Seguridad en centros de procesamiento de datos

1. INTRODUCCIÓN

Debido a la evolución de las tecnologías, de los servicios y de los entornos empresariales en general, la información se ha convertido quizás en el primer patrimonio de las empresas. De ahí que se pueda asegurar que la Seguridad en los Centros de Procesamientos de Datos (C.P.D.) es una necesidad impuesta a toda entidad o empresa de cualquier rango.

La seguridad constituye, por consiguiente, uno de los principales problemas en todo sistema de procesamiento de datos; la expansión de los sistemas informáticos hace que sea imprescindible la implantación de nuevos elementos de seguridad que protejan de una forma adecuada estos entornos.

2. RIESGOS DE LOS CENTROS DE PROCESAMIENTOS DE DATOS

La seguridad del Centro de Procesamiento de Datos hace referencia a los riesgos que afectan a las instalaciones donde se encuentra el mismo y a las soluciones que han de adoptarse para su protección.

La clasificación general de estos riesgos contemplados desde la posibilidad de que ocurra un evento/siniestro en función de los recursos y el entorno, es la siguiente:

Siniestros en:

- Recintos y edificio
- Instalaciones auxiliares
- Equipos o hardware
- Software

Mapa de riesgos:

- Incendio
- Gases
- Explosión/implosión
- Daños por agua
- Rayo. Tensión inducida
- Sobretensiones/cortocircuitos
- Robo. Hurto
- Actos vandálicos
- Avería de componentes
- Cambio de condiciones ambientales
- Virus informático
- Modificaciones o espionaje de datos
- Pérdidas de datos/copias de seguridad

Algunos de estos riesgos representan una problemática diferente, que debe ser tratada individualmente y de acuerdo con las peculiaridades de cada instalación.

Incendio

Todos los incidentes producidos a causa del fuego en un C.P.D. pueden causar un daño significante y graves pérdidas incluso cuando se trata de fuegos pequeños. Los gases corrosivos y el humo desprendido por el PVC y otros plásticos en combustión pueden dañar las placas del circuito electrónico. Además el calor generado puede destruir la sensibilidad del equipo y dañar el disco duro.

- **Causas de incendio**

  La experiencia ha demostrado que los fuegos se producen principalmente por:

  - Inflamación del aislante del cableado por aumento del calor.
  - Negligencia provocada por fumadores o trabajos con fuegos abiertos incontrolados, como puede ser la soldadura.

- Defectos de los componentes eléctricos del equipo, especialmente fuentes de alimentación.
- Cortocircuitos.
- Incendios exteriores a las instalaciones.

- **Daños producidos**

  Los daños producidos en el C.P.D. en caso de incendio son fundamentalmente:

  - Derrumbamientos.
  - Deformaciones parciales y totales de los equipos.
  - Oxidaciones en los componentes microelectrónicos producidas por los humos de las combustiones y el agua y humedad relativa elevadas, provenientes de las tareas de extinción, como de los gases generados en incendio.

- **Medidas para limitar los daños después del incendio**

  Los daños de incendio comprenden los daños directos e indirectos consecuentes del incendio.

  Desde el momento de la concepción del incendio en el C.P.D., se deben estudiar las medidas para minimizar las consecuencias del mismo.

  Las medidas a tomar en el caso del equipo y del soporte registrado serán las siguientes:

  a. *Equipo*:

     Para limitar la corrosión sobre el equipo se procederá:

     - Limpiar aspirando la mayor parte de los hollines depositados sobre los aparatos y equipos.
     - Embalar estos herméticamente y sacar el aire del embalaje.La desecación del aire en el interior del embalaje se obtiene mediante la utilización de sales hidrófilas como el silicagel.
     - Si el almacenamiento se debe prolongar, renovar el silicagel.

  b. *Soportes registrados*:

     Nada más acabar el incendio se procederá al salvamento y a la limpieza de los soportes registrados implicados en el siniestro y se hará una copia rápidamente.

- **Sistemas contra incendios**

  Se define de este modo a las actuaciones y medios de protección contra incendios exigibles a cualquier instalación, sea cual sea su potencial de incendio.

