



**UNIVERSIDAD DE CHILE
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
DEPARTAMENTO DE INGENIERÍA INDUSTRIAL**

**DISEÑO DE UN MODELO CONCEPTUAL PARA LA GESTIÓN DE LA
CONTINUIDAD DE NEGOCIOS Y RESPUESTA ANTE CRISIS
ORIENTADA A MEDIANAS Y GRANDES EMPRESAS EN CHILE**

**TESIS PARA OPTAR AL GRADO DE MAGÍSTER EN GESTIÓN Y
DIRECCIÓN DE EMPRESAS**

RODRIGO FABIÁN PEDREROS MÉNDEZ

PROFESOR GUÍA:
IVÁN MIGUEL BRAGA CALDERÓN

MIEMBROS DE LA COMISIÓN:
**ANTONIO AGUSTÍN HOLGADO SAN MARTÍN
MANUEL HUMBERTO ROJAS VALENZUELA**

**SANTIAGO DE CHILE
2018**

RESUMEN

DISEÑO DE UN MODELO CONCEPTUAL PARA LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIOS Y RESPUESTA ANTE CRISIS ORIENTADA A MEDIANAS Y GRANDES EMPRESAS EN CHILE

El contexto mundial actual exhibe riesgos y amenazas que aumentan en frecuencia e intensidad, tanto por origen natural como antrópico, e impulsados por fenómenos como la globalización, el cambio climático, y el mayor acceso a nuevas tecnologías. En este escenario, la gestión de la continuidad del negocio por parte de las compañías se vuelve cada vez más importante. El presente trabajo propone un modelo conceptual que destaca los elementos clave de la gestión de la continuidad de negocios y la respuesta ante crisis, dirigido principalmente a empresas medianas y grandes en Chile, con el objetivo de reducir las pérdidas económicas y mitigar el daño en la reputación posible de ocurrencia generando afectación al normal funcionamiento de sus actividades cotidianas.

El presente trabajo, se inicia con la identificación de contexto actual de riesgos y amenazas a nivel mundial expuestas en reportes internacionales, ámbito que permite identificar los principales efectos que una nula o deficiente gestión de la continuidad de negocio ocasiona en las compañías. Esta información se complementa con la descripción de las definiciones conceptuales y la identificación de las principales normas vigentes y guías de buenas prácticas en gestión de riesgos, continuidad de negocios, y gestión de crisis.

En este contexto se planteó un modelo conceptual que integra y prioriza tres elementos clave en la siguiente secuencia: apetito de riesgo – estrategia de preparación y respuesta – evaluación y desarrollo extendido. Se analizan y describen los supuestos sobre los que se basa el modelo, sus beneficios y limitaciones. En esta dirección adicionalmente se identifican los sectores de la economía chilena según prioridad estratégica país, nivel de exposición a riesgos, sumando al contexto regulatorio y legal, para los cuales la aplicación del modelo conceptual propuesto constituye una ventaja competitiva.

Finalmente, se realiza la aplicación del modelo propuesto a un caso real, situación que permite evidenciar que la utilización de los elementos clave del modelo propuesto posibilitan mitigar riesgos y permiten generar un impacto positivo cuantificado en términos de pérdidas evitadas bajo el marco legal y regulatorio en Chile.

DEDICATORIA

Dedico este trabajo a mi esposa Verónica y a mi hija Valentina, bellas inspiradoras de toda mi vida que me han regalado generosamente el tiempo, la motivación y energía necesarias para alcanzar este importante logro personal y profesional

TABLA DE CONTENIDO

1. INTRODUCCIÓN	1
2. OBJETIVOS	2
2.1. Objetivo General	2
2.2. Objetivos Específicos	2
2.3. Hipótesis iniciales	2
2.4. Alcance	3
2.5. Exclusiones de alcance	3
3. METODOLOGÍA	4
4. CONTEXTO	5
4.1. Antecedentes	5
4.2. Marco Conceptual	13
4.2.1. Gestión de Riesgos	13
4.2.2. Continuidad de Negocios	14
4.2.3. Recuperación ante Desastres	15
4.2.4. Gestión de Crisis	15
5. MODELOS Y ESTÁNDARES VIGENTES	17
5.1. BS 31100 (2011) – Gestión de Riesgos	18
5.2. ISO 31000 (2018) – Gestión de Riesgos	19
5.3. COSO Framework	20
5.4. BS 25999 (2007) – Gestión de la Continuidad de Negocios	21
5.5. ISO 22301: 2014 – Sistemas para la Gestión de la Continuidad de Negocios	21
5.6. ISO 27001 (2011) – Gestión de la Seguridad de la Información	22
5.7. NFPA 1600 – Estándar en Gestión de Desastres/Emergencias y Programas de Continuidad de Negocios	23
5.8. BS 12999 (2015) – Gestión de daños	24
5.9. NIMS: National Incident Management System (FEMA, Estados Unidos, 2018)	24
5.10. BS 65000 (2014) – Guía para la Resiliencia Organizacional	25
5.11. ISO 22316 (2017) – Seguridad y Resiliencia	26
5.12. BS 11200 (2014) – Gestión de Crisis (Directrices y buenas prácticas)	27
5.13. Oportunidades de los modelos y estándares existentes	27
6. DISEÑO DEL MODELO PROPUESTO	30
6.1. Supuestos	30

