EL BÚNKER DE LOS DATOS

Guía para preparar la última línea de defensa de su información crítica.

IBM | GBM

Cuando todo cae ¿qué queda en pie?

Imagine que una empresa después de una explosión digital, va a encontrar sistemas bloqueados, usuarios sin acceso, operaciones detenidas y equipos de TI intentando responder bajo presión.

El ataque ya ocurrió, pero qué es más importante preguntarse ¿cómo lo remediamos? o ¿qué información sigue a salvo y desde dónde podemos restaurar? la respuesta es, se deben plantear ambas preguntas.

Con GBM ese es el principio de El Búnker de los Datos, una última línea de defensa diseñada para proteger la información crítica y permitir la recuperación cuando el entorno principal queda comprometido. El riesgo no es teórico, el costo promedio global de una brecha de datos fue de **US$4,44 millones en 2025,** aunque bajó frente al año anterior, sigue representando un impacto significativo para las organizaciones.

En este orden de ideas, aquí conocerá que la resiliencia en ciberseguridad se mide por la capacidad de prevenir y también de restaurar.

La recuperación ya no puede depender de la improvisación

Diferentes organizaciones trataron el respaldo como un seguro, es decir, algo que se guarda por si acaso, pero la recuperación ante ciberataques exige más que las prácticas tradicionales de disaster recovery, porque no basta con tener copias; las empresas necesitan capacidades reales de cyber-recovery para reducir vulnerabilidad y proteger misión, operación y resultados.

En la práctica, los puntos débiles suelen aparecer en cinco lugares:

Ventanas de respaldo cada vez más cortas
Los datos crecen, pero el tiempo disponible para respaldarlos no.

Restauración lenta o incierta
Tener respaldo no siempre significa poder recuperar rápido y con confianza.

Sistemas críticos con baja tolerancia a interrupciones
Mainframe, core bancario, transacciones, clientes y operación no pueden esperar.

Complejidad operativa en crecimiento
Más datos, más plataformas, más presión sobre equipos de TI.

Ransomware y desastres como escenarios reales
La estrategia debe asumir que algo puede fallar y preparar cómo volver.

Aquí es donde una Virtual Tape Library (VTL) combina la lógica confiable del tape con capacidades virtualizadas para respaldar, proteger y recuperar datos críticos con mayor eficiencia.

IBM TS7700: el búnker virtual para datos críticos

IBM TS7700 Virtual Tape Library está diseñada para responder a tres necesidades empresariales:

1. Crecimiento de almacenamiento.
2. Ventanas de respaldo más pequeñas.
3. Acceso confiable a los datos.

Esto funciona como un búnker virtual, permite conservar la lógica de protección del tape, pero con una arquitectura moderna que ayuda a acelerar respaldos, facilitar recuperación y sostener continuidad en entornos empresariales críticos.

¿Qué permite habilitar?

A. Resiliencia frente a eventos críticos
Una capa preparada para respaldar información esencial y apoyar procesos de recuperación.

B. Modernización sin romper lo existente
Permite evolucionar el respaldo sin abandonar la compatibilidad con operaciones de tape.

C. Escalabilidad y eficiencia operativa
Ayuda a responder al crecimiento de datos y a la presión de administrar menos complejidad.

D. Una última línea de defensa
Cuando el entorno principal queda comprometido, la empresa necesita una fuente confiable para restaurar.

¿Su organización tiene respaldos o tiene un búnker listo para resistir el peor escenario?

En ciberseguridad, detener el impacto y asegurar que, después del impacto, exista una ruta para recuperar la información crítica y volver a operar, es la clave.

Con **IBM TS7700 Virtual Tape Library**, GBM ayuda a las empresas a fortalecer su estrategia de resiliencia, recuperación y protección de datos desde una infraestructura diseñada para entornos donde detenerse no es una opción.

www.gbm.net

mercadeo@gbm.net | /gbmcorp

IBM | GBM