  Dichas medidas en un Centro de Procesamiento de Datos serán:

  - Extintores portátiles de CO_2 de 5 Kg.
  - Bocas de incendio equipadas situadas próximas a la entrada del centro. Estas bocas de incendio dispondrán de lanza de tipo "eléctrico", esto es, con posiciones de cierre y niebla.
  - Hidrantes exteriores a la edificación.
  - Abastecimiento de agua adecuado, con suficiente cantidad de agua para la extinción y con la presión necesaria.
  - Diseño adecuado de la red de agua contra incendios.

- **Sistema de extinción y detección de incendios**

  El objetivo es proteger completamente el edificio donde está el C.P.D. de no ser posible se deberá proteger al menos:

  - El sector contra incendio que contiene el área de procesos de datos.
  - La sala contigua al área de procesos de datos.
  - El suministro de aire del área de proceso de datos.

  Se puede omitir la protección de falso suelo o techo sólo cuando éstos no contengan materiales combustibles o fuentes de ignición.

  El C.P.D. puede contar con los siguientes sistemas de protección contra incendios de funcionamiento automático, cuya sucesiva implantación aumentará considerablemente su nivel de seguridad:

  - Detección automática de incendios.
  - Rociadores automáticos de acción previa.
  - Sistema de extinción automática por CO_2.
  - Sistemas de nebulización de agua.

- **Detección automática de incendios**

  La instalación de detección de incendios tiene una doble misión:

  1. Avisar del inicio de un incendio al encargado del área de informática, o responsable de seguridad.
  2. Desconectar la corriente eléctrica al ordenador, el sistema de ventilación, cerrar de las compuertas cortafuego y disparar el sistema de extinción automática.

  Para la detección en la propia sala también puede emplearse un sistema de fuegos incipientes que muestra y analiza en continuo el aire del local protegido. El aire se aspira por conductos mediante un ventilador y a través de una red de tuberías es conducido a un detector de alta sensibilidad.

  

  Se instalará un sistema de detección automática de incendios de tipo "puntual-analógica-inteligente", en falso techo, falso suelo y ambiente. Este sistema de detección será el encargado del disparo del sistema de CO_2 de inundación total del falso suelo y del llenado de las tuberías del sistema de rociadores, si existiesen tales instalaciones.

  Se utilizarán detectores iónicos de humos para detectar fuegos abiertos, como pueden ser lugares donde se almacene papel.

  Por regla general, el conducto de ventilación también debe protegerse mediante sistemas de aspiración con detectores iónicos de humo.

- **Sistemas de Extinción Automática por CO_2**

  Los rociadores automáticos se justifican cuando el edificio no dispone de las garantías suficientes contra incendio o cuando el C.P.D. se encuentra ubicado en un edificio con cobertura de rociadores automáticos y la separación del centro con el edificio no tiene suficiente resistencia al fuego.

Además se instalarán sistemas independientes de aplicación local de CO_2 dentro de las carcasas de las C.P.U.

Este sistema de detección de puntual da la alarma y señala el armario donde posteriormente se producirá descarga del CO_2 en su interior.

Análogamente puede explicarse en los falsos techos y falsos suelos.

- **Sistemas de Protección Contra Incendios**
    - CO_2 en ambiente:

      La función de esta instalación, es la extinción de un fuego cuando está todavía en estado incipiente y si es necesario, mantener la precisa concentración de CO_2 durante el tiempo concreto para minimizar el peligro de una reignición.

En toda instalación en la que las personas puedan estar en peligro, deben preverse salvaguardias para asegurar la rápida evacuación de la zona, para evitar que se entre en la misma después de la descarga, y para disponer de medios para el inmediato rescate de personal atrapado. Deberán considerarse aspectos relacionados con la seguridad tales como formación del personal, señalización de emergencia, alarmas y dispositivos de retardo.

La concentración de CO_2 necesaria para un efecto extintor suficiente es peligrosa para la vida de las personas en la zona inundada.

Deberán cumplirse los siguientes requisitos:

- Previsión de rutas de evacuación, que deben mantenerse libres en todo momento y adecuadamente señalizadas.
- Una zona inundada no debe servir como única ruta de evacuación para otras zonas.
- Las puertas deben abrirse únicamente hacia afuera, mantenerse cerradas automáticamente y deberán poder abrirse desde dentro, aún en le caso de que estén cerradas desde fuera.
- Las alarmas serán diferentes de cualquier otra zona de señalización de alarma y operarán inmediatamente, una vez detectado el fuego.
- Se dispondrá de indicaciones luminosas en las entradas, hasta que la atmósfera se haya hecho segura.