6.2. Las tres claves fundamentales	31
6.2.1. Definir claramente el apetito de riesgo.	31
6.2.2. Priorizar la preparación y respuesta para el peor escenario.	33
6.2.3. Integrar apetito y estrategia de respuesta, iniciando un proceso de evaluación más detallado.	39
6.3. Beneficios e impacto del modelo propuesto	41
6.4. Limitaciones del modelo	45
7. SEGMENTACIÓN DE MERCADO POTENCIAL	47
7.1. Desafíos para las Grandes Corporaciones	47
7.2. Desafíos para las Empresas Medianas	55
7.3 Propuesta segmentos clave para la continuidad de negocios.	58
8. EXTRAPOLACIÓN A UN CASO REAL	62
8.1. Contexto y descripción del caso	62
Figura 27. Nota de prensa crisis Enel	63
Antecedentes relevantes para el análisis.	63
8.2. Contraste a partir del modelo propuesto	64
9. CONCLUSIÓN	68
BIBLIOGRAFÍA	70

1. INTRODUCCIÓN

La gestión de la continuidad de negocio en las empresas empieza a tomar cada vez mayor relevancia, y es especialmente relevante cuando las compañías son proveedoras de bienes o servicios básicos para las personas y para otras actividades productivas de carácter esencial o que incluso han sido declaradas como estratégicas. El cambio climático ha incrementado la frecuencia e intensidad de eventos asociados al clima, mientras que los riesgos de tipo antrópico crecen en la medida que el desarrollo de las sociedades aumenta y, en particular para los de tipo tecnológico, la globalización amplía su poder de alcance. La masificación del uso de redes sociales además permite a los clientes y usuarios expresar en tiempo real su malestar por las pérdidas de continuidad y degradación de los servicios que contratan, transformando rápidamente los problemas de discontinuidad del servicio en crisis comunicacionales y de reputación para las empresas. Los impactos por estos incidentes se concretarán en pérdidas económicas inmediatas y futuras debidas principalmente a la degradación de la calidad de servicio, lucro cesante, insatisfacción de clientes e impacto en la reputación percibida por los *stakeholders*. Además, las empresas que no han previsto ni se han preparado para responder a este tipo de situaciones ven caídas importantes en su productividad debido al desvío de recursos para atender los incidentes y asegurar así la continuidad de manera improvisada sin preparación ni entrenamiento previos. Y debido a la severidad de algunos eventos, incluso aquellas que han previsto planes podrían ver cómo éstos se ven superados obligándoles a enfrentar dificultades mayores que llamamos crisis o catástrofes a las cuales deberán responder con eficiencia y eficacia ya que las consecuencias pueden afectar la continuidad del negocio de tal forma que podría implicar la paralización indefinida de las actividades; en cualquiera de estas situaciones, las pérdidas se traducirán en menor valor para la compañía. Por ello es urgente que las empresas y organizaciones chilenas, de todos los tamaños y sectores realicen procesos sistemáticos de evaluación y mitigación de sus riesgos, y de preparación y entrenamiento frente a eventos que atenten contra la continuidad de sus operaciones o del negocio en su conjunto. La continuidad de negocio y el manejo de crisis va más allá de dar continuidad a los procesos operativos, está referida a asegurar la supervivencia del propio negocio y constituye hoy un instrumento estratégico y de ventaja competitiva para cualquier empresa.

En este sentido, la principal contribución de este trabajo está en proponer un modelo conceptual simple que explique e integre los conceptos de gestión del riesgo, continuidad de negocios y gestión de crisis, de cara a una implementación factible en empresas en Chile, asegurando que los

elementos esenciales de cada uno de estos campos sean considerados apropiadamente.

2. OBJETIVOS

2.1. Objetivo General

Proponer un modelo conceptual integral que facilite la gestión de la continuidad de negocios y la respuesta ante crisis, dirigido principalmente a empresas medianas y grandes en Chile, y que permita reducir las pérdidas económicas y mitigar el daño en reputación que podría producir la afectación en el funcionamiento normal debido a incidentes, emergencias y/o crisis.

