Continuidad de Negocios
(ISO 22301:2019)

LOCKTON®

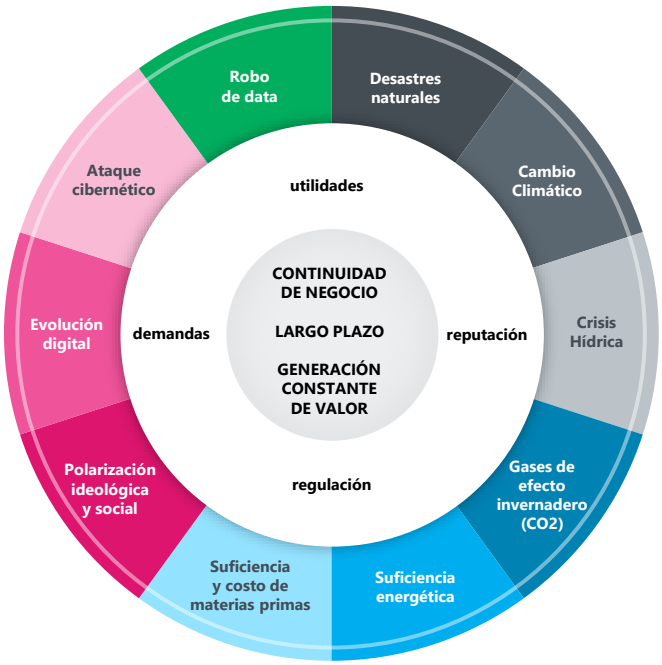
Reto empresarial derivado de cambio constante y disrupción

El ambiente empresarial está en constante cambio y disrupción. Las externalidades (factores externos) son cada vez más recurrentes, e impactan de forma relevante a los negocios.

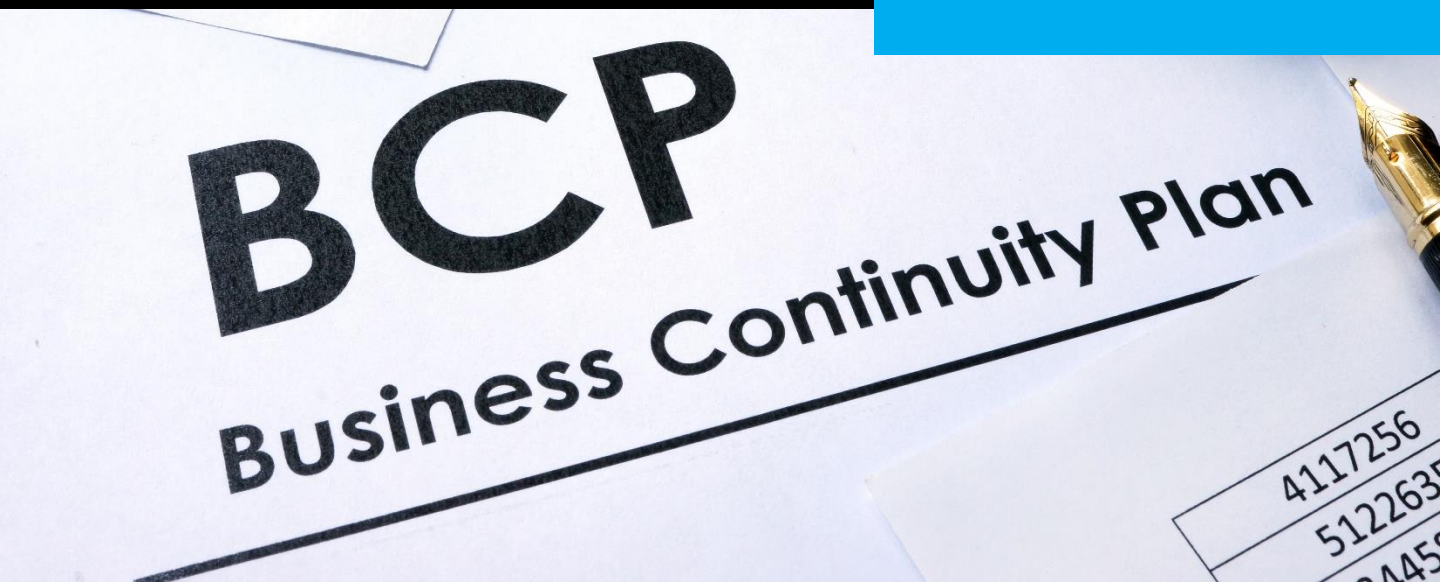
Es común escuchar situaciones inesperadas que impactan a las organizaciones. Los temas son muy variados, desde desastres naturales como huracanes, inundaciones o terremotos, hasta aspectos sociales, como bloqueos y boicot a empresas por el impacto ecológico y social que deriva de la fabricación/distribución de sus productos. Las organizaciones están constantemente expuestas a lo inesperado. Secuestro de la información del negocio, robo de datos y hasta actos de terrorismo a instalaciones y al producto, se han vuelto también una constante.

