



Protegiendo la TI – NFPA 75

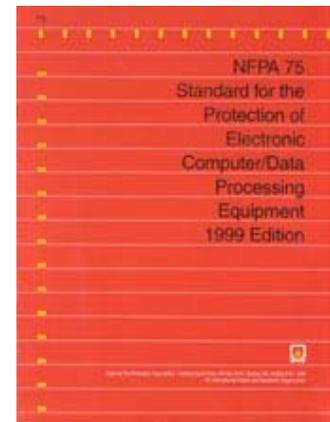
Escrito por Mark Conroy

El corazón de la mayoría de los negocios es la tecnología de la información. La NFPA 75 proporciona orientación para la protección contra incendios y la continuidad del negocio

El 11 de agosto de 1999, se produjo un incendio en el Centro de Control de United Airlines en Elk Grove, Illinois, que podría haber paralizado abruptamente las operaciones de la empresa deteniendo 24.000 vuelos que transportaban 300.000 personas. El impacto financiero en United podría haber sido tremendo.

Afortunadamente, la aerolínea había tenido la prudencia de desarrollar un plan de continuidad del negocio que incluía una instalación redundante. Aunque, en su momento, el desarrollo e implementación de este plan le costó a United millones de dólares, la compañía había comparado oportunamente el costo del plan con el costo de la interrupción del negocio y decidió que la inversión valía la pena.

Al igual que en United, el corazón de la mayoría de los negocios es el centro de tecnología de la información (TI), cuya continuidad operativa es crucial para sostener los procesos del negocio. La disponibilidad ininterrumpida de estos recursos se denomina “continuidad del negocio”.



Debido a que la protección contra incendios es una parte integral de la continuidad del negocio, la NFPA desarrolló la *NFPA 75, Protección de equipos electrónicos procesadores de datos por computadora*, que presenta un enfoque lógico de la protección contra incendios y la continuidad del negocio basado en el riesgo.

Desde el punto de vista del negocio, el factor de riesgo más importante usualmente es el perjuicio económico ocasionado por la pérdida de equipos o registros. Aquí es donde muchos gerentes de negocios centran su atención.

En lugar de comenzar por el devastador punto final de la interrupción del negocio, mitigación, control de daños, recuperación del desastre, y reanudación del negocio; comencemos por el principio. Asumamos que existen factores de riesgo que lo han llevado a utilizar la NFPA 75 y veamos qué tiene esta norma para usted.

Prevención de incendios

El enfoque lógico es en primer lugar prevenir incendios, lo que simplemente implica eliminar todas las fuentes de ignición y reducir la cantidad de materiales combustibles en la sala. En el improbable caso de que un incendio se propague desde otra área a una sala de TI, minimizar los combustibles tanto de papel como electrónicos, le dará al incendio menos materiales de los cuales alimentarse.

El área por debajo de pisos elevados puede ser la pesadilla de las tareas domésticas. No sólo se acumula la basura y otros combustibles debajo de él, sino que también a veces allí se almacenan cosas. Una inspección periódica del área, conducida por alguien cuya prioridad sea la protección contra incendios, puede eliminar muchos innecesarios combustibles potenciales.

Las áreas de subsuelo también suelen contener cables. Los que no estén actualmente en uso pero que serán utilizados en el futuro deben ser etiquetados e identificados como tales. Todos los otros cables abandonados deberían ser removidos siempre que fuera posible.

Esto es necesario por varias razones. Una gran cantidad de cables no utilizados puede interferir con el flujo de aire destinado a mantener la temperatura de la computadora dentro del margen de funcionamiento. En el caso de un incendio, el aislamiento del cable puede generar humo corrosivo. Y si existe una gran cantidad de cables enmarañados, el incendio podría llegar a estar arraigado en lo profundo, haciéndolo más desafiante para combatir que un incendio de superficie. Los cables excedentes pueden también obstruir los patrones de descarga de los sistemas de extinción de incendios.