2.2. Objetivos Específicos

- a) Proponer un modelo simple que permita una comprensión conceptual de alto nivel pero que contenga los elementos mínimos para una adecuada gestión de continuidad de negocios y respuesta ante crisis en las organizaciones.
- b) Que el modelo constituya una guía con lineamientos generales de aplicación en las fases de preparación, previas a la ocurrencia de algún incidente o crisis.
- c) Que el modelo constituya una guía que facilite la toma de decisiones durante la ocurrencia de un incidente de cualquier tipo y escala.
- d) Proveer de algunos lineamientos clave que permitan la implementación del modelo propuesto y su adecuación de acuerdo a la realidad de la organización.
- e) Estimar los beneficios de implementar el modelo.

2.3. Hipótesis iniciales

Tan relevante como declarar los objetivos con claridad, es mencionar las hipótesis sobre las que se inicia este trabajo, las cuales se pretende validar o refutar en el desarrollo de este documento:

- La comprensión en las empresas acerca de la gestión de riesgos, continuidad de negocios, gestión de crisis, la relación entre estas disciplinas, sus similitudes y beneficios, es parcial o incluso mínima.

- En caso de existir elementos de tal gestión en las empresas, es mayormente escasa, reactiva y focalizada sólo en aspectos que permitan cumplir las obligaciones legales y regulatorias mínimas.
- Incluso para aquellas que poseen cierto nivel de avance, la continuidad de negocios es entendida y gestionada en forma separada de la gestión de crisis mayores o que afectan a la empresa en su conjunto.
- Existe una oportunidad real de desarrollar y/o profundizar los campos mencionados en empresas de tamaño mediano y grandes en Chile, acrecentando su comprensión y alcance.
- Para abordar esta oportunidad, será posible generar más valor cuando se busca cubrir las oportunidades de mejora a través de un enfoque integral, en contraposición a una gestión de riesgos y continuidad de negocios desagregada y focalizada sólo en algunos tipos de amenazas en los ámbitos de seguridad física, informática, riesgo laboral, entre otras.
- Tal propuesta de valor podrá ser percibida de manera favorable por los segmentos target identificados, existiendo disposición a pagar por ello.

2.4. Alcance

El alcance, en función del modelo, considera:

- a) Su diseño a alto nivel
- b) Su desarrollo y explicación de componentes principales
- c) El planteamiento de algunos lineamientos clave para su implementación
- d) La identificación de posibles limitaciones en su aplicación
- e) La identificación de posibles rubros o sectores de la economía dentro de los segmentos Medianas y Grandes Empresas en Chile para los cuales sea beneficioso su aplicación o uso

2.5. Exclusiones de alcance

Es importante mencionar los elementos que el modelo no pretende:

- Recomendaciones para la adquisición y/o implementación de herramientas tecnológicas, plataformas y sistemas para la continuidad de negocios.
- Evaluación financiera de las inversiones identificadas como necesarias para mejorar aún más la resiliencia.
- Identificar los procesos clave de negocio de cara a una certificación de gestión de la calidad.

- Guiar la preparación de una certificación en cualquiera de las normas y estándares internacionales de gestión de riesgos, continuidad de negocios, respuesta ante crisis o resiliencia organizacional.

3. METODOLOGÍA

Para alcanzar los objetivos planteados se utilizó la siguiente metodología y herramientas teóricas:

1. Investigación del contexto actual de amenazas, gestión de riesgos, continuidad de negocios y respuesta ante crisis, tanto en el mundo como en Chile, a partir del análisis de estadísticas contenidas en publicaciones y estudios recientes.
2. Identificación de las principales normas y modelos vigentes en gestión de riesgos, continuidad de negocios y el contexto de su formulación.
3. Identificación de los elementos fundamentales presentes en los modelos identificados, según sus campos de aplicación.
4. Integración de los elementos identificados en el punto anterior, y formulación de un modelo general cuya efectividad pueda ser medida a través de algunos indicadores de gestión.
5. Identificación de segmentos de empresas potenciales para la implementación del modelo, a través de análisis de sectores de la economía, segmentación de empresas, datos secundarios, encuestas y estudios disponibles.
6. Validación de las hipótesis planteadas en el punto 2.3 a través de la revisión de datos e información secundaria disponible.
7. Consolidación de conclusiones y recomendaciones finales.

