Articulo Original Páginas: 1-5 ISSN
Paradigma Volumen XXII Abril 2021

Seguridad Contra Incendios en Centros de Datos

Ing. José Miguel Ando Alvarez.
SENIOR Carrera de Ingeniería de Sistemas, Escuela Militar de Ingeniería
La Paz, Bolivia
jmiguelando@yahoo.com jandoa@doc.emi.edu.bo

Fire Safety in Data Centers

Resumen- El presente artículo muestra la necesidad técnica de abordar la seguridad por medio de los avances tecnológicos que son motivados a través de las normas internacionales reconocidas que rigen las buenas prácticas en los centros de datos a nivel mundial y que explican la evidente evolución del mercado boliviano. Este artículo está enfocado en investigación sobre infraestructura, así como las demandas del exterior, estado sociedad y empresa. El área de investigación se estructura en la gestión del conocimiento, nuevas tecnologías y la seguridad informática.

Palabras Clave- *NFPA 75, Protección contra incendios, Inundación de Agentes Limpios, Seguridad de la información, Infraestructura, Centro de Datos, National Fire Protection Asociation.*

Abstract- This article shows the technical need to address security through technological advances that are motivated with recognized international standards that govern good practices in data centers worldwide and explain the evident evolution of the Bolivian market on this field. This article is focused on research on infrastructure, as well as the demands from abroad of the university, society and company status. The research area is structured in knowledge management, new technologies and computer security.

Keywords- *NFPA 75, Fire Protection, Clean Agents, Infrastructure, Data Center, National Fire Protection Association*

I. INTRODUCCIÓN

Cuando se habla de confiabilidad y protección de los sistemas de tecnología e información, es normal que las empresas asocien a ello un costo que, sin las destrezas financieras del responsable de este departamento, con el tiempo dicha inversión puede ser fácilmente dejada de lado, más aún cuando las soluciones sugieren montos que implican la renuncia a inversiones requeridas en la operativa diaria de una organización.

Si el contexto de confiabilidad y protección se enfoca en los sistemas de protección contra incendios, el abordaje es aún más lejano, cuando en el medio no se cuenta con especialistas en protección contra incendios y los diseños que se realizan localmente no responden a las exigencias mínimas de normas como la NFPA 10, Norma para extintores portátiles contra Incendios, sin duda la norma más conocida y utilizada en el medio local o normas más sofisticadas como la NFPA 72 Código Nacional de Alarmas y Señalización de Incendios o la norma NFPA NEC 70 Código Eléctrico Nacional, las cuales nos mencionan sobre la protección a través de equipos extintores, sistemas de detección como los detectores de humo o el tipo de cableado eléctrico, aterramiento o equipotencialidad mencionados respectivamente en cada una de las normas anteriores. Las soluciones contra incendio deberían ser consideradas siempre en ambientes clasificados como los centros de datos y su revisión debiera ser obligatoria.

Si bien en Bolivia se observa un cambio positivo en los últimos años, donde los centros de datos para la Industria de la Banca Privada, Instituciones Gubernamentales o Industria de Producción Privada asumió el reto tecnológico y económico de invertir en Centros de Datos y traer consigo grandes desafíos para los profesionales que se avocan a la infraestructura para Información y Tecnología IT, aún se observa que certificaciones y gestión como los que exige la serie de normas ISO 27000 son apenas abordadas o desconocidas por estos responsables.

La nueva normativa que rige el entorno de los centros de datos ha evolucionado en los últimos años con exigencias como las desarrolladas por el Uptime Institute, con la certificación Tier para los niveles de alta confiabilidad en los centros de datos, la ANSI 942 A con exigencias para la infraestructura y diseño en la construcción de un Data Center o la norma NFPA 75, Norma para la Protección Contra Incendios en Equipos de Tecnología de la Información. Todas ellas exigidas, por ejemplo, por instituciones como las compañías de seguro para la suscripción de pólizas de protección de equipos electrónicos.

El presente artículo se avoca en la revisión, análisis y recomendaciones de esta última norma, la norma NFPA 75, para difundir las buenas prácticas contra incendio que son requeridas previa, durante o después de la construcción de un centro de datos, a fin de garantizar

que las grandes inversiones realizadas en el medio local asuman la importancia de una protección contra incendios apropiada y así puedan garantizar una mayor durabilidad, confiabilidad y continuidad para áreas destinadas a la operación de sus equipos dentro de las áreas de tecnología e información. Este artículo también hará críticas a las soluciones adoptadas en el medio local, donde los daños ocasionados por el fuego o por sus efectos asociados como el humo o en el caso de una intervención no adecuada con agentes no diseñados para este fin, la corrosión, el calor y agua pueden ocasionar pérdidas incalculables y de difícil reposición para la reconstrucción al interior de un centro de datos.