Factores como el galopante crecimiento demográfico, cambio climático y la imparable transformación digital indican que las empresas se deben ajustar a una "nueva normalidad". Una normalidad en la que la gestión proactiva de sus riesgos, debe ser cultura y constante.

La generación de valor y riqueza es clave, pero también lo es la permanencia y el largo plazo



Evolución y factores de éxito ¿DRP, BCP o BCMS?



Las empresas iniciaron una constante dependencia a la tecnología hace aproximadamente 4 décadas. Como consecuencia, en esos años surgieron los primeros **DRPs** (Disaster Recovery Plan), enfocados primordialmente a la recuperación de sistemas e información. Con el tiempo se observó que la recuperación tecnológica, si bien fundamental, requería otras actividades para lograr reestablecer operatividad. Así nacen los **BCPs** (Business Continuity Plan), que plantean una recuperación considerando aspectos tecnológicos junto con actividades prediseñadas y gente responsable, informada y capacitada para su realización.

En 2012 la "International Organization for Standardization" (ISO) emite su estándar 22031 **BCMS** ("Business Continuity Management System" o Sistema Gerencial de Continuidad de Negocios por su traducción al Español), el cual actualiza en 2019 (**ISO22301:2019**), agregando a su título la definición de "Seguridad y Resiliencia". Se podría decir que la misma es integradora de "todo" lo crítico para la operatividad del negocio, incluyendo procesos, tecnología y estructura orgánica. Lo antes mencionado de forma coordinada y con actividad constante, presente en el día a día de la organización.

Continuidad de Negocios (ISO 22301:2019)

Reto empresarial derivado de constante cambio y disrupción

ISO 220301:2019

Seguridad y Resiliencia – Sistema de Gestión para la Continuidad del Negocio

ALCANCE Y RETOS

Un error recurrente es pensar que un sistema de gestión de la continuidad se activa "únicamente" cuando se presenta una disrupción. En realidad dicho sistema hace referencia a actividades, desarrolladas recurrentemente en la empresa, para mantener operatividad y facilitar la recuperación cuando llegase a ser necesario.

La definición un sistema de gestión de la continuidad, debe ser un traje a la medida de la empresa.

Su empresa debe diseñar e implementar un "Sistema de Gestión de la Continuidad del negocio" buscando valor desde el inicio. Diseñar un sistema únicamente considerando la posibilidad de un evento adverso desconocido, sobre el cual no tiene idea siquiera de cuándo y cómo va a suceder, no sería razonable.

BENEFICIOS

Los beneficios de implementar un sistema de gestión para la continuidad deben estar siempre presentes en la definición del proyecto, y son:

- Viabilidad de seguir operando, de la mejor forma, en caso de un evento inesperado.
- Reducción y gestión de costos por disrupción.
- Protección de la reputación.
- Fortalecimiento de confianza y relacionamiento con grupos de interés, como accionistas e inversionistas.
- Reducción de costos recurrentes, como seguros.
- Cumplimiento regulatorio, para algunas industrias.
- Contribución a la resiliencia de la empresa.

Un plan de continuidad debe generar valor constante y no solo durante una eventual interrupción del negocio

El ISO 22301:2019 “especifica la estructura y requerimientos para implementar y mantener un Sistema de Continuidad de Negocios (BCMS) considerado la cantidad y tipo de impactos que la organización pudiera o no aceptar, en forma posterior a un evento de disrupción”.

