RECOMENDACIÓN DE NORMA TÉCNICA "REQUISITOS BÁSICOS PARA LA IMPLEMENTACIÓN Y/O ADECUACIÓN DE CENTROS DE PROCESAMIENTO DE DATOS"

PRÓLOGO

Esta Recomendación de Norma Técnica asociada al tema de los Requisitos Básicos para la Implementación y/o Adecuación de Centros de Procesamiento de Datos, establece las especificaciones técnicas que podrán considerarse para mantener el correcto funcionamiento de estos espacios, garantizando el resguardo de la información, con la finalidad de impulsar la Gestión Gubernamental enmarcada en un modelo eficiente, de calidad y sustentable.

La finalidad de abordar este tema en la presente Recomendación de Norma Técnica es promover la adecuación de los Centros de Procesamiento de Datos de los Órganos y Entes de la Administración Pública, consiguiendo la infraestructura idónea para el manejo, almacenamiento y administración óptima de volúmenes de datos.

1 OBJETO Y CAMPO DE APLICACIÓN

1.1 Generalidades

Esta Recomendación de Norma Técnica establece los lineamientos básicos necesarios para el diseño, instalación y/o adecuación de los Centros de Procesamiento Datos de cualquier Órgano o Ente de la Administración Pública de la República Bolivariana de Venezuela, todo esto enmarcado por lo establecido en el Decreto N° 3.390 publicado en la Gaceta Oficial N° 38.095 de fecha 28 de diciembre de 2004.

1.2 Aplicación

Los elementos descritos en esta Recomendación de Norma Técnica deberían ser aplicados por todos los Órganos y Entes de la Administración Pública, a los fines de mantener una estructura uniforme en los Centros de Procesamiento de Datos, que permita disponer de ambientes seguros y confiables para el resguardo de la información.

2 RECOMENDACIONES

2.1 Requisitos Fundamentales

Con el propósito de asegurar la implementación y/o

adecuación integral de los Centros de Procesamiento de Datos de cualquier Órgano y Ente de la Administración Pública podrá considerar los siguientes requisitos: seguridad, disponibilidad, escalabilidad, acceso y administración.

En este sentido se establecen los siguientes parámetros:

2.2 Consideraciones de Infraestructura, Refrigeración, Control de Temperatura y Humedad.

2.2.1. Acceso redundante al edificio por vías separadas, en lo posible con un espacio exclusivo para el centro de datos, con distribución adecuada entre columnas que optimicen la dimensión disponible para equipos.

2.2.2 Verificar que los materiales de construcción del sitio sean incombustibles y que las paredes perimetrales sean de concreto o ladrillo de manera que provean la mayor seguridad.

2.2.3 Verificar el cumplimiento del código internacional de construcción V-N para corroborar su adecuación e idoneidad en relación a su infraestructura física, sistemas de incendio, separación de espacio, características de disponibilidad y funcionalidad.

2.2.4 Se recomienda evitar que el edificio o lugar de ubicación del Centro de Procesamiento de Datos, tengan otros inquilinos que se dediquen a actividades industriales.

2.2.5 Considerar una altura de hasta cuatro metros para albergar la totalidad de la instalación del Centro de Procesamiento de Datos.

2.2.6 Existencia de un sitio (muelle) destinado para la descarga de equipos.

2.2.7 Es conveniente que la ubicación del Centro de Procesamiento de Datos se encuentre a una distancia considerable de fuentes de radiaciones electromagnéticas y de radiofrecuencia.

2.2.8 La ubicación del Centro de Procesamiento de Datos debería estar por encima de los niveles de agua. No es recomendable instalar sistemas críticos en los sótanos; ni tampoco ubicar la sala de alojamiento por debajo de salas con tuberías de agua.

2.2.9 La sala debería estar diseñada en torno a un sistema de suelo técnico por el que pueda llevarse todo el cableado necesario, según lo estipulado en la norma TIA-942 vigente.

2.2.10 El suelo técnico no deberá tener ningún elemento susceptible de acumular electricidad estática y debe estar conectado a una toma de tierra en el caso de ser metálico.

