (que pueda cubrir posibles expectativas de crecimiento).
— Zona de fácil suministro de líneas telefónicas.
— Dotada de puertas de emergencia y seguridad.
— Pasillos, montacargas y puertas de dimensiones suficientes para movimiento de equipos y material.
— Utilización de materiales de seguridad en la construcción.
— Falsos suelos y techo si procede:

  * Altura libre mayor o igual que 250 cm.
  * Suelo capaz de soportar 1.000 kg/m^2.

Distribución del centro.

El centro deberá constar con las siguientes salas u oficinas:

— Sala de ordenadores:

  * Superficie según requerimientos hardware.
  * Sistema de climatización.
  * Protección contra incendios.
  * Control de acceso.
  * Falso suelo y techo.

— Zona del personal:

  * Superficie según personal de CPD desplazado.
  * Oficinas para el responsable, técnicos de sistemas, operadores y personal administrativo.
  * Sala de reuniones.
  * Aseos y servicios.

— Cintoteca.
— Almacén.
— Volumen técnico (UPS s, TRF s...)
— Centralita.
— Sistema de control de acceso y vigilancia.

Equipamiento básico.

— Termohidrógrafos.
— Grupos convertidores.
— Detector de fluidos.
— Sistema contra incendios.
— Sistema de aire acondicionado.
— Sistema de control de acceso a la sala de ordenadores.
— Instalación eléctrica:

  * Centro de transformadores.
  * Alumbrado de emergencia.
  * Líneas de 50 c/s.
  * Bases de enchufes.
  * Cuadros de distribución del A/A, ordenadores, alumbrado y fuerza.
  * Sección de la acometida sobredimensionada en un 75%.
  * Línea de tierra independiente.

* UPS s.
* Tubo traqueal en falso suelo.
* Alumbrado con nivel de 440 lux, aproximadamente.

— Material auxiliar:

* Bastidores para módems.
* Soportes magnéticos.
* Mobiliario: mesas, sillas, estanterías.
* Papel y cintas para impresoras.
* Guillotinas y máquinas de encuadernación.

● Fecha de puesta en marcha efectiva del centro.

● Coste de la inversión.

— Inmovilizado.
— Equipamiento.:

* Sistemas informáticos.
* Sistemas de seguridad y volumen técnico.
* Mobiliario, etc.

— Gastos generales.
— Gastos de explotación y mantenimiento.
— Gastos de comunicaciones.
— Coste de realización del plan de contingencia, si no se ha desarrollado. ■