gerencia de riesgos

PROTECCION DE INSTALACIONES DE PROCESAMIENTO ELECTRONICO DE DATOS

James D. Blinn y Carl H. Sangree
Consultores de Risk Planning Group, Inc.

1.- INTRODUCCION

El experto en informática Donn Parker, analizando el futuro de la informática, escribió en 1976: "Nadie va a desconectar esas máquinas". [1] La población de ordenadores instalados en el mundo se estima entre 1 millón y 2 millones de unidades, dependiendo de quién es el que está contando y qué es lo que se considera un ordenador. Con el advenimiento de la tecnología de micro chips y la reducción que esta tecnología produjo en los costos de memoria, el ordenador ha salido del santuario de los centros especializados de procesamiento de datos para unirse a los trabajadores en las fábricas y a los empleados en sus escritorios. Los ordenadores ya no son las herramientas especializadas de sólo las más grandes organizaciones, un ejército de computadoras especializadas en compañías pequeñas a través del mundo, testifican la validez de la profecía de Parker.

El riesgo asociado con el uso de ordenadores en la empresa se ha multiplicado por dos razones. En primer lugar, con la proliferación ha venido una familiarización muy grande y un mayor acceso a los equipos electrónicos de procesamiento de datos. Las operaciones de ordenadores ya no están protegidas o cubiertas por un velo de misterio. Hoy en día, aun el ciudadano promedio sabe algo sobre el valor y la operación de sistemas de procesamiento de datos. Gra-

cias al microprocesador, el acceso a sistemas de informática ha sido descentralizado dentro de corporaciones y a través de la sociedad. Hay una ola de informática que está envolviendo a todos los hogares. Antes de que el siglo termine es muy posible que existan equipos de informática en la mayoría de los hogares. Equipos que, según Business Week, "podrían ser una herramienta tan poderosa para el asalto a un banco o para la ejecución de un fraude, como es importante un revólver para llevar a cabo un robo."[2]

En segundo lugar, debido al costo cada vez menor de las unidades de memoria y al aumento en el poder de los ordenadores modernos, el valor de las operaciones llevadas a cabo por estas máquinas versátiles ha aumentado sustancialmente. Estamos en camino a una sociedad sin papel. Existen hoy en día muchas operaciones computarizadas que no serían reproducibles en base a procesos apoyados en el uso de papel. Los impulsos eléctricos y magnéticos que pasan a través de transistores, burbujas, cintas y discos son muchas veces los únicos registros y los únicos conjuntos de instrucciones o incluso los únicos activos convertibles, propiedad de una empresa comercial.

Este estudio tiene como objeto ayudar al gerente de riesgos a enfrentar los 3 grandes retos del control de riesgos en las instalaciones de procesamiento de datos: proveer la seguridad de la instalación, protegerse contra el fraude por ordenador, y recuperarse lo más rápidamente posible después de un desastre. La primera parte de este estudio hará referencia a recientes pérdidas asociadas con ordenadores para ilustrar estos problemas de control de riesgo. La segunda parte es una discusión sobre equipos de control de riesgo tanto físicos como de seguridad de información y programas. La tercera parte está consituida por

unos formularios especialmente diseñados para hacer una evaluación de control de riesgos en instalaciones de procesamiento de datos y la cuarta es una bibliografía sobre fuentes que pueden ser consultadas para obtener información adicional.

1.1 PERDIDAS

Las pérdidas de equipos o pérdidas operativas en instalaciones de procesamiento de datos, generalmente inspiran una atención sensacionalista más que un disgusto del público. Los sentimientos contradictorios de fascinación y miedo sobre la complejidad y el poder de los ordenadores de hoy en día producen una ambigüedad curiosa. El fraude por informática genera robos gigantescos de dinero que si hubieran sido realizados con un arma, hace mucho tiempo que hubieran producido una fuerte campaña para la erradicación del delito. La sociedad generalmente ve al ladrón por ordenador como un simpático campeón en la lucha contra las máquinas super humanas, su crimen es percibido como una parábola de David y Goliath. De que los fraudes de ordenadores resultan en pérdidas gigantescas no cabe duda: Un profesor de administración de empresas de la Universidad de Virginia, el Dr. Brand Allen, encontró en un estudio de 150 casos que la pérdida promedio por fraude computarizado a empresas era de 621.000 dólares, de 193.000 dólares a bancos, y de 329.000 dólares a instituciones estatales o gubernamentales y de 45.000 dólares al gobierno federal de los Estados Unidos.[3]

A continuación presentamos algunos ejemplos de pérdidas recientes que ilustran el amplio rango de pe-

ligros a los que está sometida una instalación de procesamiento de datos:

La revista The Economist del 19 de abril de 1980,[4] informa que un grupo francés autodenominado CLODO el Comite Liquidant et Detournant des Ordinatewrs (Comité de Liquidación y Secuestro de Computadoras) atacó dos instalaciones de informática en Touloise. Creyendo en parte que "el ordenador es la herramienta favorita de la clase dominante, utilizada para explotar, para reunir archivos de información, para controlar y para reprimir", los atacantes de CLODO causaron daños estimados en 1 millón de dólares quemando datos y medios de almacenamiento magnético propiedad de Phillips Data Systems y de CII-Honeywell Bull. El sabotaje de CLODO fue seguido dos semanas más tarde por ataques con cohetes contra otras instalaciones de ordenadores por otro grupo francés de "asesinos de ordenadores".

El 9 de agosto de 1979, por razones que aún no están claras, un empleado de mantenimiento operó manualmente el sistema de rociadores automáticos que protege los cuatro ordenadores Univac del Departamento de Procesamiento de Datos del U.S. Census Bureau en Suitland, Maryland. La sala de informática se inundó con varias pulgadas de agua y a pesar de que el centro fue desconectado inmediatamente y se utilizó asistencia de expertos para tratar de restituir las unidades, dos de las cuatro máquinas Univac fueron totalmente destruidas. Después que la corriente normal fue eliminada, una fuente ininterrumpible de corriente entró a funcionar para proteger la gran memoria de las

gerencia de riesgos

unidades, lo cual causó un corto circuito y extenso daño al equipo.[5]

Un comité de investigación del congreso norteamericano que estaba probando un nuevo sistema de seguridad que había costado 500.000 dólares en el año 1978, en el departamento de sistemas de la Administración del Seguro Social en Baltimore, tuvo éxito en la desactivación de las alarmas contra robos y la remoción de 38 de las más importantes cintas de Informática sin ser detectado. En ese momento, el centro de informática manejaba 80.000 millones de dólares en ingresos por impuestos del Seguro Social y beneficios anuales.

Entre las pérdidas que evidencian los problemas de seguridad de programas y datos podemos destacar las siguientes:

En uno de los más grandes robos de ordenadores descubiertos y publicados hasta la fecha, el Wells Fargo Bank (el onceavo más grande en los Estados Unidos) anunció pérdidas estimadas en 21.3 millones de dólares entre los años 1979 y 1982. Un oficial de operaciones había creado créditos fraudulentos a través del sistema de compensación interbancario para cubrir retiros realizados a cuentas externas. La investigación aún continúa.