El resultado del BCMS debe ser un traje a la medida que deriva de la integración de los siguientes puntos:

Requerimientos operacionales, industriales, legales, reputacionales y regulatorios de la organización.

Sistemas en uso

Productos y servicios otorgados

Tamaño y estructura de la organización

Procesos utilizados

Requerimientos de sus partes interesadas

El BCMS conforme ISO 22301:2019, debe integrar lo siguiente:

1. Una política.
2. Gente calificada y con responsabilidades (responsables de acción, liberación y evaluación).
3. Procesos de gestión con relación a:
    i. Políticas y procedimientos
    ii. Planeación
    iii. Implementación y Operación
    iv. Evaluación de Desempeño
    v. Revisión y liberación de Dirección
    vi. Mejora Continua
4. Formalización de la operación y sus controles que permitan una evaluación futura del desempeño.

La evolución de un BCMS busca – **ASEGURAR una continuidad de la operación** en una razonable integración de Procesos – Gente – Tecnología.

Integra tanto sus plataformas comunes como sus aspectos particulares – como pueden ser diversas localidades o aún modelos de negocio específicos dentro de un grupo.

¿QUÉ NO ES UN BCMS?

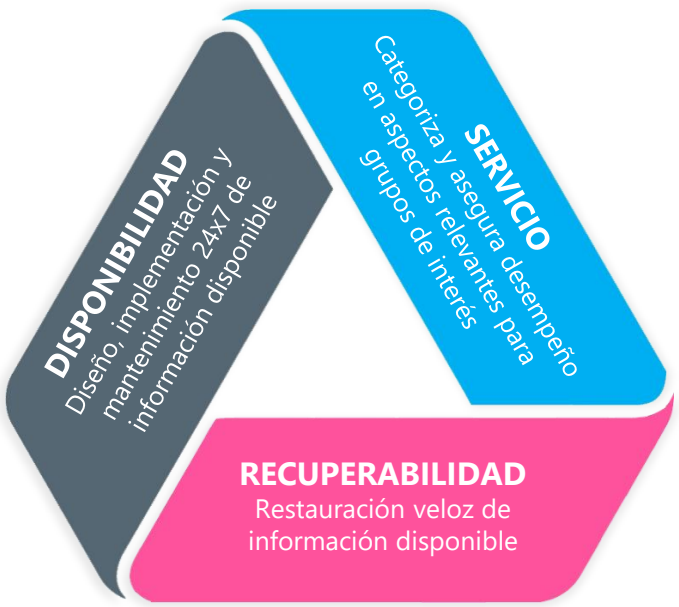
Un Plan de Continuidad de negocio NO busca una recuperación inmediata de todo al instante. Eso sería extremadamente caro, sin relación beneficio, además de ser soberbio, considerando la volatilidad e incertidumbre del mundo de negocios actual.

Un BCMS SI busca, a través de un comprender a la organización y sus aspectos relevantes (Factores críticos de éxito), lograr una reactivación, oportuna y lógica, de aquellas actividades/procesos, con la información suficiente, para operar en el momento requerido y proceder a una recuperación sin dañar aspectos fundamentales para el negocio (internos o externos).

Los sistemas (TI) son importantes en este esfuerzo, sin embargo, son una pieza más de una cadena de valor que necesita de todas sus partes para operar. Específicamente su relación y coordinación tanto con la gente como con los procesos de la empresa.

Finalmente lo que busca un BCSM es tener operatividad, en lo crítico y relevante, para poder continuar:

- Otorgando Servicio.
- Mostrando Disponibilidad.
- En un proceso continuo y constante de recuperabilidad, cuanto hubiera habido una disrupción.



El BCMS bajo ISO 22301:2019 debe partir de un conocimiento del negocio, sus riesgos y sus aspectos fundamentales.

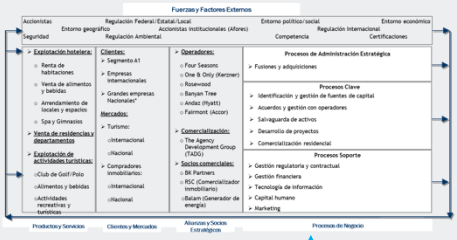
Adicionalmente el ISO 22301:2019 debe integrarse en un plan MAESTRO junto con otros esfuerzos de alto nivel de la organización, como son:

- Gobierno Corporativo.
- Análisis de Impactos de Negocios (BIA – Business Impact Analysis).
- Evaluación de Riesgos (Risk Assessment).
- Marcos de Gestión de Riesgo / Control.
- Marcos de Control en Tecnología de Información.