II. CONTENIDO

II.1. ORIGEN DE UNA NORMA DEDICADA A LA TECNOLOGÍA E INFORMACIÓN

Cuando uno imagina que la evolución tecnológica en el país tiene un giro creciente desde hace 25 años cuando el ingreso de las computadoras de escritorio inicia una cabalgata en el desplazamiento de los procesos y procedimientos cotidianos, es difícil imaginar, el momento en el cual se habría considerado la importancia de un desarrollo normativo sobre la protección de estos equipos, que sin duda pudiera tratar; de las condiciones eléctricas, de las condiciones ambientales de operación y de la protección contra incendios.

Sin embargo, la evolución de una norma para la protección contra incendios en equipos de la tecnología de la información tiene un origen con un horizonte más lejano y que ha evolucionado a la par de cómo los equipos electrónicos han evolucionado.

Como menciona la norma (NFPA, 2013), el origen de la norma NFPA 75 se da gracias a la conformación del comité sobre Sistemas de Computadores Electrónicos en enero del año 1960. Si bien esta naciente reglamentación se basaba en recomendaciones para la protección contra incendios, fue adoptada ya como una norma NFPA en el año 1962 y en adelante sufriría 8 revisiones hasta el año 1992 donde la norma es reescrita en su totalidad bajo los lineamientos de las otras normas NFPA.

La última versión publicada en español de la norma NFPA 75 responde a la edición del año 2013, aunque las versiones en inglés ya están vigentes con actualizaciones al año 2017 y recientemente impresa la versión 2020. Es importante mencionar que la evolución en el sector exige muchas veces cambios radicales y por ello la NFPA incluso adelantó la revisión y publicación de esta norma, prevista inicialmente para el año 2020, y donde la revisión al segundo borrador fue editado en abril del año 2019. Para la publicación de la NFPA 75 versión 2019 en español se espera pueda ser publicada durante el año 2020 o incluso más adelante.

Este desplazamiento natural del idioma, nos invita a no dejar la competitividad por esta limitante, cuando este sector es indudablemente uno de los más dinámicos. Las normas son, sin embargo, muy diversas e invitan a contrapesar y concebir que la especialización puede darse en diferentes marcos, como lo hace la norma UL 60950 Information Technology Equipment - Safety - Part 1: General Requirements describe los requisitos de Seguridad para equipos de Información y Tecnología, cuyo apartado 2.3. Fuego, hace énfasis en las recomendaciones para la protección contra incendios. Esta norma que aborda de forma integral varios aspectos relacionados al riesgo en un data

center, a diferencia de la norma NFPA 75, hace su aparición recién en el año 2006. Otra norma relacionada a los riesgos con un enfoque a la seguridad de la información es la ISO/IEC 27005 Information security risk management, cuya valoración no es objeto del presente artículo.

La exigencia de estas como otras normas especializadas en la seguridad de la información en general y normas contra incendio en particular, hacen que hoy en día la gestión de riesgos en centros de datos signifique uno de los ítems de mayor inversión en Hospitales, Industria, Banca, Universidad, entre otros sectores.

II.2. LOS RIESGOS EN TELECOMUNICACIONES

Los riesgos en telecomunicaciones forman parte de un continuo complejo de elementos, que comprende desde aspectos generales y triviales, combinados continuamente con riesgos complejos y especializados para el rubro.

El primer elemento de los riesgos es el que mayor daño combinado puede generar en los sistemas y aspecto central del presente artículo, el riesgo de incendios. Indudablemente, el fuego en una sala de datos se comporta como el elemento más dañino, si el fuego ocurre, es posible perder los datos y la comunicación, que son en el interior del centro de datos lo más importante.

II.2.1. Riesgos de incendios

Son siete los factores que deben ser considerados para determinar un nivel adecuado de riesgo

a) Aspectos de la seguridad humana. Es indudable que la seguridad humana es el factor más sensible a ser protegido en un centro de datos o sus alrededores. La protección humana debe garantizar que más allá de la pérdida de información, la vida de quienes están cerca o ingresan para salvaguardar una sala de datos, está siempre en primer lugar

b) Tratamiento al fuego expuesto. El confinamiento es el elemento más importante en el tratamiento al fuego, su aparición ya marca una elevada ausencia

de control, pero si el fuego existe el daño es catastrófico, su contención y confinamiento, sectorización serán entonces lo más importante.

c) Pérdida económica por pérdida de función o pérdida de los archivos. La continuidad de las empresas hoy en día puede depender exclusivamente de la información, los datos y su comunicación, si esto falla, una empresa con miles de empleados puede quedarse periodos largos sin alcanzar beneficios, ingresos, o su producción planificada. La continuidad de las empresas hoy depende de la eficacia con la cual se aborde la continuidad de un negocio desde el enfoque de un centro de datos robusto.