Entre el 16 y 24 de abril de 1980 un grupo de estudiantes del Dalton School de Nueva York utilizó los terminales del colegio para ingresar a través del sistema telefónico, violando los códigos de seguridad, a unos 21 sistemas de computación de em-

presas y universidades canadienses. Dos de estas compañías sufrieron daños como resultado de los ingresos no autorizados. Un ejecutivo de la empresa de Cemento La Farge informó que los intrusos al sistema "empezaron a eliminar nuestras memorias de informática una por una y eventualmente borraron un quinto del almacenamiento de nuestra computadora, aproximadamente 10 millones de bits."[6]. No hubo otro daño comunicado.

Un consultor de informática para el Banco Security Pacific de Los Angeles fue acusado y convicto de robar 10,3 millones de dólares en 1978. Después de obtener un código secreto para transferencia electrónica de fondos, este señor se hizo pasar como un ofical del banco y dió instrucciones telefónicas para que el dinero fuese transferido a una cuenta bancaria en Suiza. Cuando el banco se dió cuenta de que la transferencia de dinero no había sido autorizada, el consultor ya había viajado a Suiza, comprado unos diamantes con el dinero y regresado a los Estados Unidos. Fue atrapado cuando comentaba con orgullo su robo.[7]

2.- CONSTRUCCION DE INSTALACIONES DE PROCESAMIENTO DE DATOS

2.1 PLANIFICACION DE UNA INSTALACION DE PROCESAMIENTO DE DATOS

El gerente de riesgos debe proveer asesoramiento a su organización cuando se está planificando un centro de procesamiento de datos. Las siguientes son algunas guías cuya implantación contribuiría a reducir el riesgo de pérdida:

1. El centro de procesamiento de datos debe ser el único ocupante de un edificio sin ventanas, especialmente diseñado para procesamiento de datos.

2. El centro no debe estar ubicado en un lugar peligroso, por ejemplo: de alto nivel de delitos, propenso a las inundaciones, en zonas de aproximación de aviones, etc.

3. El centro de procesamiento de datos debe estar por encima del nivel de la calle y no debe tener una pared común con el exterior del edificio.

4. El edificio, las separaciones, los muebles y el equipo deben ser construidos de materiales no combustibles.

5. El almacenamiento de papel dentro o cerca del centro de procesamiento de datos y la biblioteca de cintas magnéticas, debe mantenerse al mínimo posible.

6. Se deben instalar equipos de detección y extinción automática de incendios en todo el edificio, incluso por encima de cualquier techo falso y por debajo de cualquier piso falso.

7. Las líneas de comunicaciones eléctricas deben ser dobles y encontrarse debajo del suelo.

8. Deben existir fuentes auxiliares de energía y aire acondiconado.

La mayoría de estas sugerencias se explican en mayor detalle en las secciones subsiguientes.

Naturalmente, podría resultar imposible implantar todas estas sugerencias. Sin embargo, el gerente de riesgos debe al menos evaluar la importancia de cada una de ellas, durante el desarrollo del proyecto.

2.2 AIRE ACONDICIONADO

El papel del equipo de aire acondicionado en el ambiente de procesamiento de datos no está limitado a la refrigeración. Un equipo de aire acondicionado específicamente diseñado para ordenadores provee también de un control de la humedad, de una distribución adecuada del aire y una limpieza del aire. En la mayoría de los casos, se utilizan sistemas dedicados para proveer esta capacidad. Esto se debe a que estos sistemas sofisticados de control de ambiente generalmente no son muy rentables para su instalación en áreas normales de oficinas o fábricas.

La necesidad de controlar el nivel de humedad y la estática en el aire, es muchas veces ignorada. Una descarga estática de una persona puede destruir circuitos de ordenadores e interrumpir operaciones. Este problema puede ocurrir tanto dentro del centro de computación, como en las áreas donde existan terminales, impresoras u otro equipo periférico. En muchas ocasiones se utilizan alfombras antiestáticas, que son básicamente alfombras con un revés de goma que puede estar conectado al suelo, en las áreas remotas donde se desea proteger equipos periféricos.

gerencia de riesgos

2.3 FUENTES DE ENERGIA

Muchas empresas han instalado fuentes secundarias de energía para los casos en que el suministro normal sufra una reducción o eliminación. Esto puede hacerse utilizando energía proveniente de un área atendida por un sector distinto de la red pública de alimentación. Además, una fuente ininterrumpible de energía(básicamente una batería) puede ser utilizada para reemplazar la electricidad, en caso de perderse toda la corriente. Estas fuentes son generalmente costosas pero podrían justificarse dependiendo de la naturaleza de las funciones del centro de procesamiento de datos y de la fiabilidad de la red de suministro público. Es importante realizar un análisis cuidadoso de las pérdidas potenciales en dinero que podrían resultar de un fallo de corriente.

Otro elemento crítico relacionado con el suministro de electricidad a un centro de cálculo , es su calidad. Aún cuando la corriente es normalmente constante, este no es siempre el caso. Muchos equipos que tienen un gran consumo de tensión, tal como los elevadores, y que se conectan y apagan contínuamente, pueden dañar la calidad del suministro de corriente. Desviaciones importantes de las tolerancias que un ordenador puede aceptar podrían causar daño irreparable a las unidades de disco y a algunos circuitos. La calidad de la línea de suministro puede verificarse con un monitor de línea el cual es fácilmente obtenible a través de suplidores de equipos de informática Si la calidad no es aceptable, puede instalarse un transformador de aislamiento y regulación que controlaría cualquier fluctuación momentánea en la fuente de energía.

2.4 DETECCION Y EXTINCION DE INCENDIOS

En la actualidad ya se ha aceptado el hecho de que los sistemas de protección para salones de procesamiento de datos basados en el hidrocarburo halogenado Halon 1301 son superiores a los sistemas tradicionales de rociadores. El Halon es un gas que no tiene color, no tiene olor, no es conductor de electricidad e interfiere químicamente el proceso de combustión. La National Fire Protection Association de los Estados Unidos ha encontrado que el Halon 1301 es un agente efectivo de extinción, excepto para aquellos incendios que involucran productos químicos que tienen su propio suministro de oxígeno, metales reactivos y metales híbridos.[8] Ninguno de estos tres tipos de incendio es probable en un centro de procesamiento de datos.

El sistema de suministro del Halon 1301 dependerá de la instalación que se desea proteger. Un sistema que se considera eficiente y confiable incluye los siguientes elementos:

° Detectores de humo ubicados en el techo, debajo del piso falso, en los servicios, y en los túneles de cables;

° Globos modulares de Halon 1301 con boquillas de descarga, unidades montadas en las paredes y debajo de los pisos falsos;

° Obturadores manuales en las salidas;

° Alarma local disparada por cualquiera de los detectores de humo;

° Sistema de disparo automático del Halon operado por 2 o más detectores;

° Extintores portátiles de Halon 1301 instalados en las paredes.