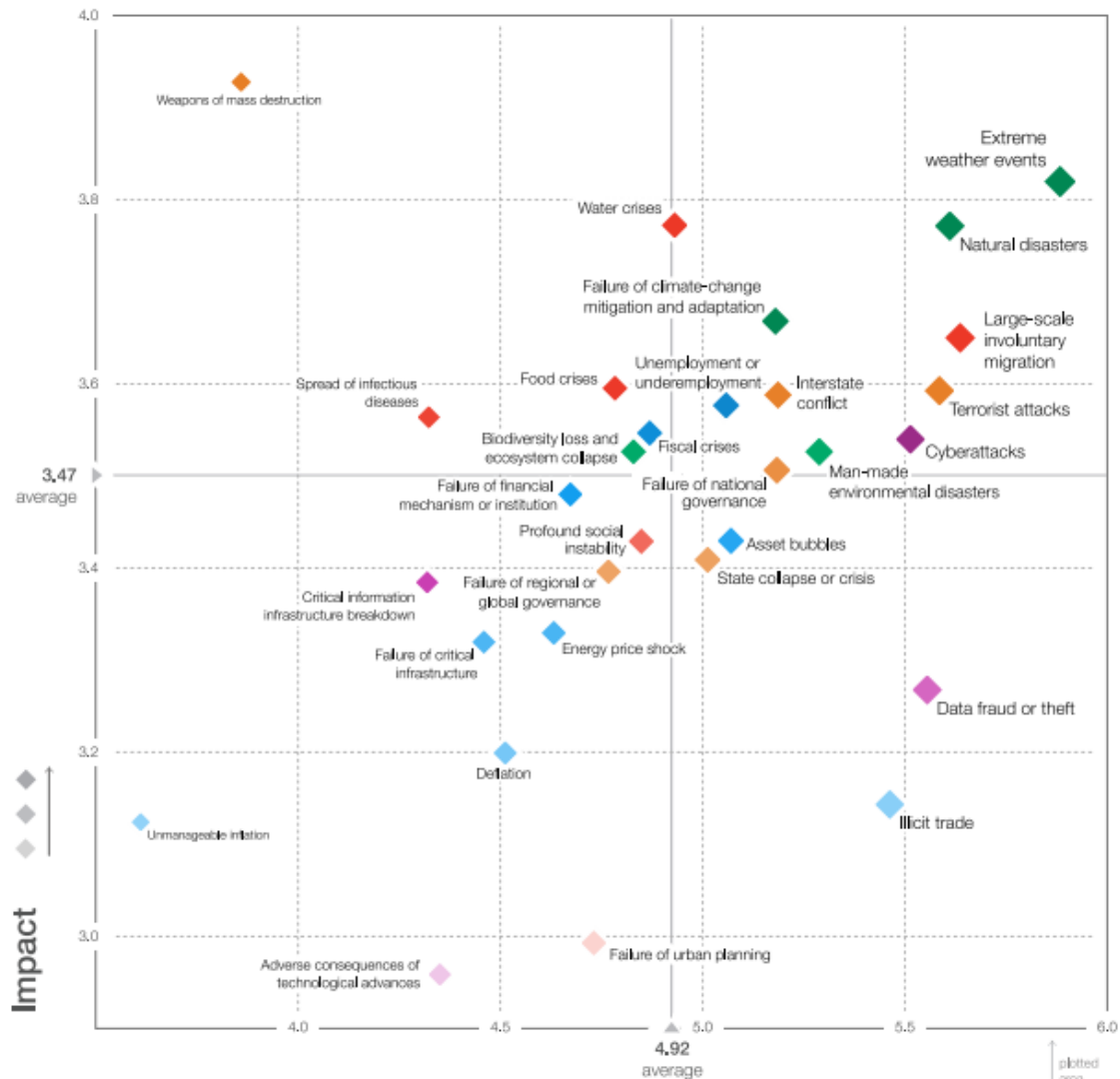
4. CONTEXTO

4.1. Antecedentes

El contexto mundial actual nos muestra que diversas amenazas van en incremento y su propia interacción genera nuevos riesgos para las naciones, sociedades y empresas. Por ejemplo, el cambio climático es uno de los principales factores que ha gatillado un incremento en la frecuencia e intensidad de eventos asociados al clima.

El World Economic Forum en The Global Risk Report 2017 destaca los eventos asociados al cambio climático como "Clima Extremo" y "Desastre Natural Mayor" dentro de los principales en cuanto a probabilidad de ocurrencia e impacto, lugar mantenido sostenidamente los últimos siete años.

Figura 1. Panorama Global del Riesgo 2017





Fuente: The Global Risks Report 2017, 12th Edition, World Economic Forum

De acuerdo al Annual Global Climate and Catastrophe Report 2016 publicado por AON Benfield, sólo en 2016 las pérdidas económicas debidas a desastres naturales a nivel mundial alcanzaron los USD 210 billones, y un 21% superior al promedio de los últimos 16 años de USD 174 billones. Además, factores de tipo antrópico pueden empeorar el impacto de los eventos de origen natural o crear nuevos riesgos: construcciones en sectores con alta probabilidad de derrumbe o de ser afectadas por un aluvión o por en zonas de inundación por tsunamis, deficiencias en mantenciones de infraestructura, entre otros.

Si bien la contratación de seguros podría considerarse una estrategia efectiva de transferencia del riesgo y reducción de las pérdidas, los datos de las últimas décadas indican que sólo un tercio de ellas son cubiertas por aseguradoras, dejando pérdidas netas para las empresas equivalentes a dos tercios del total. Sea debido a un deficiente análisis y transferencia hacia las aseguradoras, o porque los riesgos y oportunidades aún no han sido comprendidas y contempladas por la industria de los seguros, es un análisis que escapa al alcance de este trabajo.

