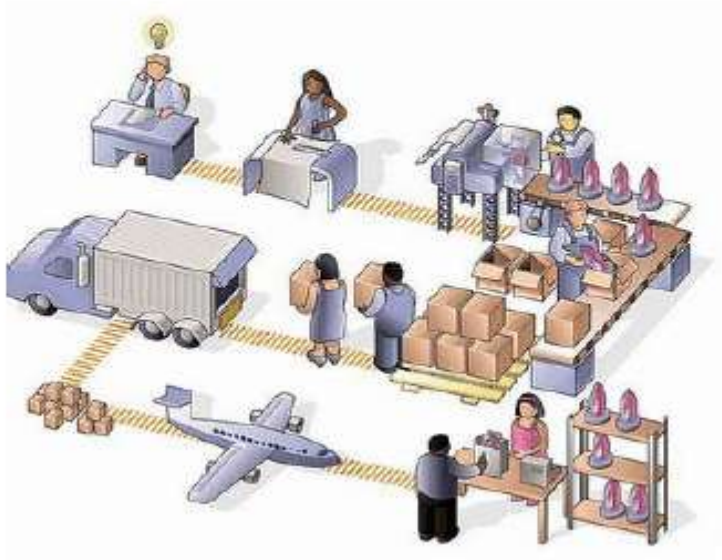
OPERADOR ECONÓMICO AUTORIZADO

Mejores Practicas en Seguridad de la Cadena de Suministros

CONCEPTOS GENERALES

Cadena de suministro

Conjunto relacionado de recursos y procesos que comienza con la provisión de materias primas y se extiende hasta la entrega de productos o servicios al usuario final a través de los medios de transporte



CONCEPTOS GENERALES

Seguridad

Resistencia al acto o actos intencionados y no autorizados, destinados a causar daño o perjuicio a la cadena de suministro o a través de ella.

¿y no intencionados?

CONCEPTOS GENERALES

Gestión de la Seguridad

Actividades y prácticas sistemáticas y coordinadas a través de las cuales una organización gestiona de manera óptima sus riesgos y las amenazas e impactos potenciales asociados

Mejores Practicas en Seguridad de la Cadena de Suministros

SISTEMA DE GESTION DE LA SEGURIDAD

El sistema de Gestión de la Seguridad para la cadena de suministro supone para una organización, una **herramienta** que proporciona los **medios y requisitos** necesarios para **alcanzar y controlar** los objetivos, metas y programas de seguridad que esta fija, incluyendo todas las actividades que tienen impacto en la cadena de suministro (Identificación de amenazas, gestión de riesgos, control y mitigación de consecuencias).

POLITICA DE GESTION DE LA SEGURIDAD

El desarrollo del compromiso de gestión de la seguridad por parte de la organización, es considerado como una de las **mejores practicas** de la cadena de suministro, la cual se plasmará a través de una ***Política de Seguridad.*** Esto supone, que el Sistema de Gestión de Seguridad para la cadena de suministro sea exitoso.

La Política de la Gestión de la Seguridad ***debe ser definida y autorizada por la alta dirección*** de la organización.

REQUISITOS PARA EL DISEÑO DE LA POLITICA DE SEGURIDAD

1. ANÁLISIS, PLANIFICACIÓN Y GESTIÓN DEL RIESGO.	
1.1. POLÍTICA DE SEGURIDAD Y SISTEMA DE ANÁLISIS DE RIESGOS	
1.1.1. Política de Seguridad. El OEA debe contar con una Política de Seguridad, que sea adecuada al tamaño y naturaleza de la empresa y de sus actividades. Es requisito que la política de seguridad sea documentada y autorizada por la alta dirección y que establezca e implemente un sistema de análisis y gestión del riesgo que permita identificar las amenazas, evaluar los riesgos asociados y controlar/mitigar sus consecuencias. (Estándar de Referencia: ISO 28001:2007)	*Adjunte el documento de la política de seguridad. Procure que en el texto estén presentes los siguientes elementos:* *a) Cómo la alta dirección se compromete con la gestión de la seguridad.* *b) Los principios y objetivos para la gestión de la seguridad en toda la empresa.* *c) Cómo la alta dirección asegura la aplicación de la política de seguridad en todos los niveles de la empresa.*