Se deben tomar en cuenta tres aspectos cuando se instalan sistemas de hidrocarburos halogenados. Primero, el Halon 1301 no es tóxico en concentraciones ambientales de menos del 10%. Concentraciones de más del 10% no son recomendables para ubicaciones normalmente ocupadas por personas. Segundo, el costo de una descarga de Halon 1301 es de aproximadamente 40% del costo inicial de instalación del sistema. Las falsas alarmas son costosas. Tercero, después de que se ha descargado y disipado el Halon 1301, existe la probabilidad de que un incendio que no se ha extinguido pueda reiniciarse. La instalación inicial de un sistema de hidrocarburo halogenado puede ser costosa pero no se justifica tratar de hacer ahorros pequeños. Es necesario proveer una cantidad de gas y un sistema de distribución suficientemente poderoso como para llevar en buenas concentraciones el Halon 1301 a todos los ámbitos del local.

2.5 CONTROL DEL ACCESO A LAS INSTALACIONES

Existen diversos tipos de sistemas independientes que pueden ser utilizados para controlar el acceso a las instalaciones de procesamiento de datos. Las posibilidades para controlar el acceso cubren desde las más sencillas tales como cerraduras, hasta los sistemas de la era del espacio que incluyen identificadores de huellas digitales. En general, la sofis-

ticación del sistema debe ser conmensurada con el valor de la información que está siendo protegida y la filosofía de la organización en lo que respecta a protección de activos. Pueden utilizarse cierres, tarjetas, llaves, tornamesas, sistemas de circuito cerrado de televisión, tarjetas magnéticas de identificación o sistemas electrónicos de reconocimiento de atributos físicos. Cada uno de estos sistemas está dirigido al mismo problema: cómo mantener a individuos no deseados fuera de los centros de cómputo.

Un punto de conflicto entre estos sistemas es su habilidad para prohibir a un individuo que entre y salga de las instalaciones. Si un sistema es controlado por una llave común o por un número de identificación sencillo, entonces esa llave debe ser cambiada cuando un empleado cesa en sus funciones. Por contraste, los sistemas que identifican a los individuos en base a una cinta magnética o a una huella digital pueden selectivamente prohibir el acceso a individuos no deseados, así como registrar todos los intentos no autorizados de acceso. Estos sistemas son, por supuesto más costosos que el primero. Otro punto de distinción es el hecho de que los sistemas de circuito cerrado de televisión y las tarjetas de identificación requieren cierta cantidad de intervención humana con el fin de controlar el acceso. Esto no es cierto en los demás sistemas. Existen ventajas para ambas partes en la comparación entre la máquina propensa a fallos, que representa una inversión una sola vez en la vida y el guardia no muy eficiente que tiene que ser pagado semanalmente para trabajar. Además, existen sistemas que controlan el acceso en base a atributos físicos, sistemas sofisticados pero nuevos que pueden

estar sujetos a más fallos que los otros, como por ejemplo los sistemas que reconocen huellas digitales o huellas de manos.

2.6 FACTOR HUMANO

Los empleados son el componente más crítico de todo esfuerzo de control de riesgo diseñado a proteger una instalación de procesamiento de datos y un equipo de computación contra fraude. Algunas de las mayores pérdidas en centros de procesamiento de datos y sistemas han sido causadas por o han tenido la participación de algún empleado del centro de procesamiento de datos. Respecto al fraude, el experto en computación Robert Jacobsen ha dicho: "En una instalación típica, el control para todos los propósitos válidos, ha sido entregado a las personas que tienen las mayores oportunidades de cometer delitos".[9]

Este comentario fue corroborado por David R. Lewis de Price Waterhouse pronunciando su discurso en la conferencia de la Risk and Insurance Management Society en San Francisco en 1981. El comentario crudo de Lewis fue que "las políticas de personal que se refieren al empleo, entrenamiento y despido son el factor más importante relacionado con la seguridad de la información".

La experiencia ha demostrado que ciertas medidas de control del personal contribuyen sustancialmente a la seguridad de los centros de procesamiento de datos. Estas medidas incluyen:

° Verificación cuidadosa y entrenamiento para todo el personal de procesamiento de datos;

° Separación de las tareas de programación y operación;

° Limitación del acceso a la zona de almacenamiento de información y a los terminales del sistema únicamente a empleados autorizados;

° Mantenimiento de registros detallados de todos los usuarios en línea del sistema;

° Control estricto de todos los visitantes o personal de servicio que ha tenido acceso al centro de computación;

° Despido de personal sin aviso previo y prohibición instantánea de acceso al computador a todo empleado despedido;

° Conducción de auditorías no planificadas de los procedimientos de seguridad y su cumplimiento por parte del personal.

Sin embargo, es cada vez más claro el hecho de que los controles al personal no son el sustituto de una gerencia efectiva de personal. El gerente de riesgos debe estar consciente que las medidas recomendadas para reducir riesgo tienen el potencial de causar lo opuesto. Si el diseño de un sistema de auditoría y seguridad crea un ambiente de trabajo draconiano, también puede crear el tipo de actitud que motiva los intentos de dañar el sistema de computación. Algunos de

los ataques físicos más destructivos y de las violaciones de seguridad de información más graves, han sido atribuidos a actos maliciosos por parte de empleados.

En un reciente artículo del Wall Street Journal se enfoca otro importante riesgo asociado con el personal de procesamiento de datos: el riesgo de huelga. No hace falta decir que el poder de negociación de un grupo de empleados que llevan a cabo tareas críticas de procesamiento de datos puede ser muy alto. Operaciones completas de procesamiento pueden cerrarse indefinidamente por un grupo muy pequeño de empleados altamente cualificados que se van a la huelga. El artículo cita una huelga en el centro de procesamiento de datos del Gobierno Británico en mayo de 1981: "Menos de 5.000 empleados de computación destruyeron el sistema de recolección de impuestos, interfirieron con la operación de los sistemas de defensa y entre otras cosas, evitaron los pagos a los dentistas en Escocia." 10

3.- PROTECCION CONTRA FRAUDE

3.1 SEGURIDAD EN EL ACCESO A DATOS Y PROGRAMAS - CONTROLES EN EL HARDWARE

En ambientes donde la información es transmitida entre diferentes ubicaciones distantes, existe una exposición a extracción de información de la vía de transmisión. Aunque acceder a esas líneas toma tiempo y es arriesgado, las ventajas que podrían lograrse al obtener información de la competencia pueden ser muy grandes. La utilización de equipos de codifica-

ción para asegurar o proteger la transmisión entre ubicaciones, aumenta significativamente la seguridad de esas transmisiones.

El más conocido standard de codificación fue desarrollado para el National Bureau of Standards en Estados Unidos por la International Business Machines (IBM). El algoritmo, conocido como Data Encryption Standard (DES), utiliza una clave variable de 56 bits para codificar los datos. Esta clave es análoga a la llave de un cerrojo y es utilizada para evitar que los datos puedan ser interpretados al momento de la transmisión y hasta que sean descifrados por la misma clave en el receptor. Para tratar de violar esa clave, un analista utilizando una computadora necesitaría probar una fórmula cada microsegundo y aún en ese caso requeriría de 2.700 años para probar todas las combinaciones posibles. Este sistema está disponible en la actualidad y es fácilmente obtenible.

Otro algoritmo de codificación de datos está siendo desarrollado por la American National Standards Institute en conjunción con un grupo de bancos. Este sistema incorporará mensajes codificados de autenticación para la transferencia de fondos. Este sistema tendrá la ventaja de ser un sistema unificado para todos los bancos, pero pronto estará disponible en los Estados Unidos a fines de este año.