El estándar ISO 22301:2019 plantea/acepta una correlación con otros de sus estándares como son ISO 9000, ISO 31000 (gestión de riesgos), ISO 27000 (seguridad de la información), ISO 2000 (calidad de servicios TI).

No obliga a cumplir con dichos estándares, pero si se sugiere considerar dichos temas en su análisis. Es un punto de referencia para enfatizar la relevación de correlación de este esfuerzo con la arquitectura de gestión y control del negocio.

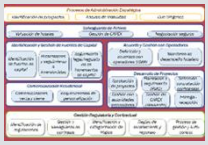
Modelo de Negocio – Factores de Éxito



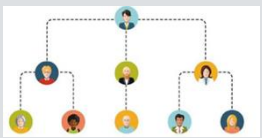
Riesgos – Business Impact Analysis

ISO 22301

PROCESO/ACTIVIDAD/CONTROL



GENTE



TECNOLOGÍA

EXTERNALIDADES DIVERSAS

Riesgos ¿Cómo gestionar lo inesperado?

Un riesgo se puede definir como cualquier obstáculo para el logro de los objetivos de la organización. Por lo tanto y si analiza la frase, las posibilidades de impacto son infinitas. Entonces ¿Cómo gestionar todo lo que puede doler a mi negocio?

Lo primero a considerar es que su empresa NO debe, y seguramente tampoco puede, gestionar todo. Intentar controlar absolutamente todo resultaría en un sistema inviable en su relación costo-beneficio.

Su "Sistema de Continuidad de Negocio" debe lograr balance en una relación de i) impacto potencial y ii) acción a tomar.

Como ejemplo, ¿Cómo controlaría un riesgo de ciberseguridad? ¿Cree que puede tener un blindaje y control absoluto sobre dicho riesgo? Pensemos que su empresa ha sido activa y responsable frente a marcos de control de tecnología y accesos. Sin embargo, ¿Está seguro de que no puede tener un evento de ciberseguridad? A finales de 2020 el Gobierno de los Estados Unidos admitió el acceso no autorizado de terceros a diversas agencias gubernamentales, como la Secretaría del Tesoro y la Secretaría de Comercio. Instituciones que sin duda tienen inversión y cuidado en este tipo de temas. Sin embargo, todo cambia tan rápido que es casi imposible un blindaje total.

Por lo tanto, su marco de gestión de riesgo y control, se sugiere integre y balancee tres conceptos por riesgo.