ASPECTOS A TENER EN CUENTA PARA DEFINIR LA POLITICA DE SEGURIDAD

- Ser ***breve*** y estar escrita en ***un lenguaje claro y sencillo,*** para ser entendida por las partes, tantos internas como externas***.***
- Considerar los ***valores y objetivos*** de la organización en materia de seguridad.
- Estar en concordancia ***con las demás políticas*** de la organización.
- No perder de vista la **Normativa**, las leyes y otros compromisos aplicables a los que se encuentre suscrita la organización.
- Ser ***coherente*** con el ***marco de trabajo global de gestión de las amenazas*** y los ***riesgos de la seguridad.***
- Ser **apropiada a las amenazas** a la organización y a la naturaleza y escala de sus operaciones.

La **Política ha de ser realista y concisa, no se puede hacer alardes de una política de gestión de la seguridad con que la empresa no se va a comprometer o cuyos fines sean inalcanzables**

CONTENIDO ADICIONAL DE LA POLITICA DE GESTION DE LA SEGURIDAD

- Definición completa de **objetivos, alcance de la cadena de suministro, declaración de aplicación y programas de seguridad.**
- Establecimiento de la **metodología de evaluación de riesgos** a utilizar y **filosofía de gestión de seguridad** de la organización.
- Definición de las **funciones y responsabilidades**, generales y especificas para la gestión de la seguridad y métodos de **comunicación.**

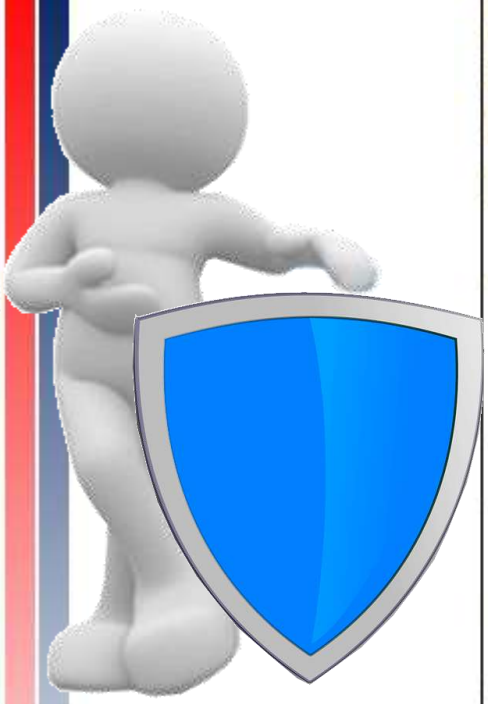
Estructura Típica de la Política de Gestión de la Seguridad

- INTRODUCCIÓN
- COMPROMISO
- DESARROLLO
- RATIFICACIÓN

EJEMPLO DE POLÍTICA DE SEGURIDAD

Estructura Típica de la Política de Gestión de la Seguridad	
Introducción	■ Referencia general a la actividad de la empresa. ■ Reconocimiento de que las actividades de la organización pueden poner en peligro la seguridad en las cadenas de suministro, tanto aguas arriba como abajo. ■ Referencia a otras certificaciones o aprobaciones internacionales obtenidos.
Compromisos	■ Compromisos de la Dirección. ■ Aumentar la seguridad de la cadena de suministro. ■ Mejora continua. ■ Cumplimiento de la legislación aplicable, requisitos legales y reglamentarios, así como otros que la organización suscriba.
Desarrollo	■ Establecimiento de objetivos para alcanzar el logro de los compromisos planteados. ■ Descripción de cómo se llevarán a cabo las correspondientes mejoras en seguridad, atendiendo a la naturaleza de las amenazas a la organización detectadas.
Ratificación	Evidencia del compromiso de la alta Dirección, normalmente representado a través de la firma en señal de compromiso.

Ejemplo de Política de Seguridad



TRANSPORT, S.A., es una empresa dedicada al transporte de mercancías por carretera, en especial mercancías peligrosas.

El objetivo prioritario de TRANSPORT. S.A. es desarrollar nuestra actividad proporcionando unas condiciones adecuadas de seguridad, así como mantener nuestras instalaciones y actividades de acuerdo a la legislación local, autonómica, estatal, cumpliendo con reglamentaciones europeas e internacionales, así como otros requisitos de nuestros clientes y partes interesadas, a la vez que preservamos la seguridad y salud del personal, público y del medio ambiente.