Otro aspecto sobre seguridad de comunicaciones involucra la ubicación de las líneas de transmisión. Al utilizar líneas telefónicas o líneas dedicadas en ubicaciones obvias, el riesgo de intromisión aumenta. El gerente de riesgo debe asegurarse que las líneas

existentes por las cuales se está transmitiendo información delicada estén codificadas y que se instalen líneas con la mayor seguridad posible.

3.2 CONTROL DE ACCESO A PROGRAMAS

El control de acceso a los sistemas de informática a través de software o de programas es una medida que puede utilizarse para proteger contra el fraude. Los sistemas de control incluyen pasos de identificación, autorización y pruebas de auditoría. Estas fases de control pueden tener lugar durante la conexión inicial, la iniciación de un trabajo o el acceso a archivos.

La identificación del usuario toma lugar en el momento de la conexión al sistema. Esta identificación puede incluir el código de identificación del usuario y del trabajo que se pretende realizar. La identificación es típicamente llevada a cabo solicitando al usuario que ingrese su información de identificación aunque ésta podría ser verificada a través de un equipo mecánico tal como un lector de tarjetas.

La autorización es un detalle muy importante para limitar el acceso a programas y a datos. El código de acceso es utilizado para verificar la identificación del usuario. El conectarse a la computadora no debe garantizar el acceso a todas las facilidades del sistema. Ciertos archivos y programas confidenciales deben tener una protección adicional para prevenir el ingreso no autorizado. Aun cuando esto impone restricciones operativas al dueño de los

programas o archivos, debe pesarse contra la magnitud de las pérdidas potenciales causadas por accesos fraudulentos o alteraciones. Además, el sistema debe permitir accesos parciales. Se permite leer un archivo o un programa pero no se permite su modificación. Estas claves de acceso deben ser alteradas con una frecuencia proporcional a la importancia del material, en rangos que van desde por lo menos mensualmente para material importante, hasta anualmente para material menos importante.

El sistema debe ser capaz de mantener en evidencia todos los intentos no autorizados de acceso al material. Debe existir un mecanismo que evalúe estos intentos de acceso. Para evitar que empleados de la empresa jueguen con el sistema, la organización debe hacer muy claro énfasis en la política contra actividades fraudulentas. Además, es importante mantener constancia de todos los accesos a archivos sensibles. Un aumento poco usual en la actividad de acceso a un archivo sensible puede ser indicador de un posible fraude.

3.3 AUDITORES DE PROCESAMIENTO DE DATOS

Los auditores pueden contribuir apreciablemente en la tarea de proteger una instalación de procesamiento de datos contra pérdidas. Cuando se utilizan adecuadamente, pueden efectuar revisiones independientes y objetivas de las instalaciones y de los procedimientos operativos.

En el artículo Guidelines for Automatic Data Processing Physical Security and Risk Management se mencionan los siguientes resultados de una auditoría de sistemas:

1. Evaluar los controles de seguridad de la instalación;
2. Proveer a la gerencia de una oportunidad para mejorar y poner al día su programa de seguridad;
3. Proveer del impulso que mantenga pendientes a los empleados y a los gerentes;
4. Descubrir áreas vulnerables[11].

Para ser efectivo, el auditor debe ser totalmente independiente y estar fuera del área de influencia de la organización de procesamiento de datos. Además, sería bueno encontrar un individuo que no conoce personalmente a la mayoría de las personas que van a ser evaluadas o estudiadas.

Existen gran cantidad de empresas que pueden realizar auditorías de procesamiento de datos. Muchas organizaciones grandes, particularmente los bancos, mantienen su propio staff. Además, cualquier individuo que esté familiarizado con las operaciones de computación o principios de auditoría pueden llenar un cuestionario, tal como el que se provee en el Apéndice A y en base a esto conducir una auditoría aceptable de las operaciones de la organización.

Muchas de las más importantes empresas de contabilidad y auditoría están en capacidad de realizar auditorías de sistemas. La profesión de contabilidad ha sido la que más ha desarrollado técnicas para

detectar fraude por ordenadores Esas técnicas se han desarrollado debido a que el fraude en computación involucra generalmente la manipulación de registros de contabilidad o pagos falsos de dinero a partes no autorizadas. Sin embargo, en consideración a la importancia del potencial para fraudes, el gerente de riesgos debe involucrarse en el diseño de procedimientos y políticas organizacionales diseñadas para prevenir y descubrir las pérdidas, independientemente del grado en el cual se utilicen personas extrañas a la empresa.

3.4 RETENCION Y ELIMINACION DE DATOS

Los medios de almacenamiento tradicionales son las cintas, discos y listados. Cada una de estos tres medios puede representar una exposición importante en un ambiente de procesamiento de datos. Por ejemplo, el que un competidor pueda obtener una copia de un análisis privado de productos, podría resultar en una pérdida de mercado si el competidor es capaz de desarrollar un mejor producto en base a la información provista. El control de los medios de información debe establecerse en varios sitios. Si un programa muy importante está siendo desarrollado, el responsable debe tener instrucciones precisas sobre su protección. Esta debe incluir firmar para aceptar cada uno de los listados y ser auditado periódicamente sobre su ubicación. Los listados no deben dejarse encima de mesas que no están ocupadas y debe exigirse una ubicación central para tirar o destruir documentos confidenciales. Antes de destruir el documento, esta circunstancia debe ser anotada.

Las salas de almacenamiento y los accesos a cintas y discos deben también ser controlados. Debe existir en la biblioteca de discos y cintas una sección especial para almacenamiento de cintas confidenciales. Deben realizarse auditorías periódicas de la existencia y contenido de estos medios de almacenamiento para asegurarse de que no han sido equivocadamente almacenados en otros lugares. Debe mantenerse y auditarse un registro del acceso a cada una de las cintas y discos, con la fecha, persona y hora de acceso. Las cintas y discos deben ser destruidas al final de su vida útil.

4.- ADMINISTRACION DE IMPREVISTOS

4.1 INSTALACIONES DE APOYO.

La existencia de instalaciones de apoyo pueden constituirse en la garantía de seguridad para el control físico del riesgo, o en una pesadilla adicional en el momento de crisis. La clave para el éxito de una instalación de apoyo es su disponibilidad y su compatibilidad. La disponibilidad de instalaciones alternas de apoyo debe pactarse o concretarse a través de un acuerdo escrito, basado en honorarios o en un intercambio recíproco de servicios. Un distribuidor de equipos o una compañía de servicios podría sugerir compañías vecinas que no son de la competencia, pero que sin embargo tienen necesidades y capacidades similares de procesamiento, las cuales puede estar interesadas en la negociación de un acuerdo de respaldo mutuo. Si esto no fuera posible, existen empresas cuyo negocio es proveer apoyo de procesamiento de datos, asignándoles espacio, equipo y

fuentes de energía a suscriptores. El costo de un servicio de apoyo puede ser muy elevado, pero el valor de no interrumpir las operaciones del departamento de procesamiento de datos podría ser aún mayor. Cualquiera que sea el acuerdo, deberá tenerse por escrito, de manera que sea legalmente válido. Cualquier acuerdo menos formal no es un apoyo adecuado en un momento de crisis.