Cuando se remueven los cables, cualquier infiltración debe ser prevenida con un 'cortafuegos' a través de construcciones de clasificación ignífuga. Dado que remover cables abandonados puede dañar otros cables, su remoción debe ser planeada cuidadosamente.

Barreras contra incendios

Dado que la historia nos dice que la mayoría de los incendios comienzan fuera del área de la TI, se colocan barreras en forma de construcción con clasificación ignífuga de una hora de resistencia para impedir que las llamas se propaguen a tales áreas.

Básicamente, la sala del equipo de TI está rodeada por una construcción de clasificación ignífuga de una hora de resistencia, y cualquier filtración a través de estas paredes de clasificación ignífuga debe ser rellenada con materiales cortafuegos. Las salas que rodean la sala del equipo de TI, que contienen equipos de ventilación, almacenamiento de medios de cinta, y oficinas de soporte, con frecuencia son importantes para la actividad de TI, entonces ellos, también, deberían tener una mínima construcción de clasificación ignífuga de una hora de resistencia todo alrededor. Se recomienda la construcción con clasificación de dos horas.

Las salas mecánicas y eléctricas, que con frecuencia son extremadamente importantes para la operación continuada de la sala de informática, también deberían tener una construcción de clasificación ignífuga de una hora de resistencia. Además, los conductos de ventilación deben estar equipados con reguladores de tiro activados mediante detectores de humo. Cualquier conducto que preste servicio a otras partes del edificio o que pase a través del área de TI debe tener reguladores de tiro de humo e incendio automáticos.

Sistemas de protección contra incendios

Es interesante observar la lógica de los sistemas de protección contra incendios para los espacios de TI. Regla número uno: si el edificio está completamente protegido por rociadores, el área de TI también debe tener un sistema de rociadores automáticos. ¿Por qué? Si el área instalada sin rociadores resultara ser el punto del origen del incendio, el mismo podría terminar devastando el sistema de rociadores del edificio.

Con frecuencia, se le teme al agua en los espacios de TI. Sin embargo, este temor usualmente es infundado.

Digamos que un incendio en la esquina de una sala de IT produjo suficiente calor para activar un rociador. Dado que el calor se localizó y el agua comenzó inmediatamente a enfriar el área del incendio, sólo uno o dos rociadores deberían activarse y descargar agua. Usted realmente querrá que el agua controle o extinga el incendio para evitar que se ocasionen daños más de la pequeña área de origen del incendio.

Otro temor es que la tubería del rociador pueda gotear. Normalmente, las tuberías de los rociadores no comienzan de repente a gotear a menos que estén físicamente dañadas, como podría ser en un depósito. La posibilidad de daño de impacto a la tubería de los rociadores en una sala de informática es remota.

Si el espacio para TI está en un edificio que no requiere sistema de rociadores, la elección es o bien suministrar un sistema de rociadores automáticos para el área de TI o bien instalar un sistema extintor de agente limpio. En aplicaciones que no pueden permitirse ninguna interrupción del negocio, incluso pueden instalarse ambos tipos de sistemas. El sistema de agente gaseoso estaría diseñado para activarse primero, y el sistema de rociadores actuaría como segunda alternativa si el sistema de agente limpio fallara. El sistema de agente gaseoso usualmente no falla a menos que esté deficientemente instalado o que las puertas fueran mantenidas abiertas por empleados desinformados, pero tales cosas suceden, así que sería bueno tener el sistema de rociadores allí.

El área por debajo del piso elevado puede estar protegida por un sistema de rociadores, un sistema de dióxido de carbono, o un sistema de agente inerte. Si se emplea un sistema de agente inerte sobre el piso elevado, entonces la cobertura se extendería al área del subsuelo. Si el área por encima del piso tiene un sistema de rociadores, tendría sentido instalar un sistema de rociadores también en el subsuelo. Sin embargo, la distancia desde la losa hasta la parte inferior del piso puede no ser lo suficientemente alta para lograr el patrón de distribución necesario desde la descarga del rociador. Si este es el caso, se puede instalar en su lugar un sistema de agente gaseoso.