- Se instalarán señales de instrucciones de emergencia e instrucciones en las entradas.
- Se dispondrá de medios para ventilar las zonas una vez extinguido el fuego.

- Rociadores:
  - Standard
  - Tubería seca
- Nebulización de agua:

  El agua nebulizada basa su principio extintor y de control de fuego en tres acciones diferentes:

  - Enfriamiento.
  - Desplazamiento del oxígeno por vapor de agua.
  - Atenuación del a transmisión de calor por radiación.

  El efecto de enfriamiento se optimiza al máximo, por la división del agua aplicada en gotas extremadamente pequeñas (80-200μ), lo que resulta en un incremento de la superficie de absorción de calor y maximización de la producción de vapor. El proceso de vaporización extrae calor de la llama y de los vapores inflamables, produciendo la extinción.

  El vapor de agua al expandirse desplaza el aire y reduce consecuentemente la cantidad de oxígeno que alimenta la combustión. Si este vapor puede quedar confinado en la proximidad del incendio, caso de recinto cerrado, o puede ser proyectado directamente a la base de las llamas, el oxígeno libre queda reducido consiguiéndose el cese de la combustión. Por otro lado las pequeñísimas gotas de agua quedan suspendidas en el aire, reduciendo la transmisión de calor, por radiación, entre las llamas y el combustible no volatilizado, impidiendo su contribución a la continuidad del incendio.

Gases

- **Causas de desprendimiento de humos**

  Centrándonos en los daños posteriores al incendio producidos por gases, están los producidos por HCl, sobre todo cuando se ha quemado PVC. El HCl se encuentra en forma de materiales de aislamiento, cables eléctricos, pavimentos plastificados, puertas plegables, etc.

  El HCl comienza a desprenderse del PVC a partir de una temperatura de 120ºC, y al llegar a 300ºC, ya se puede desprender en su totalidad de cualquier tipo de PVC.

  Otros gases de combustión se desprenden de productos de limpieza o disolventes.

- **Daños producidos**

  La acción de los gases se puede detectar a simple vistas debido:

  - El hierro es coloreado de marrón oscuro.
  - En el acero inoxidable las superficies se vuelven mates, apareciendo manchas de color marrón oscuro con puntos negros en el centro.

  En el cobre comienzan a aparecer manchas rojas y a continuación de un color verde claro.

- **Medidas para limitar los daños después del siniestro**

  - Se evacuarán lo antes posible, con permiso de los bomberos, los gases provenientes de la combustión al exterior abriendo ventanas y puertas, por efecto Venturi o mediante equipos de evacuación de humos.
  - Se desconectarán lo antes posible los equipos de aire acondicionado y ventilación.
  - Se cerrarán todas las puertas y ventanas que comuniquen con el resto del edificio.

- Se evitará tocar o manipular los equipos hasta la llegada de un especialista.
- Se evacuará el agua utilizada durante las tareas de extinción, ante la existencia de rociadores automáticos en el área de informática o proveniente de tareas de extinción en otras áreas, directamente al exterior.
- Se limpiarán los equipos aspirando los hollines depositados en su interior.
- Se salvarán y limpiarán inmediatamente los soportes magnéticos. Se recuperarán todos los datos posibles, aunque la recuperación sea parcial.

Agua

- **Causas de los daños por agua**

  Los daños producidos por el agua se entienden como inundaciones debidas a diversas causas, como son la rotura de conducciones, de agua sanitaria o de los equipos acondicionadores de aire, las extinciones de incendios y las inundaciones propiamente dichas.

- **Medidas de prevención**
  - Se tendrá en cuenta que no pase ninguna conducción de agua o desagües por la vertical del Centro de Procesamiento de Datos.
  - Será necesario que la impermeabilización de las cubiertas se haga contemplando normas más estrictas para otros edificios, poniendo especial cuidado tanto en la calidad de los materiales utilizados como en la ejecución de la mamo de obra.
  - Deberá existir una impermeabilización al agua de todos los conductos que penetren dentro del C. P.D.
  - No deberán existir bandejas de condensación en el falso suelo ni en el falso techo.

