

Centros de datos que enfrentan riesgos: amenazas controladas

La nube ha conseguido convencer a muchos seguidores gracias a estas múltiples ventajas: sencillez, adaptabilidad o costes controlados. Para proteger mejor los datos que se les confían, los proveedores éticos siguen una regla de oro: anticiparse a lo imprevisible.

De hecho, los [centros de datos](#), como cualquier otra instalación, se enfrentan a varios riesgos y esto puede asustar a empresas y personas. Sin embargo, los servidores del centro de datos suelen ser mucho más seguros que las propias estructuras de TI de las empresas. Existen varias amenazas y los proveedores de la nube tienen especialistas para analizar y anticipar cada uno de estos riesgos.

Riesgo físico y vandalismo

Este es el riesgo asociado con una intrusión física en el sitio: robo de equipos que contienen datos, incendio provocado o incluso rotura del servidor. Para responder a este riesgo, se han puesto en marcha sistemas de videovigilancia y detección volumétrica de movimientos dentro del perímetro de seguridad.

Además, la entrada al edificio está asegurada por un estricto control de acceso con diferentes niveles de derechos según la sección. En caso de problemas, los derechos de acceso se pueden revocar rápidamente y las credenciales se desactivan automáticamente. El edificio también está equipado con puertas

blindadas, sistemas de detección de golpes en puertas y ventanas. Toda esta instalación tiene como objetivo poder reaccionar muy rápidamente en caso de un intento de robo, con un rápido apoyo por parte del personal in situ presente 24/7 y de la policía.

Para mitigar la amenaza de incendio, se han instalado detectores. Los centros de datos también están equipados con un sistema automático de extinción de gas, si un incendio es confirmado por 2 detecciones simultáneas, los cilindros se golpearán instantáneamente para llenar la sala de computadoras con un gas que evite la reacción química del Dispare y bloquee cualquier incendio en curso.

El riesgo meteorológico

Esta categoría incluye todos los peligros relacionados con las condiciones climáticas extremas: inundaciones, rayos u olas de calor. Para prevenir posibles desastres, este riesgo se estudia incluso antes de la instalación del centro de datos para evitar la construcción en una zona de inundación. El edificio también está rodeado de pararrayos y armarios eléctricos equipados con pararrayos para proteger el lugar en caso de tormenta.

Las unidades de aire acondicionado se eligen específicamente para funcionar incluso cuando se someten a temperaturas muy altas.

Riesgos intrínsecos y eléctricos



Para la parte eléctrica, los inversores están presentes para compensar un posible microcorte; en caso de problemas más graves, como un fallo total del suministro eléctrico principal de alta tensión, los centros de datos están equipados con un generador que puede garantizar su autonomía. También se llevan

a cabo auditorías anuales para garantizar una seguridad óptima del sitio.

Una cámara térmica permite verificar que no haya puntos calientes que puedan generar un inicio de incendio y el cableado también se verifica una vez al año.

Finalmente, en caso de una fuga de agua, un sistema automatizado corta el suministro de agua a la sala de computadoras.

Riesgo digital

Las amenazas digitales son todos los riesgos asociados con la piratería. Para ello, los servidores pueden estar equipados con un antivirus, un firewall, pero también una solución para bloquear los ataques DDoS. Por tanto, se controla un amplio espectro de vectores de ataque.

Estas son las precauciones que toma cada proveedor para un solo centro de datos. La creación de un segundo centro de datos, especialmente si se utiliza para realizar planes de recuperación empresarial, también requiere algunas buenas prácticas. Lo ideal es que los dos edificios no estén separados por más de 50 km entre sí para tener una baja latencia para la sincronización de datos. Pero tampoco deben pertenecer a las mismas redes eléctricas, porque si se produce una interrupción prolongada, ambas se verían potencialmente afectadas.

Leer también: [¿Porqué se llama Nebula el data center de HostDime Colombia?](#) ; [Importancia del Data center Nebula de HostDime para Colombia y Sudamérica](#) ; [Data center, edge cloud, nube híbrida y atada](#)