Si se selecciona un sistema de dióxido de carbono, se debería utilizar un sistema especial de descarga de baja velocidad de modo que el dióxido de carbono no se eleve por encima de la altura de la rodilla en la sala. Este tipo de sistema es bien conocido en la industria y debería ser el único tipo de sistema de dióxido de carbono instalado en esta aplicación.

Los sistemas de agente de hidrocarburo halogenado de subsuelo no se permiten cuando el espacio encima del piso elevado no está equipado también con sistema de agente de hidrocarburo halogenado. Un incendio en el espacio ubicado por encima del piso elevado podría

mover hacia arriba el agente de hidrocarburo halogenado descargado, causando que se descomponga y se vuelva muy tóxico.

Registros

Los registros siempre son un punto de discusión cuando se refiere a las áreas de TI. Aquí hay unas pocas reglas básicas.

Los registros en la sala de TI se deben mantener en el mínimo absoluto y deberían ser sólo aquellos necesarios para la operación esencial. Todos los registros importantes se deben duplicar y almacenar en una ubicación remota de modo de no estar expuestos al mismo incendio que los originales.

Los registros se deben almacenar en gabinetes metálicos cerrados. Los sistemas automatizados de almacenamiento de información (AISS por sus siglas en inglés) son permitidos en las salas de TI sólo si un sistema dedicado de rociadores o sistema de agente gaseoso está instalado en cada unidad.

Las salas de bibliotecas de cintas y de almacenamiento de medios deben estar fuera de la sala de TI, estar protegidas con un sistema de extinción de incendios, y tener al menos una construcción de clasificación ignífuga de una hora de resistencia. No debería haber nada más en estas salas, y no se deberían permitir actividades sino aquellas relacionadas al almacenamiento.

Construcción

La construcción de clasificación ignífuga alrededor de la sala de TI y de toda el área de TI debería extenderse desde el piso estructural hasta el piso/cielorraso estructural de arriba. Esto con frecuencia se lo conoce como construcción "losa a losa". Esto sirve a dos propósitos. El primero debería ser obvio: usted no quiere que el humo o las llamas fuera del área se traslade dentro del área de TI.

El segundo entra en juego cuando se emplea un sistema de agente gaseoso. Uno de los componentes más críticos del sistema de inundación total de agente limpio es "el gabinete" que contiene la concentración del agente extintor suficiente tiempo para extinguir el incendio y prevenir la re-ignición. Las paredes de la sala de TI deben ser lo bastante herméticas como para contener la concentración del agente extintor por este período de tiempo. Los instaladores de sistemas extintores de incendios saben bien esto, pero tienen poco o ningún control sobre la construcción de la sala, y el problema de "filtración" no se descubre hasta que la prueba de presurización de la sala es efectuada durante la puesta en servicio del sistema extintor de incendios. Prestar atención a este detalle durante la construcción ayuda a evitar dolores de cabeza y demoras de ocupación más tarde.

Los materiales para la construcción de edificios deben ser cuidadosamente seleccionados con la idea de minimizar la propagación de incendio potencial. La NFPA 75 entra en grandes detalles respecto de los materiales de construcción permitidos desde puertas con clasificación ignífuga hasta los materiales de paredes, piso y cielorrasos interiores. La cubierta del piso elevado debe estar provista de paneles y herramientas de acceso que sean fácilmente accesibles y con ubicaciones claramente señalizadas. Cualquier canal de cables en el suelo debe emparejarse para prevenir la posibilidad de daños en los cables.

Debajo del piso elevado y encima del cielorraso suspendido

Las áreas debajo del piso elevado y encima del cielorraso suspendido que se utilizan para circular el aire son denominadas "espacios de aire", no "plénium", y les permite cumplir con el Artículo 645 del *Código Eléctrico Nacional*. El Artículo 645 brinda excepciones a los requerimientos de conductos metálicos, cubierta metálica o cable con clasificación de cámara, aunque estos por supuesto, serían aceptables, ya que serían considerados mejoras. Se requieren sistemas de detección automática en subsuelos que contengan cables y en el área encima del cielorraso suspendido que se utiliza para la circulación de aire. Los sistemas de detección también deben ser instalados al nivel del cielorraso a lo largo del área de TI completa.