Mitigación

Acciones que limitan impacto

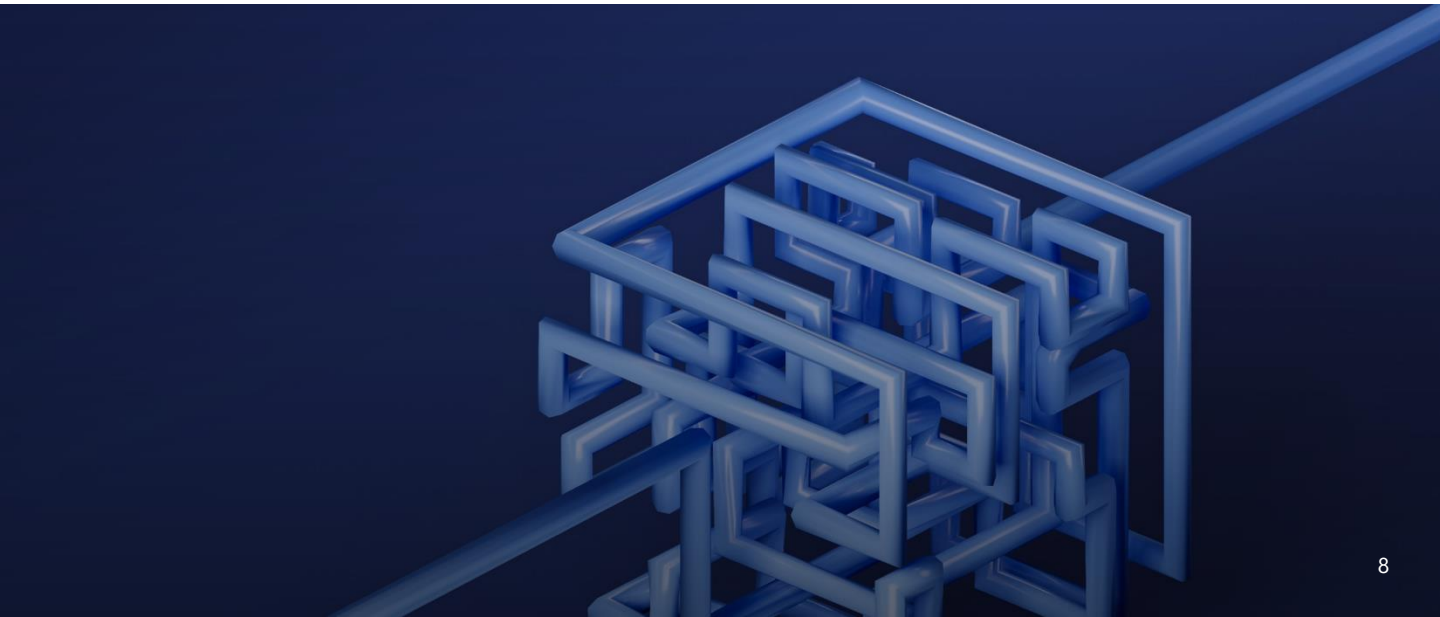
Prevención

Acciones que limitan ocurrencia

Transferencia

Traspaso de riesgo a un tercero – regularmente un seguro – en caso de eventualidad

Los costos y valor de cada acción arriba mencionada puede ser muy diferente. Donde en ocasiones, las empresas aún llegan a mezclar las tres para lograr una gestión de riesgos razonable.



Conclusión

Las empresas hoy operan en ambientes altamente dinámicos y cambiantes. Los factores externos, no controlados por la organización, deben identificarse proactivamente. **Una gestión anticipada de riesgos,** en la mejor relación costo-beneficio, **debe ser parte de la cultura y estructura del negocio.**

Un "Sistema de Continuidad de Negocio" debe considerar como crítico lo siguiente:

a) Es un sistema integral – por lo tanto acciones independientes o separadas no necesariamente darán el resultado esperado cuando fuese requerida su operación.

b) El "Sistema de Continuidad del Negocio" se desarrolló considerando los potenciales riesgos para el negocio (BIA o Business Impact Analysis). Si su identificación y análisis de riesgos es pobre y limitada, es probable que su sistema no esté preparado para una potencial eventualidad.

c) El "Sistema de Continuidad de Negocio" debe ser algo "vivo" en su empresa. Tener únicamente carpeta con procedimientos en espera de alguna eventualidad, no necesariamente le dará resultados.

Si lo analiza, un "Sistema de Continuidad de Negocio" surge por una nueva realidad empresarial. Una realidad con fuerte dinámica y constante cambio. Donde el continuo análisis de lo que pueda doler y en consecuencia como se mitiga, transfiere o reduce, debe estar siempre presente en la visión de los líderes empresariales.

Seguramente su empresa ha desarrollado esfuerzos en control y gestión de temas diversos como tecnología, reputación y otros varios. Le sugerimos que su "Sistema de Continuidad de Negocio" sea un integrador de dichos esfuerzos. Más que un proyecto aislado, un BCMS debe ser una oportunidad de reflexión sobre qué tan preparada está su empresa para lo inesperado.

Una reflexión, con acción, en el constante camino de la resiliencia empresarial.

Risk Consulting

Business Resilience

LOCKTON®

¿Quiénes somos?