Considerando el contexto económico actual, las amenazas y riesgos a la seguridad que acechan nuestro negocio, hemos adquirido los siguientes compromisos:

- En TRANSPORT S.A., estamos comprometidos a desarrollar nuestras actividades mejorando la seguridad de la cadena de suministro, y a mejorar continuamente nuestras prácticas de gestión de la seguridad, por lo que hemos implantado un Sistema de Gestión de la Seguridad para la Cadena de Suministro conforme a la Norma ISO 28000, aplicable a nuestras operaciones de recepción, transporte, almacenaje y disposición de mercancías, sustentados por esta Política de Gestión de la Seguridad.
- Establecemos objetivos, metas y programas de gestión de la seguridad a corto y largo plazo, y verificamos su aplicación y seguimiento.
- Garantizamos transparencia e información sobre nuestra actividad, poniendo a disposición de las partes interesadas un informe anual con los objetivos conseguidos.

Para ello la alta dirección de TRANSPORT S.A., declara que:

- Contrae el compromiso de mantener un SGSCS, dirigiendo sus esfuerzos a la búsqueda de un mayo nivel de seguridad en nuestro transporte, a través de la mejora continua.
- Proporciona un entorno seguro en todas las operaciones involucradas en la cadena de suministro, incluyendo la protección de nuestros empleados y de la mercancía transportada.
- Cumple con todos los requisitos legales aplicables incluido el Acuerdo europeo sobre transporte de mercancías peligrosas por carretera (ADR) y otros requisitos específicos suscritos por TRANSPORT S.A. en materia de gestión de la seguridad para la cadena de suministro.
- Cumple con los requisitos de la certificación internacional TAPA, *Transport Asset Protection Evaluation,* para el transporte en carretera, utilizando siempre las mejores tecnologías disponibles tanto en nuestros camiones como en los subcontratados.
- Evalúa e identifica todas las amenazas a la seguridad de nuestro negocio, para poder evaluar los riesgos asociados.
- Revisa periódicamente el SGSCS, con el fin de mejorarlo, y adecuar esta Política a las condiciones cambiantes de nuestro entorno.
- Proporciona una adecuada formación al personal, y les incentiva a desarrollar buenas prácticas de seguridad en el trabajo.

DIFUSION DE LA POLITICA DE SEGURIDAD

La difusión de la Política de Seguridad se utiliza como instrumento para fijar los objetivos, metas y programas de seguridad, es decir, la **Política debe convertirse en un objetivo a cumplir**

METODOS DE DIFUSION DE LA POLITICA DE SEGURIDAD

- Entregar una copia de la misma a todos los empleados (por ejemplo en el envío de nóminas)
- Publicarla en posters o carteles en las instalaciones.
- Incluirlas como temas en las reuniones de trabajo
- Incluirla en la formación de los trabajadores
- Publicarla en revistas sectoriales
- Publicarla en la pagina web de la organización.

REVISION DE LA POLITICA DE SEGURIDAD

La Política de Seguridad no es un documento indefinido, tiene una vigencia limitada y ha de ser renovada y actualizada periódicamente

RAZONES PARA LA REVISION DE LA POLITICA DE SEGURIDAD

- Cambios en la demanda de mercado
- Avances Tecnológicos
- Cambios en la estructura global de la empresa.
- Cambios en la propia cadena de Suministro.

OPERADOR ECONÓMICO AUTORIZADO

Muchas Gracias !!

Waleska Lufin Briones
Auditor Senior
wlufin@aduana.cl

OPERADOR ECONÓMICO AUTORIZADO

Mejores Practicas en Seguridad de la Cadena de Suministros

Daniel León
Auditor Senior OEA
Dleon@aduana.cl

Contexto a la gestión de riesgo

Las actuales cadenas de suministros cada vez más globalizadas y complicadas, son mucho más vulnerables que nunca a los desastres naturales y humanos. Las empresas deben flexibilizar sus cadenas de suministros e introducir la gestión del riesgo de interrupción en cada una de sus facetas.

Riesgo

Probabilidad de ocurrencia

Nivel de impacto

¿ Por que tomamos riesgos ?

- Por que es divertido, adrenalina
- Por que queremos ganar mas dinero
- Por que queremos mejorar nuestra reputación
- Emprender un nuevo negocio
- Innovar
- Etc.