Modificación o espionaje de datos

- **Causas**

  En los entornos del C.P.D. se incluyen como errores y omisiones, los problemas de organización, los montajes incorrectos de soportes de datos, la liberación de ficheros no caducados, la distribución incorrecta de información confidencial, los trabajos realizados con versiones de programas incorrectas, etc.

  El espionaje de datos es causado generalmente por empleados insatisfechos o descontentos. La utilización fraudulenta de datos o software puede dar lugar a pérdidas importantes en la empresa.

- **Control de riesgos**

  Las medidas para el control de riesgos se centran básicamente en el control de accesos al C.P.D. y las medidas de seguridad para la utilización de aplicaciones y datos que se desarrollarán más adelante.

3. PROTECCIÓN DE SERVICIOS TÉCNICOS

3.1 Energía eléctrica

Es importante tener contratadas dos compañías suministradoras de electricidad independientes para evitar así la falta de alimentación. En caso de no disponer de una segunda fuente de energía externa, se debe salvaguardar la continuidad de la corriente mediante baterías que aseguren automáticamente y sin interrupción el funcionamiento adecuado de la instalación al menos durante 60 horas o bien grupos electrógenos. En caso de fallo de energía, se deben iluminar las salas con luces de emergencia.

En los casos en los que una interrupción del ordenador suponga grandes pérdidas económicas, se utilizarán cables F3 capaces de suministrar corriente incluso cuando tenga lugar un incendio. Estos cables serán utilizados para la alimentación del ordenador, la instalación de aire acondicionado y la instalación de protección contra incendios.

3.2 Aire acondicionado

Debido a la permanente facilidad a dañarse de los equipos electrónicos cuando se exponen al calor, es conveniente su localización en salas debidamente acondicionadas en las cuales se realice un control riguroso de la temperatura y humedad ambiente con instalaciones de acondicionamiento.

Las unidades del C.P.D. suelen disponer de indicadores o sensores de las variaciones anormales de temperatura y humedad, que desconectan el equipo electrónico, evitando así posibles daños.

Los conductos de ventilación representan un riesgo importante de extensión del incendio y de humo a sectores distintos de los de origen. Por ello deben estar formados por elementos resistentes al fuego. Para evitar la propagación del incendio dentro del propio conducto cada vez que atraviesen un sector de compartimentación se deberá disponer de trampillas cortafuego.

En caso de incendio, la instalación de aire acondicionado será rápidamente desactivada, bien manualmente o bien mediante la instalación de detección automática, las compuertas cerrarán automáticamente cuando la instalación automática de extinción entre en funcionamiento.

Los filtros de aire serán incombustibles y estará equipado con un sistema que detecte posibles embozamientos.

Cerca de cada puerta de acceso al local de ordenadores, se instalará un interruptor de puesta en marcha y parada del sistema de aire condicionado.

3.3 Protección estructural de salas de C.P.D.

- **Medidas de protección en función del tipo de edificio**

Tipos de edificios en los que se instala el C.P.D.		Medidas básicas
A	Sólido, construcción resistente al fuego (edificios nuevos y antiguos)	• Protección estructural contra el fuego: el área de procesos de datos debe formar un compartimento aislado. • Sistema de detección de incendios en el área de procesos de datos.
B	Edificios de estructura mixta. Resistencia al fuego variable (sólo edificios antiguos)	• Protección estructural contra el fuego: el área de procesos de datos debe formar un compartimento aislado, de lo contrario ver edificio tipo C.
C	Edificios con estructura no resistente al fuego (sólo edificios antiguos)	• Protección estructural contra el fuego: el área de procesos de datos protegida al menos con una pared aislante. • Sistema de detección de incendio (protección completa)

- **Revestimientos, falsos techos y falsos suelos**

Un incendio puede proceder del exterior, producido en un local o edificio limítrofe, o del interior. Lo que se tratará es de conseguir que si el fuego procede del exterior no penetre y si es de dentro no se propague. Por ello es conveniente tener en cuenta:

- Los suelos, paredes y techo se construirán con material resistente al fuego.

