G.I.EICOM®

Cybersecurity as a fundamental pillar in Intralogistics

> *Intralogistics gains strong relevance for companies, since this area is essential to manage and control all internal operations of the supply chain. The intralogistics sector even projects that by 2026 the market value will reach 30 billion dollars.*

However, as changes or improvements are generated, new risks are also born, which is why another vital process that we must consider deeply enters the scene: cybersecurity.

The Importance of Cybersecurity in Intralogistics

As we already mentioned, cybersecurity has become a fundamental pillar within intralogistics, as there are more and more cyber-attacks and threats that companies face. The protection of each of the computer systems and the information handled in these operations becomes crucial to guarantee the continuity of the processes and the integrity of the data.

One of the main concerns regarding cybersecurity in intralogistics is the protection of warehouse management systems and logistics process control and automation systems, among others. These systems are the heart of intralogistics operations, since they allow the monitoring and control of stocks, order management and the flow of goods.

As companies continue to digitize and automate their intralogistics operations, the need to protect their systems and data against cyberattacks becomes increasingly critical. This is why companies must implement robust cybersecurity measures and keep up to date with the latest cybersecurity trends and threats, to guarantee the efficiency, protection and security of intralogistics operations.

¿Why cybersecurity is key?

- In 2022, 493.33 million ransomware attacks were detected, according to Malwarebytes. Ransomware is a form of malware that is currently on the rise and locks a user's files or devices, subsequently demanding an anonymous online payment so that access can be restored.

These attacks can be catastrophic since intralogistics focuses all its data on the cloud, simplifying order management, purchasing process, inventory management, costs and user information.

- According to the report “The Global State of Industrial Cybersecurity 2023, new technologies, persistent threats and maturing defenses”, during 2022, 75% of those surveyed suffered “ransomware” attacks in the company they work for , of which 69% paid the ransom that the hackers requested, which implies expense and risk for companies, since there is no guarantee that the data will actually be returned without copies being made of it.

- Some of the countries that have been most affected by this nature (ransomware) are Chile with 9.1% of attacks, followed by Brazil, Mexico and Colombia. Services, Industry and the financial world have been the most affected sectors.

G.I.EICOM®

How to start integrating intralogistics security systems?

Nowadays, creating security systems that protect the information of clients, suppliers and the company itself is part of the priorities that must be considered the most. However, it can be overwhelming to take the first step. According to IKUSI, cybersecurity specialists, this may be a first path to take:

- **Evaluate the existing Infrastructure:** Conduct a comprehensive assessment of the current intralogistics infrastructure to identify potential vulnerabilities and security risks.

- **Establish security objectives:** Clearly define the security objectives you want to achieve. This could include data protection, preventing unauthorized access, and ensuring system availability. Each company has different priorities and information sensitivity, it will be worth developing this mapping with your team.

- **Establish security policies:** Digital security methods must be included within the security policies, along with determining what the responsibilities and scope of each collaborator will be.

- **Have cybersecurity infrastructure:** Once the previous matters have been identified, you can take a more certain path and integrate the necessary cybersecurity systems, as well as the appropriate software (and support).

Make sure you deal with situations that put your operations at risk with the help of specialists. Anticipating the challenges facing the logistics sector is part of the activities that are not optional.

The information puts you one step ahead, so we recommend not missing the publications created by our experts, where we share the trends and highlights of the industry.

Posted by: G.I.EICOM
Leaders in Material Handling & Intralogistics Solutions

Material Handling & Logistics Solutions
WE CREATE | VALUE