Figura 2. Pérdidas totales vs. pérdidas aseguradas 1970-2017 (Catástrofes Naturales)

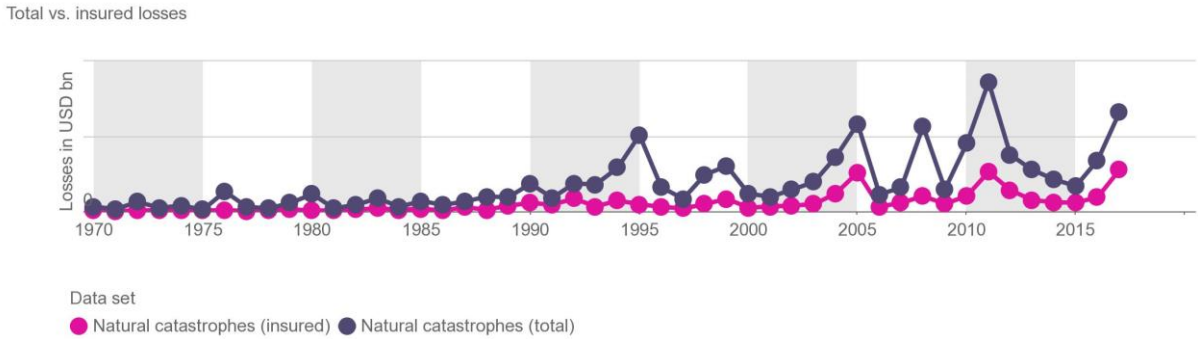


Tabla 1. Pérdidas totales vs. pérdidas aseguradas 1970-2017 (Catástrofes Naturales)

USD bn	avg	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
total	162	58	48	72	97	181	291	56	79	284	73	226	430	187	138	106	84	170	329
insured	51	12	16	19	24	59	129	15	28	50	25	51	131	70	37	30	28	47	138
%	30%	21%	33%	26%	25%	33%	44%	27%	35%	18%	34%	23%	30%	37%	27%	28%	33%	28%	42%

Fuente (figura y tabla): Sigma world insurance satabase 2017, Swiss Re Econocmic Research & Consulting

Figura 3. Pérdidas totales vs. pérdidas aseguradas 1970-2017 (Terremotos)

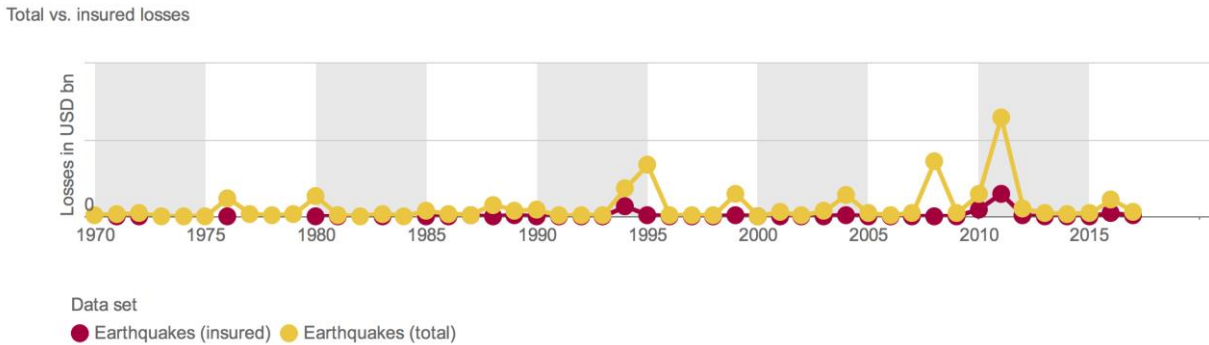


Tabla 2. Pérdidas totales vs. pérdidas aseguradas 1970-2017 (Terremotos)

USD bn	avg	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
total	37	0.7	10	2	13	55	7	4	8	144	7	57	258	19	8	7	7	43	12
insured	5.4	0.03	1	0.01	0.59	3.5	0.3	0.1	0.6	0.4	1	18	59	2	0.05	0.3	0.5	8	1.6
%	9%	4%	10%	1%	5%	6%	4%	3%	8%	0%	14%	32%	23%	11%	1%	4%	7%	19%	13%

Fuente (figura y tabla): Sigma world insurance satabase 2017, Swiss Re Econocmic Research & Consulting

Figura 4. Pérdidas totales vs. pérdidas aseguradas 1970-2017 (debidas al Clima)