Los procedimientos de recuperación y emergencia

Cada operación de TI debe contar con tres planes: plan de emergencia de incendios, plan de control de daños, y plan de procedimientos de recuperación. El más ignorado de estos planes es, con frecuencia, el plan de procedimientos de recuperación, el cual delinea las tareas que el personal debe emprender, incluyendo transporte y comunicación críticos para la continuidad de las operaciones del negocio.

Al desarrollar un plan de recuperación, el objetivo es regresar la operación del negocio al nivel en que estaba el día antes de la catástrofe. Si su negocio es tomar pedidos por medio de una línea telefónica gratuita y continúa con la entrega de productos, el esfuerzo de recuperación debería estar dirigido hacia el restablecimiento de la operación telefónica y la conexión del personal a los sistemas de procesamiento informático y telefónico, lo cual permitirá que continúen los envíos.

El plan final incluiría una instalación redundante en un sitio remoto que tenga acceso a los datos de las copias de seguridad. Si la operación no es tan crítica o la instalación redundante ha sido considerada poco realista por razones económicas, es imprescindible un buen plan de recuperación en sitio.

Una vez que ha ocurrido un incendio o algún evento catastrófico, el lugar no necesita ser desalojado. Si la instalación incorpora las características de diseño delineadas en la NFPA 75 y tiene planes efectivos de control de daños e incendio, el plan de recuperación es el que hay que implementar.

Daños

Al desarrollar un plan de recuperación, deben producirse discusiones sobre los daños ocasionados por el agua, humo y calor. El daño por el calor es con frecuencia la razón por la que los artículos expuestos son irrecuperables. Los daños por agua y humo usualmente son menos severos, pero con frecuencia son los que más se malinterpretan.

El humo de una sala de informática usualmente contiene cloruro y azufre que corroe el delicado equipo electrónico. Siempre es necesario remover cualquier remanente de estos contaminantes. El humo puede ocasionar pequeños daños inmediatos, pero cuando se los deja desatendidos por un período prolongado, los derivados corrosivos de la combustión actúan con la humedad en el aire para comenzar el proceso de corrosión.

Siguiendo a un incendio extinguido con agua, la preocupación inmediata es el nivel de humedad que el agua ha introducido en el aire, lo que brinda una indicación de la velocidad a la que ocurrirá la corrosión. Los planes deberían enfocarse en remover el equipo de la sala a un área climatizada de humedad controlada donde se lo pueda estabilizar, limpiar con solventes y, de ser necesario, recubrir con un aerosol especial para evitar la corrosión.

Entonces el daño sería analizado con mayor profundidad antes de tomar cualquier decisión sobre la disposición del equipo. Las compañías con frecuencia venden el equipo a un tercero en vez de arriesgarse a tener problemas futuros.

El daño ocasionado por el agua no es inmediato a menos que el equipo estuviera conectado a la electricidad cuando se mojó. En ese caso, son probables los corto circuitos dañinos. Sin embargo, si el equipo conectado no hubiera sido mojado, se podría evitar o minimizar el daño.

Aunque la NFPA 75 delinea métodos para secar equipos, el mejor plan supone un arreglo contractual con una compañía de recuperación profesional y experimentada que rápidamente pueda comenzar a recuperar los medios electrónicos que contengan datos valiosos, para transferirlos a medios nuevos. Cada hora perdida decidiendo sobre un enfoque o experimentando con diferentes métodos es una hora de interrupción del negocio y funciona en contra del objetivo final de la recuperación de datos.

Toda compañía que tenga una instalación TI deberá desarrollar un plan o enfrentar las consecuencias el día del desastre. No hacer nada podría ser la peor alternativa.

Mark Conroy es un Ingeniero Senior de Protección contra Incendios en la NFPA y el enlace de personal del comité técnico de la NFPA 75.