d) Pérdida económica por el valor en los equipos. Los equipos en un centro de datos pueden alcanzar valores exorbitantes, donde su inversión puede perderse en tan solo un par de segundos. Los costos de información por pérdida de un equipo pueden ser incalculables para una empresa y hacer que esta pierda su continuidad en el mercado.

e) Impacto regulatorio. La regulación debe estar a la par de los requisitos en centros de datos. Afortunadamente para el país aún no se tienen políticas claras sobre el control y desempeño de estos, Esta ausencia de condición hace que muchos de ellos se construyan bajo estándares internacionales, alcanzando importantes desempeños que superarían con creces primeros intentos normativos locales.

f) Impacto reputacional. La información y su contenido forman parte hoy en día de uno de los insumos más importantes de cualquier empresa. La pérdida de datos o su manejo irresponsable indudablemente podrían generar la pérdida reputacional de una empresa, incluso llevándola a la quiebra. Un centro de datos es el corazón operativo del manejo, custodia y salvaguarda de esta información. Un diseño débil permitiría la intrusión y posterior robo, pérdida o manejo inapropiado de este invalorable recurso.

g) Redundancia de los sistemas Off site. Las pérdidas son previsibles, sin embargo, una esencia de la continuidad se estructura con buenos manejos del sistema Off Site. El principio de redundancia en equipos, desde los equipos de ventilación hasta servidores, debe ser la premisa en el manejo de un centro de datos.

Los riesgos asociados al análisis de incendios pueden dividirse en los siguientes:

- Factores de Control. Los factores de control se estructuran en los medios que permitirán obtener información fidedigna y continua sobre cualquier evento.

- Factores de Reacción. Los elementos de reacción son imprescindibles para contener cualquier contingencia presente en un centro de datos, esto debe ser acompañado por un plan de contingencia, cuyos atributos definirán estrategias para la reacción del personal.

- Factores de Confinamiento. Los sistemas de protección contra incendios deben ser los más importantes medios de confinamiento para la protección integral de los equipos. Un sistema de inundación por agentes limpios debe permitir el sofocamiento del fuego, así como la refrigeración y detener posibles propagaciones de humo

- Factores de Recuperación. La recuperación de un centro de datos puede valerse en tan solo unos segundos, el mal uso de un sistema contra incendios, pueden dejar sin operación y dañado severamente a un centro de datos. Falsas alarmas entre otros son recurrentes en la ausencia de operación de un sistema, por otro lado, la falla en sensores generará agudeza en los daños generados al sistema.

II.3. LOS CENTROS DE DATOS EN BOLIVIA

Los centros de datos en Bolivia, han sufrido un crecimiento positivo en la última década, posterior a una evaluación continua en centros de datos de distintas instituciones vemos 2 características relevantes:

1. Inversión en protección contra incendios.
2. Inversión en infraestructura

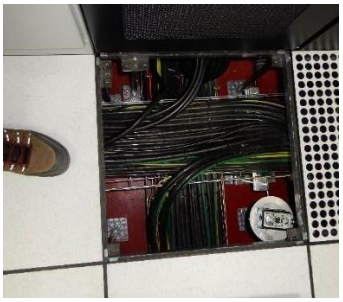

Figura 1. *Fotografía de un piso técnico, se observa el cableado estructurado y sensórica.*

La necesidad de migrar a sistemas de comunicación sofisticados a fin de brindar productos al menos al nivel que se ofrece ya en otros países de Latinoamérica, permitirá sin dudas brindar a los clientes en Bolivia, soluciones sofisticadas y de vanguardia.
Los centros de datos sin embargo no tienen en nuestro país las directrices correctas, muchos de ellos son construidos de forma improvisada, otros cuentan con con cableados combinados de baja categoría, otros presentan una severa saturación en el cableado, bajos criterios eléctricos que genera campos magnéticos y puede reducir la vida útil de los equipos.