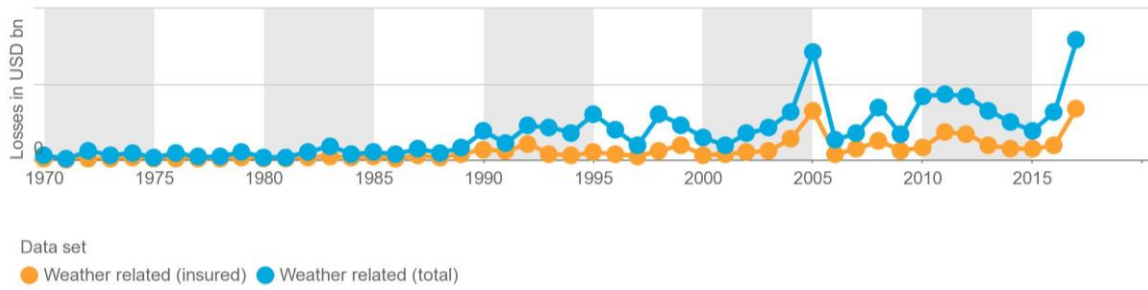


Tabla 3. Pérdidas totales vs. pérdidas aseguradas 1970-2017 (debidas al Clima)

USD bn	avg	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
total	125	58	38	69	84	126	284	52	71	139	66	168	172	168	130	99	76	127	317
insured	45	12	15	19	23	56	129	15	28	49	24	32	72	68	37	30	28	38	136
%	34%	21%	39%	28%	27%	44%	45%	29%	39%	35%	36%	19%	42%	40%	28%	30%	37%	30%	43%

Fuente (figura y tabla): Sigma world insurance satbase 2017, Swiss Re Economic Research & Consulting

Figura 5. Pérdidas totales vs. pérdidas aseguradas 1970-2017 (causas Antrópicas)

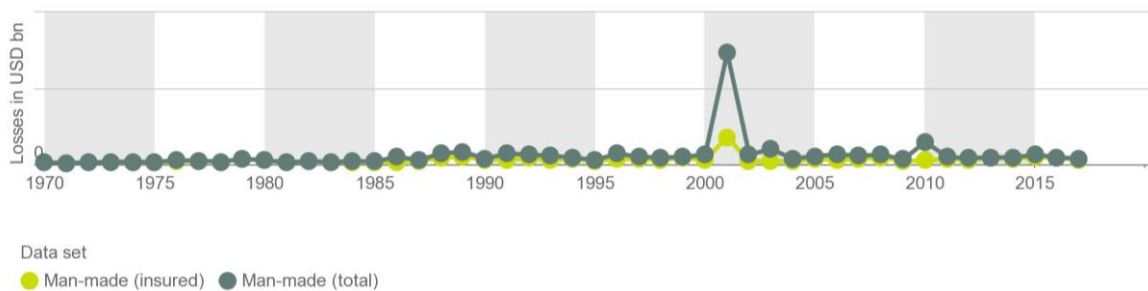


Tabla 4. Pérdidas totales vs. pérdidas aseguradas 1970-2017 (causas Antrópicas)

USD bn	avg	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
total	19	9	12	146	19	7	10	13	11	12	6	29	9	8	9	9	12	9	7
insured	8	8	6	35	4	4	6	6	6	9	4	5	7	6	8	7	9	8	6
%	30%	21%	33%	26%	25%	33%	44%	27%	35%	18%	34%	23%	30%	37%	27%	28%	33%	28%	42%

Fuente (figura y tabla): Sigma world insurance satbase 2017, Swiss Re Economic Research & Consulting

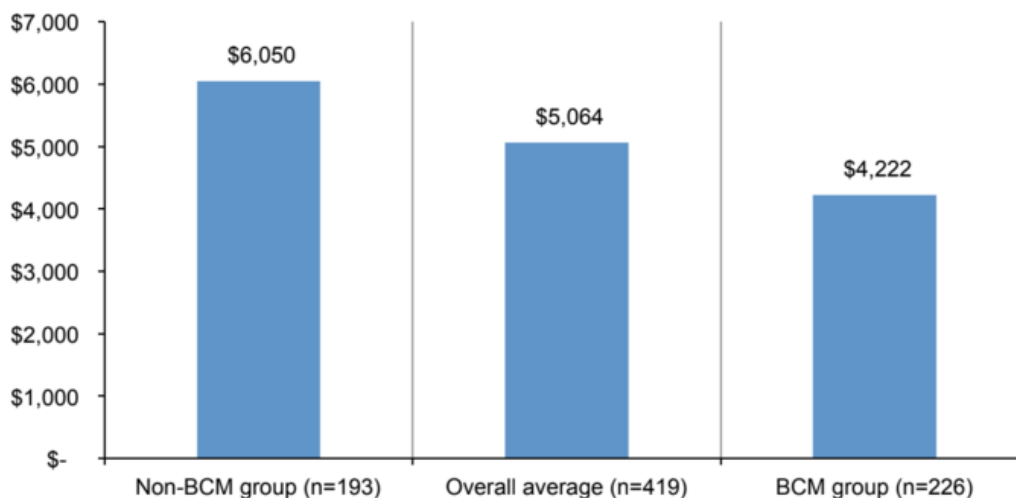
Las cifras anteriores también revelan un crecimiento de más de un 400% en los eventos asociados al clima y los de tipo catástrofe natural.