  Según el tipo de ordenadores, será necesaria o no la instalación de falsos techos y suelos. Para los suelos se utilizará madera laminada y para el techo material no

combustible. Deberán tener resistencia al fuego de al menos una hora.

- La puerta del C.P.D. debe abrirse de dentro hacia afuera para que en caso de incendio la presión de las personas sobre las barras antipánico de las puertas haga que las abra. Debe de tener una resistencia al fuego entre 60 y 90 minutos.

- Las aberturas para cables deben estar cerradas herméticamente con un material resistente al fuego.

4. COPIAS DE SEGURIDAD

Es uno de los puntos fundamentales a tener en cuenta en cualquier C.P.D.

Las copias de seguridad son un elemento básico para recuperar aplicaciones y asegurar el funcionamiento del trabajo en cualquier C.P.D.

Existen muchos soportes para la realización de estas copias, actualmente en el mercado pueden encontrarse:

- Casetes digitales
- Cintas de audio digital.
- Cintas magnéticas de cartucho.
- Cartuchos de cinta de 8 mm.
- Cintas de nueve pistas.
- Tocadiscos de cintas.
- Discos ópticos.
- Worm.

Para la seguridad física de los soportes, se tendrá en cuenta su naturaleza, fácilmente alterable por campos magnéticos, humedad, etc., y por su tamaño, que los hace fácilmente hurtables y transportables, y por su estandarización, que los hace utilizables en equipos que no sean los del C.P.D.

Almacenamiento de copias de seguridad

- **Archivos de explotación**

  Normalmente se utilizarán en ellos las copias de seguridad, conteniendo datos útiles cuya creación sea factible con pocos inconvenientes.

  Los soportes que contengan los datos se deberán archivar en armarios o estanterías ignífugas o elementos refractarios al fuego y apropiados para soportes informáticos. Su ubicación será el interior del C.P.D., en salas de archivo, siendo su protección determinada por el Plan de Seguridad y acceso a estas zonas.

- **Archivos externos**

  El lugar de almacenaje externo deberá estar los suficientemente alejado del C. P.D., por ejemplo, desde el punto de vista de incendio mediante una compartimentación especial, en diferentes alas del edificio o en dos edificios. En numerosas empresas se utilizan como lugares externos las bóvedas acorazadas de bancos o empresas especializadas en el archivo de datos informáticos.

  Para que la protección sea idónea, deberá existir un control de accesos a los datos archivados y existir lugares de almacenamiento, armarios, etc., que ofrezcan una protección adecuada a los riesgos posibles

que puedan amenazar la información depositada, puertas blindadas, cámaras ignífugas y acorazadas.

- **Archivos de seguridad**

  En ellos se guardarán:

  - Datos vitales que no se podrían recuperar y que resulten imprescindibles. Se archivarán en cámaras cerradas, los originales, o si su actualización es superior a seis días.
  - En cámaras abiertas si son copias o su actualización es inferior a seis días. Asimismo, se pueden archivar en ellos datos importantes cuya creación es posible pero costosa.

  Es imprescindible contar con copias en el exterior, convenientemente protegidas, y de un C.P.D. alternativo que permita poder continuar con el proceso en caso de emergencia.

  Para dar mayor seguridad a los archivos, es conveniente tener en cuenta una serie de puntos:

  - Los inventarios de los soportes ubicados en los archivos se deben realizar diariamente.
  - Se fijarán personas y responsabilidades para realizar los traslados de material de archivo, llevando constancia documental de los movimientos de material y de las personas que los ha realizado.
  - Se confeccionará un índice de materias clasificadas y de sus lugares de archivo, que deberán ser situados en lugares distintos de la zona de archivos y sujetos a protección especial.

5. PROTECCIÓN DE ACTIVOS INFORMÁTICOS

Es aconsejable que la posibilidad acceso/no acceso esté centralizado en el Centro de Señalización y Control, por medio de un ordenador tipo PC o mediante la existencia de Sistemas Automáticos de Control en la misma ubicación, que llevará un control del número de tarjetas leídas, identificación de las mismas, hora y zona de acceso o salida y ejecute la respuesta en función de dichos parámetros.

