Gestión del Ciclo de Abastecimiento

Segundo encuentro
Tendencias en Supply Chain: Ciberseguridad, Blockchain y Normativa UE en Sostenibilidad

Invitados

Fabian Descalzo, Julio Navarrete y María Bladimirsquy

BDO

Introducción

Desde BDO entendemos que Supply Chain es un modelo fundamental para el cumplimiento de los objetivos estratégicos, desde la Planificación de la Demanda, Capacidad Operativa S&OP, Suministros, Logística y Abastecimiento, y lógicamente cómo estos se relacionan con el contexto local e internacional, y su impacto con Compliance y Sostenibilidad.

Creamos este ciclo de charlas para exponer los desafíos y tendencias que se presentan en la Gestión de la Cadena de Suministro como mirada integradora holística con el propósito de satisfacer las necesidades de los clientes (internos y externos). Un espacio para el diálogo, el intercambio de experiencias e inquietudes, propiciando el nacimiento de nuevas relaciones colaborativas.

Nos motiva la experiencia de saber que todo proyecto de transformación exitoso se apalanca fuertemente en la tecnología aplicada al servicio de los negocios, la integración de los procesos y el impacto que estas dimensiones tienen en las personas.

BLOQUE 1

Ciberseguridad: Evolución del negocio. Cómo pensar en Seguridad desde la Estrategia.

Invitado
Fabian Descalzo, Socio de Ciberseguridad y Gobierno Tecnológico,
BDO en Argentina

La evolución tecnológica ha transformado radicalmente la gestión de las cadenas de suministro. Desde la introducción de los códigos de barras en los años 50 hasta la revolución del e-commerce liderada por gigantes del comercio electrónico en los 90, la tecnología ha sido un catalizador de eficiencia y competitividad. Sin embargo, esta dependencia tecnológica ha traído consigo nuevos riesgos que las empresas deben gestionar activamente.

Hoy en día, los proveedores y partners logísticos no son meros prestadores de servicios, sino socios estratégicos cuya ciberseguridad impacta directamente en la continuidad del negocio de sus clientes. Según proyecciones de Gartner, para 2025, el 45% de las organizaciones a nivel mundial habrán sufrido algún tipo de ataque a su cadena de suministro, evidenciando la urgencia de abordar esta problemática.

La vulnerabilidad de las empresas frente a ciberataques es alarmante: se estima que el 82% de las compañías en el sector de logística y cadena de suministro son susceptibles a estas amenazas. Esta situación se debe tanto a la obsolescencia tecnológica como a la implementación inadecuada de soluciones de seguridad.

Los impactos de un ciberataque en la cadena de suministro pueden ser devastadores, como lo demuestran casos emblemáticos:

- Una de las navieras líderes mundiales en el transporte y clave en la cadena global de suministros sufrió un incidente de seguridad que paralizó su flota, generando pérdidas millonarias y afectando a sus clientes globalmente.
- Una empresa líder en soluciones de software para la gestión de infraestructuras IT fue víctima de un ataque de ransomware que tuvo repercusiones en miles de sus clientes, incluyendo compañías que cotizan en la bolsa de Nueva York, lo que llevó a cambios regulatorios por parte de la SEC.
- El puerto del Mediterráneo más importante de España quedó inoperativo durante 6 días debido a un ciberataque, con consecuencias económicas significativas para el comercio regional e internacional.

Para ilustrar la complejidad de estos riesgos, consideremos el caso de un laboratorio farmacéutico que delega su distribución a una empresa logística. Un ataque a los sistemas del proveedor logístico no solo interrumpiría la entrega de medicamentos, sino que podría resultar en la pérdida de lotes enteros debido a incumplimientos regulatorios, generando pérdidas económicas y daños reputacionales.

BLOQUE 1

La gestión efectiva de la ciberseguridad en la cadena de suministro requiere un enfoque holístico que integre tecnología, procesos y personas. Solo así las empresas podrán innovar de forma segura, manteniendo la confianza de sus clientes y partners en un ecosistema digital cada vez más complejo y amenazado.

Conclusiones

La ciberseguridad es un componente crítico en la gestión moderna de la cadena de suministro, trascendiendo el ámbito puramente tecnológico para convertirse en un imperativo de negocio.

Las empresas deben considerar a sus proveedores y partners logísticos como extensiones de su propia infraestructura de seguridad.

La innovación tecnológica debe ir acompañada de una estrategia de seguridad robusta para proteger los procesos de negocio y la información sensible.

Es fundamental realizar evaluaciones periódicas de seguridad tanto de los sistemas propios como de los proveedores críticos.

La preparación y respuesta ante incidentes de ciberseguridad debe ser una prioridad en la planificación estratégica de las empresas.

La colaboración y el intercambio de información sobre amenazas entre empresas del sector pueden fortalecer la resiliencia colectiva frente a ciberataques.

