ConaLog
Consejo Nacional de Ejecutivos
en Logística y Cadena de Suministro, A.C.

“HASTA QUE TE SUCEDE, SE VUELVE PRIORITARIO”

KARLA VANESSA RAMÍREZ GARCÍA
Estudiante, Ingeniería Industrial

GUSTAVO EQUIHUA ALBARRÁN
Consejero ConaLog | Director de Análisis y Gestión TI, Frialsa Frigoríficos

Sin duda, la pandemia, vino a retar a casi todos los negocios exigiéndoles herramientas tecnológicas para trabajo en home office, a lo cual se suma al desafío de trabajar de manera segura desde un lugar donde no existe una política de seguridad y desde el que los empleados pueden navegar libremente por internet. Actualmente las empresas están apostando en inversiones tecnológicas de diversos tipos, y la gestión de la información en el ámbito logístico no es una excepción, por su complejidad y relevancia.

Sobre ello discurrieron recientemente en el webinar “El flujo de información, como centro del proceso logístico, y su seguridad”, varios expertos.

El Director de Gestión y TI de Frialsa Frigoríficos, Gustavo Equihua, destacó que la información que fluye en todos los eslabones de la cadena de suministro es no solo vital sino también cuantiosa dependiendo el volumen de operación de cada compañía; por ejemplo: geolocalización de vehículos, gestión de inventarios, generación de facturas o nóminas, historial de clientes o servicio y, desde luego, las cuentas por pagar y por cobrar, todo lo cual representa una enorme de datos que es complicado de cuantificar.

Por su parte, la Gerente de Proyectos de TI de Estafeta, Beatriz Aguiriano, expresó que puede haber fuga o pérdida de información a partir de fallas administrativas en la manipulación de la información de los datos a través de los empleados, consecuencia de errores por simple desconocimiento por lo cual una buena práctica es velar por la seguridad con base en capacitación que todos en la empresa conozcan el valor de la información y cómo cuidarla. Ya que ciertamente, ante cualquier tipo de error, fuga de información o ataque, la productividad de la empresa puede afectarse por varios días, y las pérdidas económicas aumentarán por cada minuto sin operar, o por la caída de la credibilidad del negocio. De ahí resulta relevante que las organizaciones aumenten la concientización sobre los riesgos y las amenazas que existen en el entorno digital, y que se asesoren con expertos internos y proveedores que los puedan asesorar.

Desde la perspectiva de Francisco Garibay, Director Comercial de Nephos IT, es paradójico que, aunque los datos son uno de los activos más valiosos para cualquier empresa, continuamente están expuestos al riesgo de diferentes tipos de accesos y manipulaciones. Por ello, plantea que una buena estrategia para protegerlos es invertir en planes de contingencia que permitan minimizar los daños en a la empresa, como la pérdida de facturación y clientes a causa de algún incidente de seguridad. Estimó que un tercio de las empresas en México no tiene cuantificado el costo de un “down-time” en su negocio, mas éste puede ser mayor que la inversión requerida para evitarlo. Por ello, recomendó que los negocios cuantifiquen y gestionen este tipo de riesgos, que sean más abiertos a la digitalización tecnológica, apalancada con expertos en herramientas y metodologías relacionadas, pues estas cambian de manera continua.

Ante la pregunta de ¿cómo ajustar o modular tales peligros?, Gustavo Equihua planteó que un buen abordaje es realizar formalmente un análisis de riesgo, ya que permite evaluar la probabilidad e impacto de cada riesgo en cada las áreas de la organización y la empresa como

un todo, completando un panorama que permite orientar de mejor manera una estrategia con los trabajos e inversiones que deberán efectuarse.

Como explicó Beatriz Aguiriano, es primordial controlar la seguridad de la información con planes de prevención, adaptables a futuras amenazas: las empresas deben invertir en seguridad de la información tanto para protección contra ataques informáticos, pero sobre todo para asegurar su continuidad como negocio.