=> El que no se arriesga, no gana

=> El que gestiona mejor/antes el riesgo gana más aun.

Análisis de riesgo

Además de la propia identificación del riesgo es importante establecer la **probabilidad** que tiene de ocurrir y la **severidad potencial** de éste en la cadena de suministro.

Una vez que las amenazas y riesgos hayan sido evaluados será el momento de actuar y desarrollar los controles para atenuarlos, reducirlos y/o minimizarlos.

Análisis de riesgo

Tras el proceso de evaluación de riesgos a partir de las amenazas identificadas, cabe esperar procedimientos documentados con la siguiente información:

- **Identificación de amenazas** a la seguridad.
- **Determinación de los riesgos** asociados a las amenazas para la seguridad identificadas.
- **Establecimiento de niveles de riesgo** relacionados con cada amenaza y clasificación en tolerables o no tolerables.
- **Descripción y referencia de las medidas para hacer seguimiento y controlar el riesgo**, en particular para los riesgos que se hayan determinado como no tolerables.
- Cuando sea apropiado, establecimiento de **objetivos de seguridad** y acciones para reducir el riesgo identificado, y actividades de seguimiento y medición de su reducción.
- Identificación de la **competencia y formación** requerida para implementar medidas de control.
- **Medidas de control** necesarias detalladas, como parte del control operacional del sistema.

Registros generados por cualquiera de los procedimientos mencionados.

TOLERABILIDAD DEL RIESGO		Probabilidad		
		Baja	Media	Alta
Severidad	Baja	Trivial	Tolerable	Moderada
	Media	Tolerable	Moderada	Importante
	Alta	Moderada	Importante	Extrema

Que podemos hacer con el riesgo

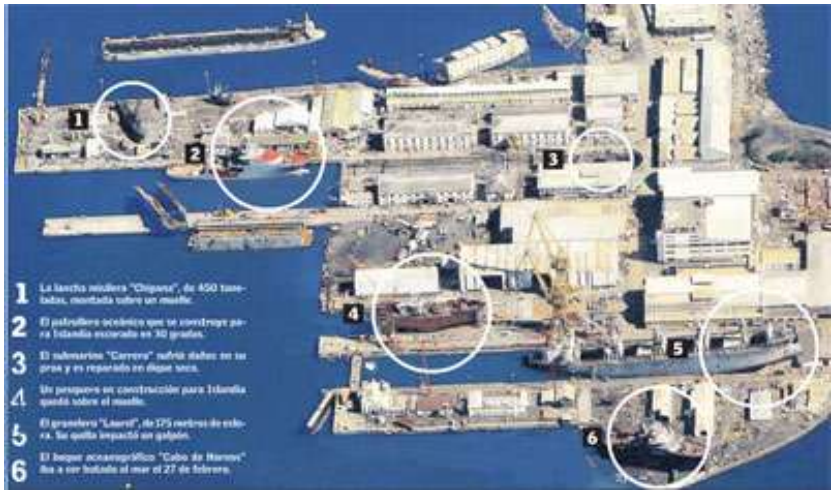
- Mitigar: protección fisica, documental, procedimientos, asignación de responsabilidad única, etc.
- Eliminar: buscar otras alternativas, tomar otras rutas de transporte, otros proveedores, …
- Aceptar: riesgo v/s rentabilidad, modelo de negocios…
- Transferir: condiciones de contrato y poder negociador. Que otro lo gestione.

Caso Asmar, terremoto tsunami 2010

Camino acceso a Asmar

Carencias: luz, agua, caminos, seguridad estructural, seguridad del personal, plan trabajo, objetivos claros, comunicación, etc.

Camino al lugar de trabajo, al interior de Asmar



Caso Nokia vs Ericsson y la triple A

- Las fábrica de Philips en Alburquerque, Nuevo México, sufrió un incendio y se quemó por completo; en ella se producían chips de radio frecuencia para grandes empresas de telefonía móvil como Nokia y Ericsson.

- Nokia
  - Creó inmediatamente un equipo ejecutivo “de placaje” que presionó a Philips para que dedicase otras instalaciones a la fabricación de los chips que necesitaba.
  - Ingenieros de Nokia rediseñaron rápidamente los chips de radio frecuencia para que sus otros suministradores de Japón y Estados Unidos pudiesen fabricarlos”. El plan funcionó:

  “Gracias a las rápidas decisiones tomadas, Nokia fue capaz de cumplir sus objetivos de producción, e incluso aumentó su cuota de mercado del 27 al 30%, un porcentaje que duplicaba al de su rival más cercano”.