BLOQUE 2

Blockchain aplicado a la integración de la cadena logística

Invitado
Julio Navarrete, Socio de Transformación digital, BDO en Ecuador

El panorama actual presenta diversos riesgos para las cadenas de suministro: biológicos, económicos, cibernéticos y tecnológicos. Estos riesgos impactan directamente en el objetivo principal de cualquier organización: llevar su producto al mercado. La creciente interdependencia entre actores a nivel global añade un factor adicional: el riesgo de la dependencia de terceros.

La aparición de nuevas regulaciones internacionales, que exigen trazabilidad de origen a destino, complejiza aún más este escenario. Leyes como la FSMA de Estados Unidos para productos frescos, el reglamento de trazabilidad de productos vinícolas de la Unión Europea, y las regulaciones sobre productos de terrenos deforestados, son ejemplos claros de esta tendencia.

Si bien muchas organizaciones ya implementan algún tipo de trazabilidad, generalmente se limita a la cadena logística bajo su control directo. La pregunta crucial es: ¿cómo garantizar la confiabilidad y seguridad de la información cuando se interactúa con actores desconocidos a lo largo de la cadena de suministro?

La tecnología Blockchain emerge como una solución robusta para afrontar este desafío. Sus características intrínsecas la convierten en una herramienta ideal para la integración de la cadena logística:

- **Naturaleza Distribuida:** La información se replica en miles de servidores a nivel global, eliminando un único punto de fallo y fortaleciendo la seguridad.
- **Inmutabilidad:** Los datos registrados en la Blockchain no pueden ser alterados ni borrados, garantizando la integridad de la información.
- **Seguridad:** Algoritmos criptográficos y mecanismos de consenso protegen la información de accesos no autorizados y manipulaciones.
- **Contratos Inteligentes:** Permiten codificar las reglas de negocio y automatizar procesos dentro de la cadena de suministro.

Al implementar Blockchain, cada etapa de la cadena logística, desde la producción hasta el consumidor final, puede registrar información relevante de forma segura e inmutable.

BLOQUE 2

La tecnología Blockchain se posiciona como un elemento clave para construir cadenas de suministro más resilientes, transparentes y confiables en un mundo cada vez más interconectado.

Conclusiones

La integración de la cadena logística basada en Blockchain brinda confianza y transparencia a todos los actores involucrados.

Los consumidores pueden acceder a información verificada sobre el origen, recorrido y tratamiento de los productos, fortaleciendo la confianza en las marcas.

Las empresas pueden asegurar el cumplimiento de las crecientes regulaciones internacionales de trazabilidad.

La inmutabilidad y seguridad de la Blockchain minimizan riesgos de fraude, falsificación y manipulación de información.

Se establece un canal de comunicación directo entre productores y consumidores finales, abriendo oportunidades para la fidelización y la personalización de productos y servicios.

BLOQUE 3

Cambios regulatorios en materia de ESG: Entrada en vigencia de la Directiva sobre diligencia debida de las empresas en materia de sostenibilidad de la Unión Europea.