2.2.11 Se recomienda que el acceso a la sala esté limitado a una sola puerta, la cual debería permanecer cerrada y controlada con las medidas de acceso físico establecidas por el Órgano o Ente.

2.2.12 Las salas del Centro de Procesamiento de Datos deberían contar con sistemas de aire acondicionado de precisión y su capacidad debe ser acorde con el tamaño y la cantidad de equipos, que mantengan una temperatura constante entre 18° y 23° centígrados. Además es conveniente que los equipos de aire acondicionado cuenten con la suficiente potencia de ventilación para disipar todo el calor acumulado en los racks.

2.2.13 Los equipos de aire acondicionado deberían estar de manera redundante, para que en la medida que falle alguno de los equipos, el resto puedan mantener la temperatura y grado de ventilación dentro de los límites.

2.2.14 Los equipos de aire acondicionado deberán encontrarse ubicados en los laterales de

la sala, y tener su salida de aire por la parte inferior, inyectando todo el aire frío bajo el suelo técnico.

2.2.15 Cada gabinete con equipos deberá tener el suelo hueco, y contar con una rejilla en el suelo técnico que permita la salida del aire frío. Esta rejilla debe tener la dimensión adecuada para permitir el paso del flujo de aire necesario en función de la carga del gabinete.

2.2.16 La sala deberá contar con sistemas de control de humedad e interactuar con los equipos de aire acondicionado para mantener la humedad de forma constante a unos niveles entre el 40-55%.

2.2.17 La sala debería contar con detectores de agua/inundación bajo el suelo técnico para detectar posibles averías de los equipos de aire acondicionado (o filtraciones del exterior) que pudieran causar grandes desastres.

2.3 Consideraciones Eléctricas

2.3.1 El suministro eléctrico proporcionado a los racks debería ser estable y filtrado de picos/caídas de tensión.

2.3.2 Se recomienda que exista al menos 2 circuitos eléctricos independientes por cada rack. El

fallo en uno de los circuitos no debería afectar al suministro proporcionado por el segundo circuito, ni al resto de los racks.

2.3.3 Cada circuito eléctrico debería estar trabajando siempre por debajo del 40 % de su capacidad. En caso de fallo de uno de los circuitos, el resto debería tener la capacidad de absorber el 100% de la carga.

2.3.4 Es conveniente verificar la capacidad de las acometidas eléctricas al edificio, disponibilidad de más de un proveedor (sub-estación eléctrica) y que el edificio disponga de acometidas eléctricas subterráneas.

2.3.5 Cada equipo debería contar con doble fuente de alimentación, conectada cada fuente de alimentación a uno de los circuitos, de forma que el fallo de una de ellas no provoque la caída del equipo.

2.3.6 Ambas líneas de alimentación deberían poseer sistemas de estabilización de corriente.

2.3.7 Es conveniente que al menos una de las líneas este respaldada por equipos de alimentación ininterrumpida.

2.3.8 Todo el suministro eléctrico debería estar a su vez respaldado por generadores eléctricos diésel.

2.3.9 Se recomienda verificar que el sistema de UPS donde se conectarán los equipos cuente con la capacidad suficiente para soportar la carga, contando con redundancia en todos los casos.

2.3.10 Es necesario contar con un sistema de puesta a tierra adecuado a las necesidades de la infraestructura a implementar.

2.3.11 Todo el cableado eléctrico debería discurrir de forma separada del resto de cableado de comunicaciones (red, telefonía, entre otros) bajo el suelo técnico.

2.3.12 Para los equipos que lo permitan, se debería contar con aplicaciones de apagado del servidor para el caso de que los sistemas de UPS indiquen que están a punto de agotar sus baterías

2.4 Consideraciones de Telecomunicaciones

2.4.1 Se recomienda disponer de al menos dos cuartos de entrada de fibra óptica u otro medio de trasmisión que sigan caminos diferentes. Estas acometidas deberían terminar en ubicaciones físicas distintas de los proveedores.

2.4.2 Diversos proveedores de servicios de telecomunicaciones tienen que ofrecer servicios en las

instalaciones (si es un solo proveedor, debería ofrecer distintos tipos de servicio, de preferencia simétricos).