Somos el bróker privado más grande del mundo

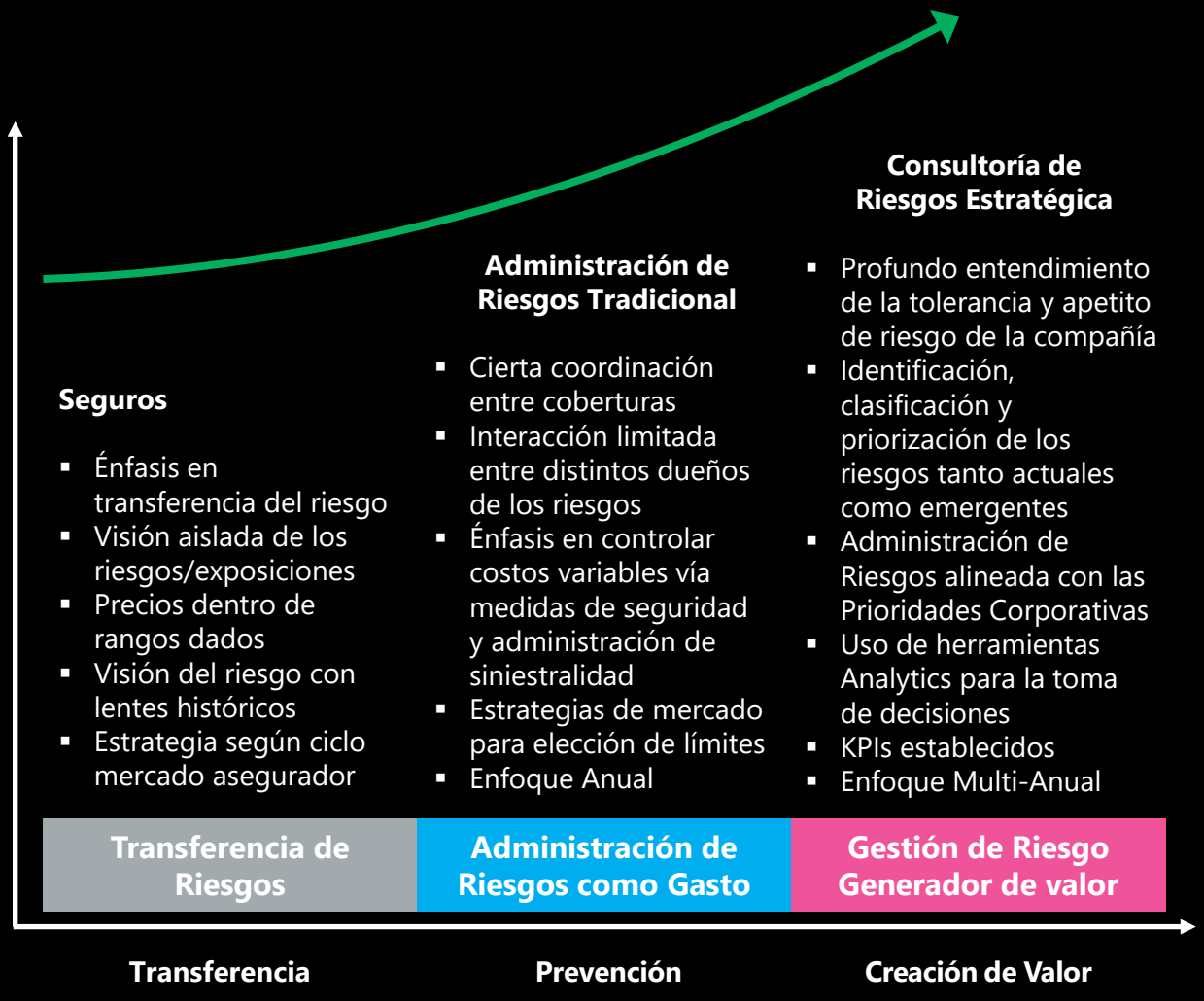
$1.72B	+7,500	+52,000	+100	96%
INGRESOS	COLABORADORES EN EL MUNDO	CLIENTES EN EL MUNDO	OFICINAS EN EL MUNDO	**RETENCIÓN DE CLIENTES**

Risk Consulting

- Somos un equipo de consultoría en riesgos.
- Dedicado a identificar, evaluar, implementar y optimizar programas.
- Para mejorar la gestión de riesgo y capacidad de resiliencia de nuestros clientes.

Evolución de la Administración de Riesgo

Risk Consulting



GESTIÓN DE RIESGOS

PROACTIVIDAD

GENERACIÓN DE VALOR

UNCOMMONLY INDEPENDENT

