Ciberseguridad como pilar fundamental en la Intralogística

> *La intralogística gana fuerte relevancia para las compañías, pues dicha área es fundamental para gestionar y controlar todas las operaciones internas de la cadena de suministro. Incluso, el sector intralogístico proyecta que para el 2026 el valor del mercado alcanzará los 30 mil millones de dólares.*

Sin embargo, a medida que se generan cambios o mejoras, nacen también nuevos riesgos, por lo que entra al escenario otro proceso vital que debemos considerar profundamente: la ciberseguridad.

La Importancia de la Ciberseguridad en la Intralogística

Como ya lo mencionamos, la ciberseguridad se ha convertido en un pilar fundamental dentro de la intralogística, pues cada vez son más los ataques y amenazas cibernéticas que enfrentan las empresas. La protección de cada uno de los sistemas informáticos y la información que se maneja en dichas operaciones se vuelve crucial para garantizar la continuidad de los procesos y la integridad de los datos.

Una de las principales preocupaciones en materia de ciberseguridad en la intralogística es la protección de los sistemas de gestión de almacenes y los sistemas de control y automatización de procesos logísticos, entre otros. Estos sistemas son el corazón de las operaciones intralogísticas, ya que permiten el seguimiento y control de las existencias, la gestión de pedidos y el flujo de mercancías.

A medida que las empresas continúan digitalizando y automatizando sus operaciones de intralogística, la necesidad de proteger sus sistemas y datos contra ciberataques se vuelve cada vez más crítica. Por ello es que las compañías deben implementar medidas de ciberseguridad robustas y mantenerse al día con las últimas tendencias y amenazas de ciberseguridad, para garantizar la eficiencia, resguardo y seguridad de las operaciones intralogísticas.

¿Por qué la ciberseguridad es clave?

- En 2022 se detectaron 493.33 millones de ataques de ransomware, de acuerdo con Malwarebytes. El ransomware es una forma de malware que actualmente está en auge y bloquea los archivos o dispositivos de un usuario, posteriormente se reclama un pago online anónimo para que el acceso pueda ser restaurado.

Estos ataques pueden ser catastróficos ya que la intralogística centra todos sus datos en la nube, simplificando la gestión de pedidos, proceso de compra, gestión de inventarios, costos e información del usuario

- De acuerdo con el informe "El Estado Global de la Ciberseguridad Industrial 2023, nuevas tecnologías, amenazas persistentes y defensas en proceso de maduración", durante el 2022 el 75% de los encuestados sufrió ataques "ransomware" en la empresa para la que laboran, de los cuales el 69% pagó el rescate que los hackers solicitaron, lo que implica un gasto y riesgo para las empresas, pues no hay garantía de que los datos sean realmente devueltos sin que se realicen copias de los mismos.

- Algunos de los países que se han visto más afectados por dicho carácter (ransomware), son: Chile con un 9.1% de ataques, seguido de Brasil, México y Colombia. Han sido los servicios, la Industria y el mundo financiero los sectores más afectados.

¿Cómo comenzar a integrar sistemas de seguridad intralogísticos??

Hoy en día crear sistemas de seguridad que resguarden la información de los clientes, proveedores y de la misma empresa es parte de las prioridades que más deben considerarse. Sin embargo, puede ser abrumador dar el primer paso. De acuerdo con IKUSI, especialistas en ciberseguridad, este puede ser un primer camino a tomar:

- Evaluar la Infraestructura existente: Realiza una evaluación exhaustiva de la infraestructura intralogística actual para identificar posibles vulnerabilidades y riesgos de seguridad.

- Establecer objetivos de seguridad: Define claramente los objetivos de seguridad que deseas lograr. Esto podría incluir la protección de datos, la prevención de accesos no autorizados y la garantía de la disponibilidad del sistema. Cada empresa tiene diferentes prioridades y sensibilidad de información, valdrá la pena que desarrolles este mapeo con tu equipo.

- Establecer políticas de seguridad: Dentro de las políticas de seguridad se deben de incluir métodos de seguridad digital, aunado a determinar cuáles serán las responsabilidades y el alcance de cada colaborador.

- Contar con infraestructura de ciberseguridad: Una vez identificados los puntos anteriores, puedes ir sobre un camino más certero e integrar los sistemas de ciberseguridad necesarios, así como el software (y soporte) adecuado.

Asegúrate de hacerle frente a situaciones que pongan en riesgo tus operaciones de la mano de especialistas. Anticiparse a los desafíos que enfrenta el sector logístico es parte de las actividades que no son opcionales.

La información te pone un paso adelante, por lo que te recomendamos no perderte las publicaciones que crean nuestros expertos, en donde te compartimos las tendencias y puntos destacados de la industria.

> Publicado por: G.I.Eicom
> Líderes en Material Handling & Intralogistics Solutions

Material Handling & Logistics Solutions
WE CREATE | VALUE