- Ericsson
  - reacción con mayor lentitud. Durante semanas la empresa no fue consciente de los problemas en la cadena de suministros; en ese tiempo su capacidad para cumplir con la demanda de los clientes estaba seriamente comprometida.
  - Ericsson, a diferencia de Nokia, dependía exclusivamente de la fábrica de Alburquerque, se encontró con que no tenía nadie más a quién acudir para adquirir dichos componentes

  Las pérdidas anuales de Ericsson alcanzaron los 1.700 millones de dólares, y en última instancia tuvo que subcontratar la propia fabricación de teléfonos móviles a otra empresa”.

Caso Nokia vs Ericsson y la triple A

"Las grandes empresas requieren cadenas de suministros que puedan responden a los cambios repentinos e inesperados, que sean "triple A" ágiles, adaptables y alineadas"

- **Agiles:** responden rápidamente a cambios repentinos en la oferta o demanda, proporcionando información constantemente a los socios de la cadena sobre cambios

- **Adaptables:** ajustan su diseño para adaptarse a los cambios en el mercado. Observar cambios económicos, buscar vendedores de confianza en otros mercados; generar flexibilidad (productos diferentes emplean los mismos componentes y procesos de producción)

- **Alineadas:** establecen incentivos para los socios de la cadena de suministros y así mejorar el funcionamiento de toda la cadena. (ejemplo, proporcionando acceso a pronosticos de ventas y planes; clarificando el cometido y responsabilidades)

Caso de Nissan, terremoto tsunami 2011

Gestión de riesgo “Nuestra filosofía de cadena de suministro es una de vigilancia y extrema capacidad de respuesta alineada con responsabilidad en un solo punto”

- Estructura de la cadena de suministro es descentralizada y regional
- Fuerte control central y coordinación para crisis globales
- Organización flexible que integra varias perspectivas.
  - Gerentes de distintas nacionalidades (gestión directa de problemas y oportunidades en todos sus mercados)
  - Línea simplificada de producción.
  - Algunos SKU se manejan JIT y para otros tiene stock de seguridad
- Rápida/oportuna identificación de riesgos e implementación de contramedidas
- Comité de riesgo define riesgos corporativos y les asigna un responsable, reporte regular a la Directiva.
- Cada división empoderada para mitigar riesgos/efectos cuando no requieren intervención corporativa.
- Plan de contingencia en caso de terremoto
  - Plan prioriza la vida humana, prevención de desastres posteriores, plan rápido de recuperación y continuidad de negocios, apoyo a la comunidad, empresas y gobierno
  - Se designa una oficina central de mando, la cual debe recabar y distribuir información
  - Entrenamiento para terremotos

Reacción post terremoto 2011

- Información y coordinación con todos los representantes de filiales
- Búsqueda de insumos críticos vs reales necesidades de clientes
- Administración de la producción (cuellos de botella, sobreproducción, horas extra, vacaciones)
- Se empodera transitoriamente a la Administraciones locales para que gestiones acciones rápidas de recuperación.