La necesidad de tener equipo compatible en las instalaciones de apoyo es primordial. No se logra nada si las instalaciones de procesamiento de datos están fuera de servicio y las instalaciones de apoyo no pueden ser utilizadas porque no pueden leer los datos o los programas y no pueden llevar a cabo las operaciones necesarias. La compatibilidad debe ser verificada periódicamente utilizando la instalación de apoyo para llevar a cabo operaciones similares a las que tendrían que realizarse en una emergencia. El acceso periódico a las instalaciones de apoyo y a los sistemas de apoyo para realizar pruebas debe ser parte del acuerdo escrito. La mejor garantía de que la instalación de apoyo proveerá protección valiosa cuando se le requiere, consiste en correr los programas y los discos que realmente podrían necesitarse en caso de accidente. Cualquier suposición podría dar un sentimiento de falsa seguridad.

4.2 ALMACENAMIENTO DE DATOS FUERA DEL LOCAL

Es necesario mantener un programa de apoyo de datos que complemente los acuerdos de esta clase para los equipos. El apoyo de datos es una responsabilidad contínua. Se debe establecer un sis-

tema regular de reproducción y almacenamiento de la información esencial. La información de procesamiento de datos es dinámica y cambia sustancialmente en una semana. Existen empresas que están dispuestas a almacenar la información en cinta en cajas fuertes o cámaras. Es responsabilidad del propietario de la información el mantenerla al día. Este tipo de almacenamiento de información fuera de las premisas, es solamente una parte de la ecuación para la protección de la información. La parte más importante es el sistema operacional que se establezca para mantener esa información al día.

4.3 PLAN DE EMERGENCIAS

Si bien todas las inversiones en sistemas de control de riesgos para instalaciones de procesamiento de datos son claramente manifestaciones de la planificación contra imprevistos llevadas a cabo por la organización, debe existir además un documento escrito que en forma explícita describa el plan de respuesta frente a emergencias. La tarea del gerente de riesgos puede compararse a la de un conductor organizacional, cuyo trabajo es el de hacer que los mecanismos de respuesta frente a emergencias funcionen en coordinación unos con otros, cual una armoniosa sinfonía. Extendiendo un poco la analogía, podemos decir que el documento donde está descrito el plan para emergencias de procesamiento de datos, es la partitura en la cual se basarán los esfuerzos de recuperación de la organización, en caso de un desastre.

La necesidad de tener un plan de emergencia para el departamento de procesamiento de datos es clara: Sencillamente no existe otra forma fiable de estructurar una respuesta cuyos costos sean controlables en situaciones de emergencia. Es imposible asignar tiempos, equipos y recursos económicos en una forma eficiente durante el tumulto de un incendio u otra calamidad, a menos de que haya algún documento detallado que describa un plan para la respuesta de la empresa.

Aunque estos documentos corporativos pueden variar de una empresa a otra, deben escribirse de forma que respondan a las necesidades organizacionales. Existen tres factores principales a través de los cuales debe estructurarse el documento de planificación de emergencias. Primero, el plan de emergencias debe ser completo. Las situaciones de emergencia que son poco probables, deben ser analizadas y reconocidas como tales y no simplemente ignoradas. Las situaciones que son más probables, deben ser planificadas con suficiente detalle para garantizar la recuperación dentro de los períodos máximos permisibles de operación.

Segundo, el plan de emergencia debe poder ser utilizado cuando se necesita. Debe estar escrito y organizado como un documento de acción que puede ser consultado en busca de instrucciones específicas durante una emergencia. El manual del plan debe ser puesto al día continuamente de forma que las instrucciones críticas de sistema, los nombres de los suplentes y sus direcciones, los contactos para las facilidades de apoyo en almacenamiento y procesamiento y los teléfonos del personal clave no se con-

viertan en información obsoleta. Es cómodo por ejemplo utilizar un sistema de carpeta de tres agujeros perforado, donde es fácil poner al día los documento periódicamente, además de facilitar su distribución a todas aquellas personas que sean responsables por el plan de emergencia.

Tercero, el plan debe ser puesto a prueba. Repetimos, el plan debe ser puesto a prueba. Se deben realizar simulaciones periódicas de la respuesta a una emergencia a pesar de que éstas impliquen costos adicionales. El plan por sí solo es una inversión importante de dinero y recursos pero las catástrofes son más costosas aún. La verificación periódica de los diversos componentes del plan de emergencia de procesamiento de datos podrá demostrar que la gerencia de riesgos ha provisto de un mecanismo efectivo para recuperarse, o que se requiere reformar el plan y mejorarlo.

5.- CONCLUSIONES

Las actividades de procesamiento electrónico de datos en las empresas han crecido dramáticamente y continuarán haciéndolo. Paralelo a la proliferación de equipos de informática y al aumento en su utilización, han aparecido nuevos retos para el gerente de riesgo.

El centro de procesamiento de datos requiere de características especiales de diseño para sus instalaciones y para sus sistemas de seguridad, de sistemas especiales de protección contra fraude y contra abusos, de análisis específicos de planificación frente a catástrofes potenciales. En resumen, requiere un ataque gerencial completo a los

problemas de riesgo puro. Estas necesidades de análisis de riesgo son las mismas para grandes equipos de informática centrales o para sencillos sistemas descentralizados de procesamiento de datos. Estas necesidades expanden las responsabilidades de la gerencia de riesgo a nuevos campos. Ella debe estar consciente de esta nueva realidad e incorporar el control de pérdidas en instalaciones de procesamiento de datos a las tareas fundamentales de administración de riesgos de la empresa.

APENDICE A

CONTROL DE RIESGOS EN CENTROS DE PROCESAMIENTO DE DATOS - AUTO EVALUACION

INTRODUCCION

Este cuestionario ha sido diseñado para ayudar en la identificación de exposiciones a pérdida y de los costos asociados con ellas, así como para evaluar los sistemas de control de riesgo de las operaciones de procesamiento de datos. Es un documento orientado hacia la acción que busca hacer resaltar las exposiciones a pérdidas, identificar los puntos fuertes y los puntos débiles de los sistemas actuales de control de riesgo e iniciar mejoras cuando éstas sean necesarias. La parte final de la forma, presenta un contexto dentro del cual puede cuantificarse el potencial de pérdida catastrófica. El formulario debe ser completado por personas que estén familiarizadas con las operaciones y procedimientos del centro de procesamiento de datos.

La primera sección de la encuesta consiste en un número de preguntas que deben ser contestadas "Si" o "No" o "No aplicable", con comentarios adicionales agregados en los espacios que se proveen. Una respuesta de "Sí" es una indicación de que la exposición ha sido identificada y mitigada. La respuesta de "No" es una indicación de que la exposición no ha sido identificada, o si ha sido identificada no se ha tomado acción al respecto. A sabiendas de que las decisiones de control de riesgo están basadas en una amplia variedad de factores, no hemos tratado de clasificar de ninguna manera las diferentes exposiciones o la adecuación de los sistemas de control. Sin embargo, en términos generales, una instalación de procesamiento de datos que tiene un alto nivel de seguridad contestaría positivamente a la mayoría de las preguntas.