La composición esquemática de un sistema de control de accesos de personas sería:

- **Acceso permitido/denegado por posesión de objetos**

  Se pueden realizar las siguientes divisiones:

  - Por posesión de llaves
  - Por posesión de tarjetas, que pueden ser:
    - magnéticas
    - ópticas infrarrojas
    - Wiegand
    - holográficas
    - de semiconductores
    - con memoria de lectura láser
  - Por emisiones, con emisores:

- infrarrojos
- electromagnéticos
- ultrasónicos

Las ventajas de estos elementos son:

- Tiempo de respuesta reducido, 0/10 seg.
- Precio medio
- Buen índice de seguridad

Inconvenientes:

- Pérdida posible del objeto (tarjeta)
- Duplicación, en algunos casos, del objeto

- **Acceso permitido/denegado por conocimiento de datos**

  - Códigos
  - Teclados
  - Cerraduras de combinación

  Ventajas:

  - Tiempo de respuesta reducido, 0/10 seg.
  - Precio medio
  - Buen índice de seguridad
  - Posibilidad de claves anti-rehén

  Inconvenientes:

  - Posibilidad de traspaso de la información, voluntaria o involuntaria a otras personas

- **Acceso permitido/denegado por propiedades físicas personales**

  - Antropométricos

    - Huellas digitales
    - Firmas
    - Voz
    - Iris del ojo

  - Ventajas:

    - Alto índice de seguridad

  - Inconvenientes:

    - Altos tiempos de respuesta, 15/30 seg.
    - Posibilidad de cambios en las características antropométricas
    - Precio elevado

- **Acceso permitido/denegado por combinación de sistemas**

  Una posibilidad importante es la combinación entre los sistemas anteriormente citados tarjetas, llaves, identificación antropométrica, etc., todas ellas con la salvaguarda de un código.

  Ventajas:

  - Aumento del nivel de seguridad
  - Aumento de la dificultad de falsificación

  Inconvenientes:

  - Precios de los componentes sumados
  - Tiempos de respuesta de los componentes sumados
  - Se dificulta el proceso productivo

Protección del software

En un sistema automatizado, los controles podrán variar según el tipo de aplicación, complejidad o impacto en las condiciones financieras y/o operativas de la Organización.

Toda organización deberá tener en cuenta la prevención, detección, corrección y rentabilidad de las medidas de seguridad tomadas. En ocasiones el coste económico de las medidas de protección tomadas es muy superior al umbral de riesgos existentes para el sistema, es decir, las medidas de seguridad tomadas no son idóneas ni rentables.

Los controles preventivos ayudarán a evitar errores y transacciones no autorizadas, tanto por parte de usuarios del sistema como de personas ajenas a éste.

Entre dichos controles se incluyen:

- el diseño de pantalla
- dígitos de control
- contraseñas, *passwords*

En cuanto a virus, como medidas de seguridad preventivas frente a los mismos sin necesidad de recurrir a un *software* ni *hardware* adicional, se pueden tomar las siguientes medidas:

- Realización de copias de seguridad, que permitan restablecer y recuperar la información.
- Protección de los disquetes de programas contra escritura, será necesario inicializar el ordenador desde disquetes de sistema limpios y protegidos.
- Alterar los atributos de los archivos ejecutables dejándolos en "sólo lectura", aunque esta protección no sirve frente a virus que actúen utilizando las funciones de las BIOS.

Para llevar a cabo una lucha específica contra los virus se utilizan programas antivirus que pueden actuar desde dos frentes distintos, bien utilizando programas correctores, que actúen cuando el virus está extendido por el sistema, tratando de paliar los efectos del mismo, y por lo tanto, no es el más aconsejable, o bien utilizando los programas que se encuentran en el mercado y que actúan previniendo la entrada del virus en el sistema.

6. MARCO LEGAL

Cabe destacar como normativa de referencia:

- Ordenanza Primera de Prevención de Incendios.
- Recopilación Normas UNE relacionadas con la seguridad contra incendios en los edificios (AENOR).
- Norma Básica de Edificación (NBE-CPI/96). Ministerio de Obras Públicas.
- Real Decreto 1.942/1993, de 5 de noviembre. Instalaciones de protección contra incendios.

volver arriba