Que determina una gestión de riesgo madura

1.- Administración/gestión del riesgo

2.- Flexibilidad y redundancia en productos, procesos y redes

3.- Alineamiento entre socios de la cadena

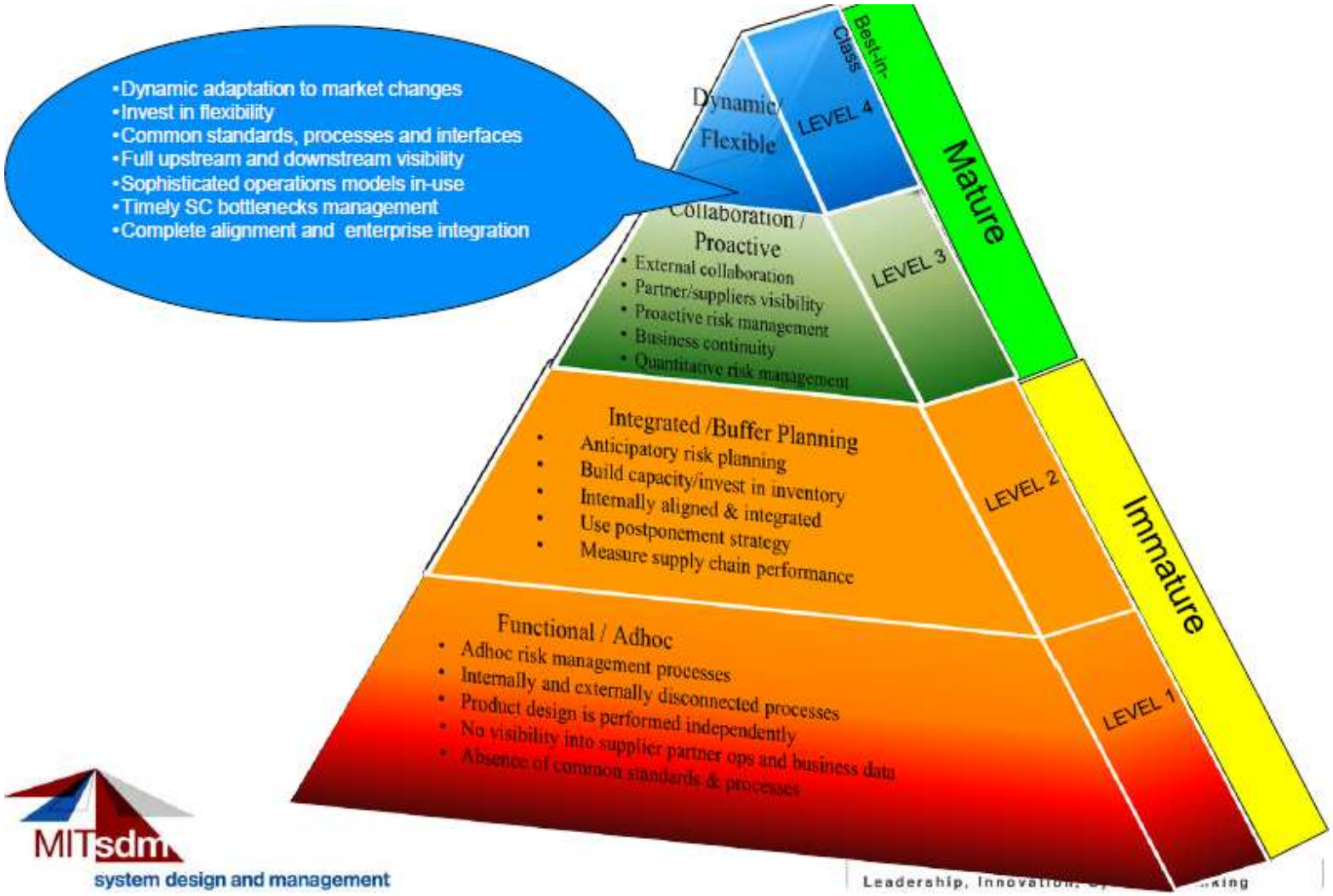
4.- Integración en la cadena, visibilidad, colaboración

5.- Alineación e integración áreas de Negocio

6.- Administración de la complejidad

1. **Risk governance—**the presence of appropriate risk management structures, processes and culture.
2. **Flexibility and redundancy in product, network and process architectures—**having the right levels of flexibility and redundancy across the value chain to be able to absorb disruptions and adapt to change.
3. **Alignment between partners in the supply chain—**strategic alignment on key value dimensions, identification of emerging patterns and advancement towards higher value propositions.
4. **Upstream and downstream supply chain integration—** information sharing, visibility and collaboration with upstream and downstream supply chain partners.
5. **Alignment and integration between internal business functions—** alignment and integration of activities between company value chain functions on a strategic, tactical and operational level.
6. **Complexity management/ rationalisation—**ability to standardise and simplify networks and processes, interfaces, product architectures and product portfolios and operating models.