La persona que está conduciendo la evaluación debe tomar en cuenta que ésta es una guía para autoevaluación, no un conjunto de reglas concretas o de estándares aplicables a todos los casos.

El objetivo de la última sección de la forma de evaluación, es el de ayudar a estimar los costos de las pérdidas, en el caso en que las instalaciones de procesamiento de datos se destruyan completamente. Se ha dicho muchas veces que son pocos los altos ejecutivos de las empresas modernas que conocen el grado en que sus negocios dependen de la continuidad de los servicios de procesamiento de datos. En la mayoría de los casos el estar desprovisto de este servicio por un período extenso de tiempo puede generar pérdidas sustanciales de ingresos. En esta sección se trata de determinar la magnitud de la pérdida potencial para estos casos.

1.- Información General

Nombre de la empresa u organización objeto de la evaluación _____

Dirección del centro de procesamiento de datos (calle, ciudad, provincia, etc.) _____

Número telefónico _____

Nombre y título de la persona responsable de la instalación de procesamiento de datos _____

Nombre y título de la persona responsable de llenar el cuestionario _____

Fecha de respuesta al cuestionario _____/_____/_____

Situación de las instalaciones principales de procesamiento de datos, en orden de importancia para la organización. (Ciudad y Provincia o Estado).

_____ _____
_____ _____
_____ _____
_____ _____
_____ _____

gerencia de riesgos

II. CONSTRUCCION DE LA INSTALACION DE PROCESAMIENTO DE DATOS (SEGURIDAD FISICA)

	SI	NO	N/A
A. Edificio donde está situado el Centro			
1. ¿Está el edificio a más de 15 metros del edificio, calle o vía férrea más cercana?			
2. ¿Está la edificación construida con materiales resistentes al fuego?			
3. ¿Están todas las puertas de la instalación construidas con materiales resistentes al fuego?			
4. ¿Se han eliminado todos los carteles o signos fuera o dentro del edificio, que indican la presencia de un centro de procesamiento de datos?			
5. ¿Está la instalación de procesamiento de datos físicamente separada de otras instalaciones, por ej. entradas separadas o pisos distintos?			
B. Sistema de Aire Acondicionado			
1. ¿Posee el centro de procesamiento de datos su propio sistema de aire acondicionado?			

gerencia de riesgos

	SI	NO	N/A
2. Si la respuesta a la pregunta anterior es sí, ¿están los compresores situados fuera del centro de procesamiento de datos?			
3. Si la respuesta a la pregunta 1 es sí, ¿puede el sistema de aire acondicionado del resto del edificio ser puesto en funcionamiento para suplir el centro de procesamiento de datos?			
4. Si la respuesta a la pregunta anterior es sí, ¿esta alternativa permitiría operaciones normales del centro por lo menos por 24 horas?			
5. ¿Existe un sistema de detección automática de incendio en los conductos del aire acondicionado?			
6. ¿Existen esclusas automáticas de humo en los conductos del aire acondicionado?			
7. ¿Está la toma de aire del sistema de aire acondicionado protegida con mallas?			
8. ¿Existe un interruptor manual del sistema de aire acondicionado dentro o cerca del centro de procesamiento de datos?			
9. ¿Está el aire frío humidificado adecuadamente para reducir la estática?			

gerencia de riesgos

	SI	NO	N/A
C. Salón de Procesamiento de Datos			
1. ¿Están los equipos de procesamiento de datos situados en un salón especial?			
2. ¿Existe un piso falso elevado?			
3. ¿Son las paredes, piso y techo de la habitación, incombustibles?			
4. ¿Está el techo encima del centro de procesamiento de datos, sellado a prueba de agua?			
5. ¿Se han bloqueado las ventanas del centro de procesamiento de de datos de manera que no sea posible ver desde fuera hacia dentro?			
6. ¿Están los vidrios del centro de procesamiento de datos protegidos contra objetos extraños?			
B. Servicios Públicos			
1. ¿Son los servicios de alimentación eléctrica y telecomunicaciones al edificio subterráneos?			
2. ¿Existe más de una fuente de suministro eléctrico?			

gerencia de riesgos

	SI	NO	N/A
3. ¿Existe más de una línea para telecomunicaciones?			
4. ¿Existe más de una línea de suministro de agua?			
5. ¿Está todo el equipo electrónico del centro de procesamiento de datos controlado por un panel eléctrico independiente?			
6. Si la respuesta a la pregunta anterior es sí, ¿está este panel de fácil acceso al operador y está cerca a la puerta de salida?			
7. ¿Se apagan automáticamente las fuentes automáticas ininterrumpibles de energía si es que entran a funcionar los sistemas de rociadores de la sala de procesamiento de datos?			
8. ¿Se ha verificado la calidad del suministro eléctrico a la computadora?			
9. Si la respuesta anterior es sí, y los resultados fueron poco adecuados, ¿se instaló algún transformador de aislamiento y regulación?			
E. Sistemas de Detección y Extinción de Incendios			
1. ¿Existe un sistema automático de detección de incendios?			

gerencia de riesgos

	SI	NO	N/A
2. Si la respuesta a la pregunta anterior es sí, ¿es un sistema de detección de humo?			
3. Si la respuesta a la pregunta anterior es sí ¿existe un detector diferencial de cambio de temperatura?			
4. ¿Existe una caja de alarma manual contra incendios en la sala de procesamiento de datos?			
5. ¿Están protegidas las áreas de almacenamiento de registros y material combustibles por sistemas automáticos de rociadores?			
6. ¿Está protegido el equipo electrónico de procesamiento de datos por un sistema automático de extinción de Halon 1301?			
7. Se encuentra protegido el espacio por encima del techo falso por un sistema automático de detección y extinción de incendios?			
8. ¿Está el espacio debajo del piso falso protegido por un sistema automático de detección y extinción de incendios?			
9. Tienen los sistemas automáticos de extinción una válvula manual de cierre convenientemente asequible?			

gerencia de riesgos

	SI	NO	N/A
10. ¿Existen extintores portátiles en el salón de procesamiento de datos?			
11. Si la respuesta anterior es sí ¿están conveniente y visiblemente ubicados?			
12. ¿Existen procedimientos de emergencia escritos para ser utilizados en caso de un incendio?			
13. Si la respuesta anterior es sí ¿han sido verificados estos procedimientos?			
14. ¿Está prohibido fumar dentro del centro de procesamiento de datos?			
F. Seguridad del Local			
1. ¿Está controlado el acceso al centro de procesamiento de datos?			
2. Si la respuesta anterior es sí ¿existen sistemas de identificación visual, por atributos físicos o por tarjeta magnética?			
3. Si la respuesta anterior es sí ¿está el sistema diseñado para impedir el ingreso a ex-empleados?			
4. Si la respuesta a la pregunta 1 es sí, ¿se utiliza un cierre con combinación?			

