Interempresas

Seguridad y Vigilancia

ACTUALIDAD

Un ciberataque puede dañar seriamente la reputación de una empresa

TDI refuerza su infraestructura en España con soluciones avanzadas de ciberseguridad y continuidad operativa

Redacción Interempresas 22/04/2025

535

La transformación digital del sector del transporte en España está en marcha, y con ella aumenta la necesidad de garantizar la seguridad de los sistemas críticos y la continuidad operativa ante cualquier incidente. En este contexto, TDI, especialista en soluciones digitales para el transporte y la logística, ha reforzado su estructura tecnológica con un plan integral de ciberseguridad y un sistema de recuperación inmediata basado en servidores redundantes.

"Nuestro objetivo no es solo proteger los datos, sino asegurar que la operación de nuestros clientes nunca se detenga. Sabemos que en el sector del transporte y la logística, cada minuto cuenta", afirma Edmundo Brito, director de TDI España.

Ciberseguridad y disponibilidad: pilares de una operación digital fiable

Según datos del Instituto Nacional de Ciberseguridad (INCIBE), el 70% de los incidentes de ciberseguridad en España afectan a pequeñas y medianas empresas, y el sector logístico no es una excepción. Un ciberataque o una caída del sistema puede paralizar las operaciones, generar pérdidas económicas y poner en jaque la reputación corporativa.

Para evitarlo, **TDI** ha implementado en sus operaciones en España un Plan de Continuidad de Actividad (BCP en sus siglas en inglés) que garantiza una respuesta automática en milisegundos ante cualquier fallo. Su estructura está basada en dos centros de datos activos, ubicados en zonas estratégicas, que replican los datos y operaciones en tiempo real. Esto permite que, si uno de los servidores falla, el sistema realice un cambio instantáneo al segundo centro sin pérdida de información ni interrupciones en el servicio.

Infraestructura para garantizar la continuidad

La solución de TDI en España permite:

- Realizar un switch over automático e instantáneo en caso de fallo del centro principal.
- Garantizar el acceso continuo a los servicios, incluso en caso de pérdida de conectividad.
- Mantener una configuración activo/activo, con la carga de trabajo distribuida de forma inteligente.
- Trabajar sobre una infraestructura hiperconvergente, segura y eficiente.

Protección proactiva con tecnología de vanguardia

Para reforzar esta infraestructura, TDI ha desplegado un conjunto de soluciones avanzadas de ciberseguridad:

- SentinelOne: instalada en todos los puestos de trabajo, esta tecnología de detección autónoma recoge y analiza en tiempo real los logs, enviándolos a un centro de operaciones de seguridad (SOC) para su evaluación.
- Monitoreo 24/7 con especialistas en ciberseguridad, que analizan y actúan ante cualquier comportamiento sospechoso.
- Auditorías periódicas para mantener actualizadas las certificaciones de seguridad y garantizar la protección de los entornos digitales.

Un modelo que ya ha sido puesto a prueba

TDI ha realizado recientemente pruebas controladas para verificar la eficacia de su sistema BCP, incluyendo la desconexión deliberada de su conexión principal entre centros de datos. El resultado: ningún impacto en los clientes, y la confirmación de que su sistema permite continuar con las operaciones incluso ante fallos críticos.

"La digitalización del transporte no puede avanzar sin seguridad y fiabilidad. Por eso hemos hecho de la continuidad operativa un pilar central de nuestra estrategia en España", concluye Edmundo Brito.