II.4. LOS EQUIPOS DE DETECCIÓN Y PROTECCIÓN CONTRA INCENDIOS EN CENTROS DE DATOS

La sensibilidad en los equipos dentro un centro de datos puede ser afectado severamente por la presencia del fuego, incluso si el fuego no logra afectar físicamente a un equipo, este puede afectar y dañar definitivamente el sistema en operación.
La probabilidad de presencia de fuego en un centro de datos es alta, donde se tienen sistemas robustos de energía, combinando desde equipos a 12V. equipos monofásicos a 110V o 220V y trifásicos que normalmente se sitúan a 220 V. o 380 V dependiendo principalmente las características de los motores de refrigeración.
Otro efecto del fuego es el humo, donde la presencia de humo dentro de un centro de datos puede ocasionar la pérdida total de operatividad de un sistema electrónico.
Según informa la NFPA, los componentes de un centro de datos pueden verse afectados por las altas temperaturas, vapor y productos de combustión provenientes de un incendio. Aunque existen una gran variedad de equipos y diferencias en sus puntos de falla, pruebas de laboratorio han demostrado que: a temperaturas superiores a 49°C pueden comenzar daños permanentes; cintas magnéticas pueden perder información a temperaturas superiores a 52°C; discos duros se dañan cuando existen temperaturas sostenidas de 66°C; componentes de los equipos empiezan a fallar a una temperatura de 79°C, con fallas en equipos principales entre 149°C y 200°C; microfilm se empieza a dañar a 107°C cuando existe alta humedad; inclusive papel se puede dañar a temperaturas alrededor de 177°C.
Las soluciones contra incendio en un centro de datos se estructuran en la percepción correcta de los riesgos:

I. Riesgos propios del sistema (riesgos internos)

II. Riesgos externos del sistema

Figura 2. *Fotografía de comunicación de cables, se observa ausencia de parche ignífugo. La comunicación de fuego entre salas es posible*

Una continua evaluación de riesgos, así como auditorías al desempeño de un sistema brindan las garantías para la supervivencia de los sistemas, establecer protocolos claros y comprensibles por el personal a cargo y desarrollar medios de comunicación que permitirán alcanzar el tiempo de vida útil o incluso superarlo haciendo y adecuando las buenas prácticas en el día a día.
Bolivia, está evidentemente retrasada en la implementación de centros de datos sofisticados y de primera línea, pero el aprendizaje de países vecinos, industrias vecinas y seguir las líneas marcadas por los países que establecen la tendencia y vanguardia en centros de datos, debe permitirnos desarrollar en breve las directrices para que toda institución valore de forma positiva la implementación e inversión en un centro de datos que seguramente generará un retorno elevado a la institución por su inversión.

III. RESULTADOS

La visita a centros de datos gracias a La Boliviana Ciacruz de Seguros y Reaseguros S.A. para la evaluación de riesgos, permite evaluar los siguientes parámetros.

1. Las empresas han empezado a invertir parcialmente en centros de datos.
2. Las inversiones no se acompañan con soluciones en infraestructura.
3. El costo de un centro de datos es elevado, sin embargo, inversión parcial o por etapas debe contemplar un análisis serio y continuo de los riesgos asociados.

4. Las empresas que decidan crecer con perspectiva deben invertir en centros de datos, que cumplan con las directrices normativas y exceder sus requisitos.

5. La tecnología avanza rápidamente, donde inversiones sin perspectiva futura pueden quedar obsoletas

IV. CONCLUSIONES

Como resultado del presente artículo, que evalúa la seguridad contra incendios en centros de datos en Bolivia, se tienen presente las siguientes conclusiones:

- ✓ El conocimiento normativo sobre la gestión de centros de datos es bajo y no permite evaluar los parámetros mínimos en las directrices normativas.
- ✓ La gestión de riesgos está normalmente por debajo de los parámetros normativos mínimos.
- ✓ Se desconoce normas de referencia como la ISO 27005, NFPA 75 u otras asociadas a TIER
- ✓ Existe una elevada exposición institucional en las empresas a perder comunicación y datos, lo que permite apreciar un amplio campo de inversión y avance en términos tecnológicos.
- ✓ La ausencia de técnicos, tecnólogos, ingenieros de sistemas, ingenieros de infraestructura y ramas especializadas, hace que la industria genere un amplio campo de crecimiento laboral.
- ✓ Los centros de datos, son inversiones estratégicas, para las empresas que decidan crecer con un elevado grado de competitividad.
- ✓ Un asesoramiento continuo y evaluación en riesgos es un requisito para mantener altas expectativas de crecimiento y dar continuidad a las inversiones en centros de datos.

Referencias

[1]. Alger, D. (2012). The Art of Data Center. Massachusetts: Pearson Education.
[2]. Bradley, L. C. (1994). Handbook of Data Center Management. 6000 Broken Sound Parkway NW, Suite 3000: CRC Press.
[3]. Donahoe, D., Zhao, K., Murray, S., & Ray, R. (2000). Accelerated Life Testing.
[4]. Geng, H. (2015). Data Center Handbook. New ersey: Wiley.
[5]. NFPA, N. F. P. A. (29 de julio de 2013). NFPA 75. Standard for the Fire Protection of Information Technology Equipment. Batterymarch Park, Quincy, MA, Estados Unidos: NFPA.
[6]. TIA-942-A, A. /. (2012). Telecommunications Infrastructure Standard for Data Centers. Arlington: TELECOMMUNICATIONS INDUSTRY ASSOCIATION.

Fecha de Envió del Articulo: 7/10/2020
Fecha de Aceptación de artículo: 20/10/2020