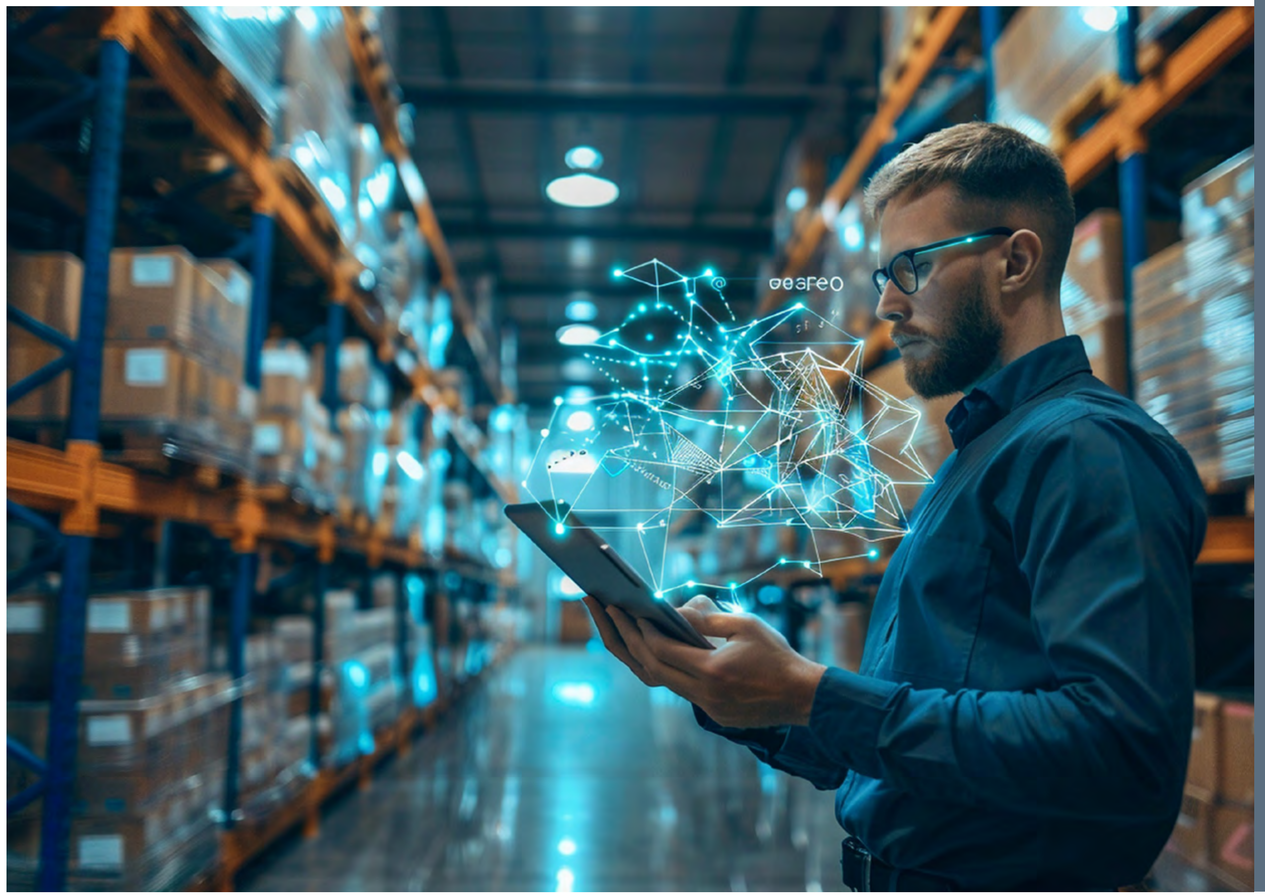
Invitado
María Bladimirsquy, Especialista en DDHH & Compliance, BDO en Argentina

¿Cómo impacta en las empresas fuera de la UE? ¿Qué debería hacer el área de Supply Chain? El pasado 24 de mayo se aprobó la Directiva sobre diligencia debida de las empresas en materia de sostenibilidad en la UE. Cada Estado parte tiene un período de gracia de dos años para incorporar el texto de la Directiva a su derecho interno.

La Directiva alcanza a las grandes empresas de la UE que tengan más de 1.000 trabajadoras/es y cuya facturación anual a escala mundial sea mayor a 450 millones de euros. Sin embargo, se exige mayor rigurosidad con el correr de los próximos años. Para 2027 afectará a empresas con más de 5.000 personas trabajadoras y con una facturación mayor a 1.500 millones de euros, para 2028 a aquellas que cuenten con 3.000 personas trabajadoras y más de 900 millones de euros y, para 2029, a empresas con 1.000 personas trabajadoras y con una facturación mayor a 450 millones de euros. A su vez, afecta a aquellas empresas externas a la UE pero que desarrollen actividades allí, siendo el mismo alcance que las grandes empresas de la UE aunque el requisito es únicamente sobre la facturación. En cuanto a las PyMES, no están afectadas de manera directa por el texto de la Directiva aunque sí quedan afectadas por ser parte de la cadena de suministro de empresas que operen con la UE o estén localizadas allí. Por último, es preciso destacar que se prevén sanciones de hasta un 5% de la facturación global neta de las compañías que realizan una debida diligencia inadecuada.

Es importante entender que los derechos humanos trascienden a toda la organización. En este sentido, para poder desarrollar una debida diligencia adecuada en materia ambiental y de derechos humanos, se necesita del trabajo mancomunado de las distintas áreas de las compañías (por ejemplo, se deberá involucrar a las áreas de Sostenibilidad, Recursos Humanos, Compliance, Compras, Legales y Gestión de Riesgos).

BLOQUE 3



Conclusiones

Si como empresa quedás alcanzada por la Directiva, deberías:

Comenzar dando los primeros pasos en la debida diligencia en derechos humanos y ambiente. Por ejemplo, diseñar una Política, identificar y evaluar potenciales y actuales impactos negativos en derechos humanos y ambiente con un enfoque basado en el riesgo. Desarrollar mecanismos de quejas, por ejemplo mediante líneas de denuncia, entre otras medidas.

Evaluar los riesgos a los derechos humanos y ambiente de proveedores, desarrollando auditorías frecuentes para proveedores de alto riesgo.

Publicar un informe anual en el que se dé a conocer la debida diligencia que se realiza en materia de derechos humanos y ambiente.

Conservar la documentación importante para justificar las acciones y decisiones tomadas en los últimos cinco años, ya que se podrían requerir auditorías de autoridades regulatorias de la UE.

BDO en Argentina

Maipú 942, C1006ACN
Cdad. Autónoma de Buenos Aires
Teléfono: 011 5274 5100

www.bdoargentina.com

Inscribirme en el evento