gerencia de riesgos

	SI	NO	N/A
5. Si la respuesta anterior es sí, ¿se cambia la combinación del cierre por lo menos cada mes?			
6. Si la respuesta a la pregunta 4 es sí, ¿se cambia la combinación cuando un empleado clave es retirado de la empresa?			
7. ¿Está controlado el acceso al área de almacenamiento de información magnética?			
8. ¿Está controlado el acceso a las áreas de los equipos de soporte de telecomunicaciones?			
9. ¿Existe uno o más sistemas para detectar las entradas por la fuerza a la sala de procesamiento de datos o de almacenamiento de información?			
10. ¿Se realizan pruebas esporádicas de seguridad física y de procedimientos de acceso?			
11. ¿Se han asignado las responsabilidades para la evaluación y respuesta a cualquier intento de ingreso no autorizado?			

gerencia de riesgos

G. Política de Personal

	SI	NO	N/A
1. ¿Se están dirigiendo verificaciones de seguridad a todo el personal que ingresa a la zona de procesamiento de datos, almacenamiento de información o telecomunicaciones, incluyendo:			
a) Operadores			
b) Usuarios			
c) Mensajeros			
d) Personal de mantenimiento			
e) Personal de limpieza			
f) Guardias			
g) Otros (Especificar)?			
2. ¿Está todo el personal de las áreas de procesamiento de datos bajo observación visual continua?			
3. ¿Está restringido el ingreso rutinario en el centro de procesamiento de datos a solamente aquellas personas que trabajan en el área?			
4. ¿Existe un mecanismo para registrar cada ingreso y salida de personas cuya área de trabajo no es la del centro de procesamiento de datos?			
5. ¿Se requiere que cada persona porte una identificación visible, indicando su autorización de acceso?			

gerencia de riesgos

	SI	NO	N/A
6. ¿Se escolta a todas las personas no autorizadas?			
7. Después de que un empleado es despedido, ¿se le prohibe ingresar al centro de procesamiento de datos o de almacenamiento de información?			
III PREVENCION DE FRAUDES			
A. Seguridad del acceso a datos y programas Control de Hardware			
1. ¿Están los terminales remotos asegurados cuando no están en uso?			
2. Se encuentran codificadas las transmisiones hacia o desde ubicaciones remotas?			
3. ¿Se han situado las líneas de transmisión de información de manera que se minimice la posibilidad de extracción de información de las mismas?			
B. Controles de Programas			
1. ¿Existe un control de ingreso al sistema basado en una identificación de usuario y código de autorización?			
2. ¿Está controlado el inicio de un trabajo y el acceso a archivos, sobre la base de un número de identificación y una autorización?			

gerencia de riesgos

	SI	NO	N/A
3. ¿Se cambian las claves de acceso por lo menos cada dos meses?			
4. La autorización de uso del sistema cesa en el momento en que finalizan las necesidades del usuario?			
5. ¿Puede el sistema detectar intentos no autorizados de acceder a información confidencial?			
6. ¿Existe una persona cuya responsabilidad es investigar los intentos no autorizados de acceder a información confidencial?			
7. ¿Están las cintas y discos que almacenan información confidencial marcados de acuerdo a una clasificación?			
8. ¿Existen restricciones sobre el manejo de cintas y discos que contienen información restringida para prevenir accesos no autorizados?			
9. ¿Se lleva a cabo un inventario por lo menos trimestral de las cintas y discos que contienen información confidencial?			
10. ¿Existe un sistema bien definido para clasificar los programas y los datos?			
11. ¿Se han identificado los dueños de todos los programas y todos los datos?			

gerencia de riesgos

	SI	NO	N/A
C. Procedimientos de auditoría			
1. ¿Está contabilizado e informado todo el tiempo de uso de la máquina?			
2. ¿Se audita periódicamente la utilización de la máquina?			
3. ¿Lleva el sistema un control automático de la actividad de los archivos para detectar variaciones poco usuales?			
D. Políticas de personal para con los usuarios del sistema			
1. ¿Se tiene la práctica de trasladar a los empleados de un trabajo a otro, periódicamente?			
2. ¿Se requiere de los empleados que tomen vacaciones periódicas, suspendiendo su derecho de ingreso al centro de procesamiento de datos?			
3. ¿Se eliminan automáticamente los códigos de acceso de los empleados que han sido despedidos?			
4. ¿Se investiga a los potenciales usuarios del sistema antes de ser contratados?			
5. ¿Se investiga a los usuarios del sistema anualmente después de ser contratados?			

gerencia de riesgos

	SI	NO	N/A
6. ¿Están todos los usuarios familiarizados con las políticas referentes a la clasificación de seguridad de los programas y los datos?			
E. Retención o destrucción de Registros			
1. ¿Están almacenados en una cámara contra fuego todas las cintas o discos que son necesarios mantener en el centro de cálculo?			
2. ¿Se mantienen duplicados de los programas?			
3. ¿Se mantienen duplicados de los datos?			
4. Si la respuesta anterior es sí, ¿se almacenan estos duplicados lejos del centro de cálculo?			
5. ¿Se despliega claramente la clasificación de seguridad de la información en toda entrada o salida de datos?			
6. ¿Firma el personal cuando retira listados confidenciales?			
7. Si la respuesta anterior es sí, ¿existen ubicaciones específicas para deshacerse de listados confidenciales después de su uso?			
8. ¿Los listados confidenciales son quemados o destruidos después de ser tirados?			

gerencia de riesgos

	SI	NO	N/A
9. ¿Se requiere de los empleados el que mantengan el material confidencial en un área segura cuando no se está utilizando?			
10. ¿Se destruyen todos los medios magnéticos una vez que ha terminado su uso?			
4. EVENTUALIDADES			
A. Equipos			
1. ¿Existe un acuerdo para utilizar otras instalaciones en caso de emergencia?			
2. Si la respuesta a la pregunta anterior es sí, ¿es por escrito y firmado?			
3. ¿Se conducen pruebas en la instalación de respaldo por lo menos anualmente?			
B. Programas			
1. ¿Se mantienen copias duplicadas de los programas y los datos?			
2. ¿Los duplicados de programas y datos se realizan con una frecuencia compatible con la velocidad de sus alteraciones?			
3. ¿Se mantienen las copias duplicadas en un edificio alejado del centro de procesamiento de datos?			
4. ¿Se mantienen las copias en una cámara contra incendio?			

gerencia de riesgos

	SI	NO	N/A
C. Plan de emergencia			
1. Se ha instruido al personal: a) ¿En el uso de extintores de incendio?			
b) ¿En como hacer sonar e informar de una alarma de incendio?			
c) ¿En la forma de llamar a la policía o a otro personal de seguridad?			
d) ¿En la forma de evacuar el centro de procesamiento de datos en caso de incendio, amenazas de bombas, etc.?			
e) ¿En la manera de detener la operación del centro de procesamiento de datos en una emergencia?			
2. ¿Existe un plan de emergencias por escrito?			
3. Si la respuesta anterior es sí: a) ¿Se ha familiarizado a todo el personal con sus características?			
b) ¿Se han conducido ensayos del plan?			
D. Suministros públicos			
1. ¿Existe una fuente auxiliar de energía?			
2. ¿Existe iluminación de emergencia en el salón de procesamiento de datos?			

	SI	NO	N/A
3. ¿Existe una fuente auxiliar de aire acondicionado?			
4. ¿Existe una fuente de reserva de agua o una fuente secundaria de agua para atender el aire acondicionado y los equipos de computación?			