2.4.3 El equipamiento de telecomunicaciones debería estar instalado en el área del Centro de Procesamiento de Datos y no en áreas compartidas del edificio.

2.4.4 El cableado debería estar adecuadamente canalizado, de acuerdo con las normas y estándares 568-A, 568-B, 569, 570, 606 y 607, en sus versiones vigentes, dispuestas por el Instituto Nacional Americano de Estándares en conjunto con la Asociación Industrial de Telecomunicaciones y la Alianza de la Industria Electrónica. Deberá estar dedicado a Telecomunicaciones y Servicios, no siendo accesible a terceros.

2.5 Consideraciones de Seguridad Física

2.5.1 La sala debería disponer de accesibilidad 24 por 7 por 365, asegurándose el monitoreo de accesos, estacionamiento y muelle de descarga, resto de zonas comunes.

2.5.2 El edificio no debería estar ubicado en una zona con riesgo medio de inundaciones o superior (es decir, frecuencia inferior a 100 años y altura no menor a 0,8 m), en áreas con riesgos sísmicos, u otro tipo de catástrofes.

2.5.3 Es conveniente que el Centro de Procesamiento de Datos no esté ubicado en edificios que puedan resultar afectados por edificios colindantes durante un terremoto o inundación.

2.5.4 El edificio no podrá ubicarse en los pasillos aéreos de aeropuertos y como mínimo 0,4 Kms. de aeropuertos, ríos, la costa o presas con reservas de agua, a menos de 0,8 Kms. de autopistas,distanciado a 0,8 Kms. como mínimo de bases militares y con separación no inferior de 1,6 Kms. polvorines y fábricas de armamento.

2.5.5 Se recomienda que el edificio o lugar de ubicación del Centro de Procesamiento de Datos no se encuentre adyacente a una embajada extranjera.

2.5.6 Se recomienda dejarse por escrito la proximidad del Centro de Procesamiento de Datos a estaciones de policía, bomberos y hospitales.

2.6 Consideraciones sobre Control de Detección y Extinción de Incendios.

2.6.1 Las salas del Centro de Procesamiento de Datos deberían contar con detectores de incendio y con un sistema de extinción de incendios, que no dañe los equipos en caso de activación.

2.6.2 Los detectores de incendio deberían ser redundantes y ubicados de forma que cubran toda la sala. Para máxima seguridad se recomienda la existencia de un detector dedicado por cada rack, además de los generales de la sala/edificio.

2.6.3 El sistema de extinción de incendios no debería dispararse hasta que no se detecte fuego o humo por dos detectores distintos.

2.6.4 Es conveniente verificar periódicamente la operatividad de los sistemas de detección y extinción, garantizando así su buen funcionamiento.

2.6.5 En el edificio o lugar donde se ubique el Centro de Procesamiento de Datos, debería estar disponible al menos una caja de seguridad ignífuga en la que guardar copias de seguridad de los servidores (cintas backup, CD, DVD, entre otros). Es conveniente que esta caja permanezca siempre cerrada.

2.7 Consideraciones sobre la Plataforma Tecnológica a utilizar.

2.7.1 Es imprescindible el establecimiento de políticas para el acceso lógico (segregación de funciones y roles) en equipos de telecomunicaciones,

así como en servidores de internet, de aplicaciones y de base de datos, a los fines de evitar que sea afectada la integridad de la información contenida en ellos (apoyándose en Logs de auditoría).

2.7.2 Se debería contar con equipos para la protección perimetral, basados en estándares abiertos, con la finalidad de proteger los activos de información que se encuentran dispuestos en la infraestructura del Centro de Procesamiento de Datos a implementar.

2.7.3 Es fundamental el establecimiento de mecanismos para la segregación de procesos, tales como la separación de ambientes lógicos para el acceso de aplicaciones críticas (extranet e intranet), que cuenten con controles de seguridad que establezcan métodos de encriptación del canal de comunicación cuando así la institución lo considere necesario.

2.7.4 Se debería diversificar la marca y modelo de equipos tanto para protección perimetral como para telecomunicaciones (no utilizar la misma marca/modelo para todos los switches/routers/firewalls/ids/ips),