Por otra parte, el Global Risk Management Survey 2017 realizado por la consultora Aon Banfield a sus empresas clientes en todo el mundo, destacó que de los diez riesgos más destacados sólo cuatro son asegurables con productos de seguros tradicionales. Esto se traduce en que las empresas deben buscar formas de asumir, mitigar y últimamente financiar estos riesgos y sus efectos.

Por su parte, los riesgos de carácter tecnológico no sólo crecen en el mundo, sino que además fenómenos como la globalización y digitalización de los mercados ha favorecido la conectividad e interdependencia entre los distintos agentes, haciendo que el nivel de alcance e impacto de este tipo de riesgos sea cada vez mayor. Ejemplo de ello es el ciberataque mundial del 12 de mayo de 2017 el que se estima pudo costar unos 8 billones de dólares en pérdidas para las empresas a nivel mundial (Cyence, cyber risk modeling firm) explicadas por pérdidas de información crítica e ineficiencias por improductividad, aunque sólo una pequeña fracción de ellas habría sido cubierta por compañías aseguradoras. Por otra parte, el estudio "The 2017 Cost of Data Breach Study: Impact of Business Continuity Management" realizado por Ponemon Institute, concluyó que el impacto de contar con un adecuado programa de continuidad de negocios, permite a las empresas disminuir en un 16,2% el costo por pérdidas de información y datos, reducir el tiempo medio de identificación de un incidente de pérdida de información, y reducir en un 28,4% la probabilidad de ser expuesto a tal evento en los próximos dos años. Como ejemplo de ello, la siguiente gráfica derivada de este estudio muestra que aquellas compañías que gestionan formalmente la continuidad de su negocio pueden estar expuestas a costos por pérdida de datos por día un 30% inferiores respecto de aquellas que no la realizan.

Figura 6. Costo por día para compañías con y sin Gestión de la Continuidad del Negocio

Consolidated view (Overall n=419; BCM group=226; non-BCM group=193)
Measured in US\$



Fuente: "The 2017 Cost of Data Breach Study: Impact of Business Continuity Management", Ponemon Institute

Estadísticas internacionales también indican que el 80% de las empresas desaparecen luego de 18 meses de haber sido afectados por un incidente mayor (The Axa Report, 2007), mientras que el 50% de las empresas que pierden su información a causa de desastres desaparece inmediatamente, y el 93% lo hace en un año (USDOL, United States Department of Labor)

Debido a su ubicación geográfica y extensión, Chile es un país expuesto a eventos principalmente de tipo natural pero también antrópico, que tienen una alta probabilidad de transformarse en incidentes, desastres o crisis reales para las empresas: todos los años el país sufre al menos un sismo superior a 6 grados Richter con riesgo de tsunamis, diversos eventos climáticos en zonas precordilleranas y valles con caída de lluvia que superan los registros históricos, además de múltiples focos de incendios forestales durante los meses de mayor temperatura y menor humedad atmosférica. En Chile las catástrofes naturales han generado pérdidas promedio anuales por USD2.838 millones y sólo en el periodo 2005-2013 alcanzaron USD3.143 millones.

El crecimiento en la cantidad de eventos por año en Chile es evidente, a lo cual debemos sumar que la globalización expone a las empresas chilenas a nuevos riesgos como el ciberataque del 12 de mayo de 2017, produciendo con ello un incremento en las pérdidas verificadas por empresas debidas a una deficiente previsión y preparación. Según el ESET Security Report 2017 para Latinoamérica, las principales amenazas informáticas para empresas

grandes y medianas al malware, fraudes y vulnerabilidad de software y sistemas, y el acceso indebido a la información. Cualquier evento de estas características puede costarle a una pequeña y/o mediana empresa alrededor de USD 86.500, mientras que a una gran empresa unos USD 861.000 (Corporate IT Security Risks 2016) Además, reportes de Panda Security indican que el 43% de estos ataques a nivel global se concentran en los segmentos de empresas pequeñas y medianas.

Un Estudio del año 2016 del Observatorio del Comercio Ilícito en Chile reveló que el 34% de las Pymes de Santiago, Valparaíso y Concepción ha sido víctima de ciberataques, y un 40% en el caso de empresas medianas. El estudio reveló además que sólo el 44,8% de estas empresas descubrieron los intentos de ciberataques gracias a mecanismos de defensa tan simples como mantener el antivirus actualizado o utilizar un software licenciado.