Niveles de madurez en la gestión de riesgo



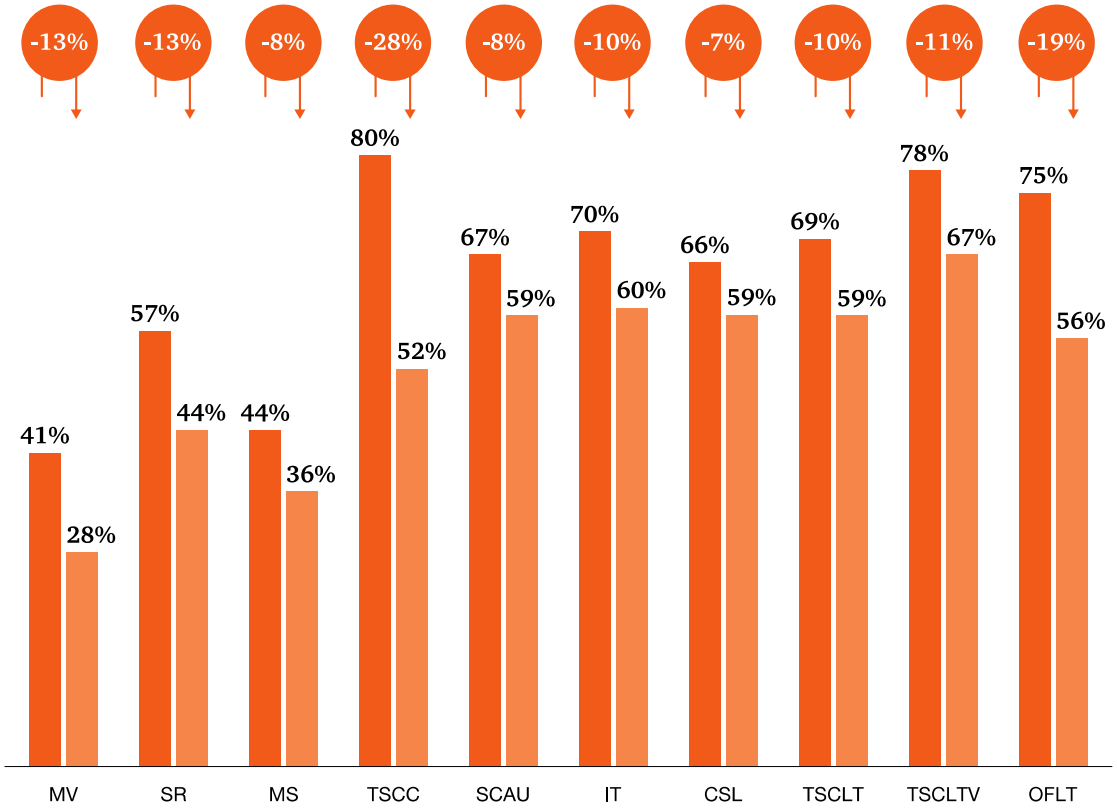
MITsdm
system design and management

Leadership, Innovation, [illegible]king

Niveles de madurez en la gestión de la cadena de suministro y la gestión de riesgo

	Supply chain management	Risk management	
Level I	**Functional** Limited co-ordination between internal functions Resources are locally owned and managed Performance is measured separately based on functional Key Performance Indicators (KPIs) Absence of integrated plans	**Ad-hoc** Ad-hoc risk management processes No visibility into changes outside the functional domain No planning of redundancy buffers towards potential disruptions Can only absorb limited volatility around standard functional input parameters	Less mature
Level II	**Integrated** Information sharing and common planning activities between internal functions Key resources and performance objectives are jointly managed	**Buffer planning** Positioning of redundancy buffers based on a common, cross-functional plan Basic risk governance processes No visibility into emerging changes and patterns outside the company domain	
Level III	**Collaborative** Visibility, information sharing and integration of key activities between supply chain partners Incorporation of external input into internal planning activities Supply chain rationalisation	**Proactive** Use of sensors and predictors to proactively position response mechanisms Business continuity plans Partner resilience monitoring Quantitative risk management	More mature
Level IV	**Dynamic** Alignment on key customer value dimensions across the extended enterprise Supply chain segmentation to match multiple customer value propositions Identification of emerging value chain patterns in complex dynamic environments Ability to adapt the supply chain to frequent changes in the value chain	**Flexible** Investment in flexibility (processes, products, plants, capacity) Management of pressure away from weak partners in the value chain Risk strategy segmentation	