COSTOS DE LAS PERDIDAS

Para llenar el resto de este cuestionario, suponga que todos los equipos de procesamiento de datos y todos los programas situados en el edificio donde se encuentra el centro de procesamiento de datos han sido destruidos. El evento ha destruido todo el edificio, incluyendo los contenidos de las cámaras contra incendio ubicadas dentro del edificio. La información y los equipos situados fuera del edifico o en otros edificios, no han sido dañados y pueden ser utilizados en la reconstrucción de la operación de procesamiento de datos. Suponga también que nadie del personal ha sufrido daños y que ningún equipo o papeles fueron sacados del local durante la evacuación. Finalmente, suponga que este evento catastrófico ocurrió en el peor momento posible durante una semana típica.

A continuación se dan algunos comentarios que tienen por finalidad ayudarlo a completar la forma de resumen de costos de las pérdidas. Todas las cifras son por supuesto estimadas y deben ser expresadas en dinero corriente, sin deducciones de impuesto. Las recuperaciones de aseguradores o de otros no deben incluirse. El objetivo es poder determinar aproximadamente cuánto costaría y cuánto demoraría la reconstrucción de la operación para llevarla lo más similar posible a la que existía inmediatamente antes del evento hipotético al que hemos hecho mención. Este análisis no es un ejercicio académico, es más bien un intento de determinar las implicaciones de costo de un evento que ha sucedido en otras ocasiones y que podría sucederle a usted.

Ambiente - Incluya bajo el ambiente solamente los costos de reconstruir el ambiente de procesamiento de datos, no incluya el costo de reconstruir el edificio. Incluya el costo de todos los equipos de telecomunicaciones, el aire

acondicionado, las fuentes auxiliares de energía, los sistemas de seguridad, los sistemas automáticos de detección y extinción de incendios, etc.

Equipos - Adjunte una lista de todos lo equipos bajo el siguiente formato. En la columna denominada descripción indique el tipo de equipo, por ejemplo: unidad de memoria, impresora, unidad de cinta, etc.

FABRICANTES	DESCRIPCION	MODELO N°	PROPIO O ALQUILADO	VALOR DE REEMPLAZO	VALOR EFECTIVO

Adjunte una copia de cada contrato de alquiler o arrendamiento financiero.

Incluya el valor de reemplazo o el valor efectivo actual de todos los equipos que son propiedad de la empresa. Incluya el incremento, si es que existiera, en el costo de alquiler de equipos arrendados. Para los equipos normalmente arrendados, incluya los pagos de arrendamiento que continúan después de la pérdida.

Programas - Incluya el valor de reemplazo de los suministros de papel, tarjetas, cintas magnéticas, discos, etc., además de los costos para reconstruir los programas y los datos perdidos. Incluya el valor del tiempo del personal y de las máquinas.

gerencia de riesgos

Valor Neto Anual del Trabajo Realizado por Otros

Esta sección sólo tiene aplicación si usted realiza trabajos para empresas externas, o sea empresas que no forman parte de su organización. Se sugiere la utilización de un período de 12 meses pero esto es arbitrario, utilice el período de tiempo que más claramente indique las características de su situación particular.

1. Si usted va a perder ese negocio, determine el importe bruto que hubiera recibido de fuentes externas, durante los siguientes 12 meses y reste a esta cifra el costo de realizar estos servicios. (Básicamente sueldos y suministros).

2. Si usted va a continuar atendiendo ese negocio, incluya solamente los gastos extras atribuibles al servicio por el período hasta que las operaciones hayan sido restituidas a su nivel original.

3. Si va a continuar atendiendo sólo una parte del negocio, aplique los métodos 1 y 2 indicados arriba a las partes que corresponda e incluya el total.

Gastos Extra

Incluya el costo de operar una instalación temporal de procesamiento de datos o de utilizar el equipo de procesamiento de datos de otra empresa, menos aquellos gastos de la instalación destruida que ya no continúan, como el alquiler de equipos, electricidad, etc. Incluya en el cálculo el alquiler de los equipos o utilice tarifas de horas extras y gastos adicionales de empleados, costos de establecer, operar y terminar operaciones si es que se requiere un local temporal, etc. Agregue una cifra de gastos extras no previsibles de por lo menos 15%. Incluya tam-

bién una estimación de lo que le costará a los demás departamentos y divisiones de la empresa el conducir sus operaciones, tales como nómina, que no pueden llevar a cabo en el equipo alterno o en la ubicación temporal.

Pérdida de Ingresos

Incluya una estimación del valor de la pérdida dentro de su organización, que puede ser asignada a la destrucción del centro de procesamiento de datos. Esta sección será la más difícil de completar y puede representar también el mayor potencial de pérdidas. Lo que se necesita es conocer la pérdida de ingresos antes de los impuestos, es decir, el valor de la pérdida permanente a toda la organización. El cálculo puede involucrar la interdependencia de muchas unidades de producción. El resultado puede variar en función de si la empresa está operando a máxima capacidad o no.

Estime los ingresos netos antes de impuestos para cada unidad de la empresa que se vería afectada materialmente por la destrucción del centro de procesamiento de datos. Ingrese la cifra total en la línea adecuada de la forma. A continuación aparece un formato para el cálculo de esta pérdida.

SITUACION (Ciudad y Provincia o Estado)	PERDIDA POR MES	NUMERO DE MESES	TOTAL
_____	$ _____	_____	$ _____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
		TOTAL	$ _____

RESUMEN DE COSTOS DE LAS PERDIDAS

	TIEMPO REQUERIDO PARA REEMPLAZARLO EN MESES	COSTO PARA REEMPLAZARLO E INGRESOS PERDIDOS
Ambiente	_____	_____
Hardware	_____	_____
Software		
Programas	_____	_____
Datos y suministros	_____	_____
Valor neto de trabajos a terceros		_____
Gastos extras		_____
Pérdida de ingresos		_____
COSTO TOTAL DE PERDIDAS		_____

gerencia de riesgos

BIBLIOGRAFIA

42 Suggestions for Improving Security in Data Processing Operations, Report No. G520-2797-0, IBM Corporation White Plains, New York.

Alloway, David N., "Computer Crime: Part II," Risk Management Manual, Supplement No. 51-7/80.

Audit and Evaluation of Computer Security II: System Vulnerabilities and Controls, NBS Special Publication 500-57, April 1980.

"The Automatic Sprinkler in Controversial Settings," Factory Mutual Record, Factory Mutual System, November-December, 1980.

Barclay, Dolores, "Today's Focus: Corruption Increasing in the Marketplace," The Associated Press, September 14, 1980.

Bryce, Heather, "The NBS Data Encryption Standard: Products and Principals," Mini-Micro Systems, March, 1981.

"Census Bureau Crisis," The Washington Post, April 10, 1979.

Computer Security Institute, Computer Security Buyer's Guide, Computer Security Institute Press, 1980.

"Computer Strike Snags a Bureaucracy," The Wall Street Journal, May 19, 1981.

The Considerations of Data Security in a Computer Environment, Report G520-2169, IBM Corporation, White Plains, New York.

The Considerations of Physical Security in a Computer Environment, Report G520-2700-0, IBM Corporation, White Plains, New York.

Data Security Through Cryptography, Report GC22-9062-0, IBM Corporation, White Plains, New York.