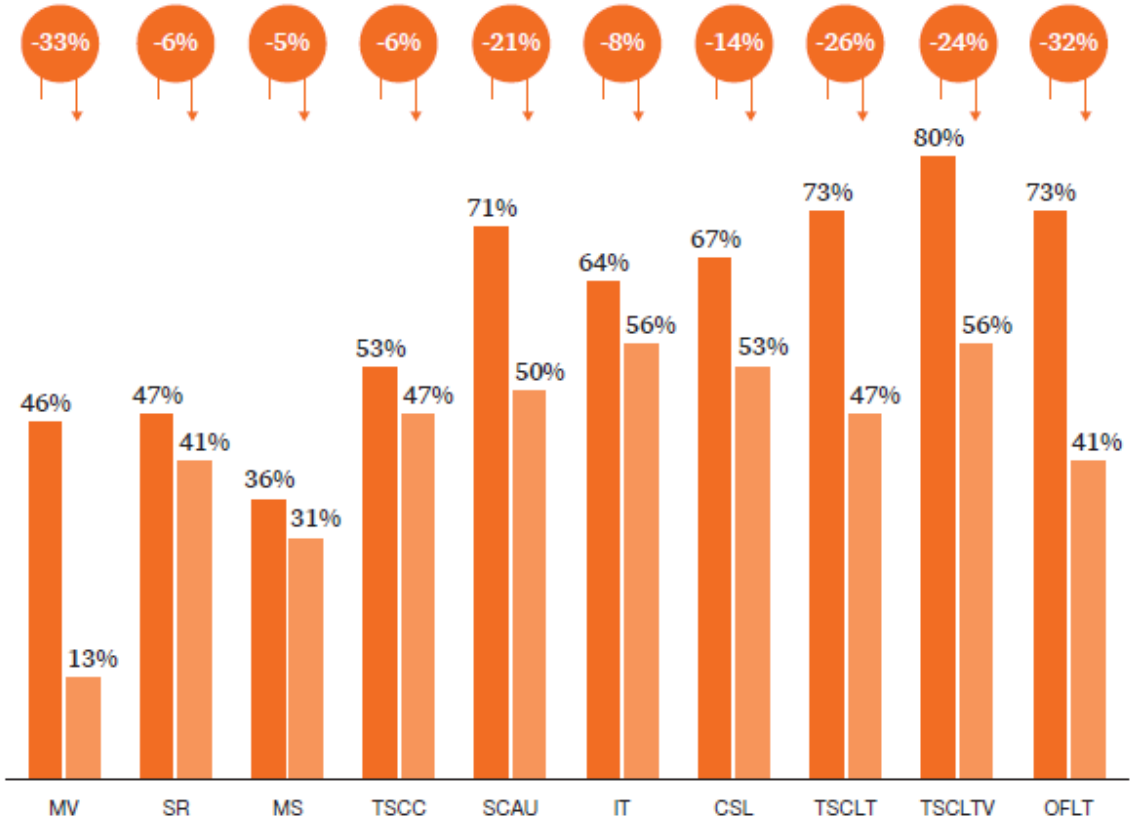
Beneficios de la madurez en la gestión de riesgo



Abbreviation list

MV	Market value	**IT**	Inventory turns
SR	Sales revenue	**CSL**	Customer service level
MS	Market-share	**TSCLT**	Total supply chain lead time
TSCC	Total supply chain cost	**TSCLTV**	Total supply chain lead time variability
SCAU	Supply chain asset utilisation	**OFLT**	Order fulfillment lead time

Niveles de madurez con flexibilidad y sus beneficios



Abbreviation list

MV	Market value	**IT**	Inventory turns
SR	Sales revenue	**CSL**	Customer service level
MS	Market-share	**TSCLT**	Total supply chain lead time
TSCC	Total supply chain cost	**TSCLTV**	Total supply chain lead time variability
SCAU	Supply chain asset utilisation	**OFLT**	Order fulfillment lead time

Conclusiones

- Las interrupciones en la cadena de suministro traen grandes impactos en los negocios, su desempeño financiero y recuperarse toma tiempo (años)
- Las empresas maduras en gestión de la cadena de suministro y gestión de riesgo son mas resistentes a las interrupciones y se recuperan mas rápido y a menor costo.
- Las empresas maduras que invierten en flexibilidad son aun mas resistentes a interrupciones y se recuperan aun mas rápido que el resto.
- La recuperación de un incidente puede representar una ventaja competitiva.
- Las empresas maduras tiene un mejor rendimiento en sus indicadores financiero, operacionales y logístico que el resto.

OPERADOR ECONÓMICO AUTORIZADO

Muchas Gracias !!