Chile además es uno de los países que ha firmado el Marco de Sendai (2015-2030) y la Política Nacional para la Gestión del Riesgo de Desastres, los que promueven una Gestión del Riesgo de Desastres basado en principios tales que le den una connotación integral, prospectiva y participativa, es decir, integrando a todos los actores relevantes - públicos, privados, académicos y de la sociedad civil.

Estos antecedentes demuestran que la pérdida de continuidad puede llevar a empresas de todos los tamaños y sectores a problemas operacionales y económicos serios, que pueden derivar en una paralización extendida y finalmente el cierre de la compañía. El problema es particularmente serio en empresas medianas y pequeñas, las cuales no pueden estar dispuestas a arriesgar el perder grandes sumas de dinero por eventos de diversa frecuencia de ocurrencia e impacto, sobre todo cuando el crecimiento y acceso a vías de financiamiento son sus principales focos.

También sería importante validar si las empresas en Chile abordan la gestión del riesgo de manera desagregada y sólo en la medida que la legislación y regulación vigente les exige, y no como un factor que les permita competir y crecer tanto en los mercados local e internacional. Es posible que la gestión de riesgos y continuidad de negocio sea tratada y contratada según el tipo de amenaza a enfrentar, de manera fragmentada y granular principalmente a:

- Proveedores de servicios de Tecnologías de la Información para ejecutar medidas de protección y mitigación informática
- Mutuales para hacerse cargo de los riesgos ocupacionales y de salud en el trabajo
- Empresas de seguridad para abordar los incidentes de seguridad física como asaltos y robos de mercancías
- Diversas consultoras de mejora de procesos y gestión de la calidad
- Expertos, asesores y consultores particulares

Ello abre un espacio a desarrollar enfoques integrales de gestión de continuidad de negocios y respuesta ante crisis, con un enfoque que aborde no sólo desde la perspectiva de incidentes menores, sino que también la respuesta frente a grandes emergencias, crisis o catástrofes, independiente del riesgo o amenaza que lo haya originado.

Además, estos antecedentes sugieren que la continuidad de negocios puede considerarse un factor de ventaja competitiva y respaldo frente a clientes (contratos) y frente a la ley. También puede ser garantía frente a compañías de seguros dando mayor poder de negociación a la empresa para la obtención de menores costos en primas y frente a la banca para acceder a financiamiento. Garantizar continuidad en el negocio es garantizar eficiencia y productividad, al evitar pérdidas gestionables al menos parcialmente además del desvío de recursos para la vuelta a la normalidad durante mucho tiempo por no contar con medidas de mitigación y planes de respuesta adecuados. Esto puede considerarse además un antecedente de profesionalismo y seriedad principalmente para empresas pequeñas y medianas en Chile, tanto de cara al mercado local como al internacional.

En Chile se encuentra muy poco penetrada la cultura de prevención de riesgos y preparación frente a cualquier tipo de incidentes (emergencias, desastres, crisis, catástrofes) aun cuando somos un país expuesto principalmente a desastres naturales. Como se expondrá más adelante, pocas empresas en Chile poseen áreas dedicadas a la gestión de continuidad y éstas son principalmente grandes empresas de sectores regulados, las que además sólo cuentan con algunas certificaciones en normas internacionales en algunos de sus procesos más relevantes (British Standard, ISO, NFPA) Tampoco existen en Chile organismos dedicados a regular la continuidad operacional.

Sin embargo, el marco normativo está cambiando en el mundo y Chile no es la excepción. Las nuevas regulaciones que se vienen tendrán un gran impacto en la industria local. Las compañías deberán adoptar una cultura de riesgos que cambie su estructura organizativa y aplicar prácticas de gestión que, en muchos casos, van más allá de sus conocimientos técnicos.

A nivel de sectores de la economía en Chile, particularmente relevantes son aquellos sectores para los que:

- La legislación y/o regulación vigente exige un estándar mínimo de estabilidad, continuidad y respuesta, por ejemplo, aquellos que por su naturaleza soportan infraestructura y procesos críticos para el funcionamiento normal del país (vialidad, telecomunicaciones, transporte, salud, seguridad, servicios financieros, entre otros)
- Proyectan modificaciones en términos de mayor rigurosidad regulatoria o legislativa. Ejemplos de ello son los proveedores de empresas de

servicios básicos o de empresas estratégicas, que en la actual discusión sobre la legislación laboral han sido declaradas como empresas estratégicas obligando a asegurar sus servicios mínimos (para la supervivencia del negocio) y profesionalizar sus equipos de emergencia, lo que refuerza la relevancia de la continuidad de servicios no sólo para estas empresas y sus recursos internos, sino que también para sus proveedores.

- Sean rápidamente requeridos al decretarse el estado de emergencia o excepción por la autoridad, debiendo responder en forma inmediata con presupuestos adicionales aprobados para estos fines tanto para atender las necesidades de la autoridad, comunidad y otras empresas. Ejemplo de ello son empresas del sector combustibles y energía, transportes terrestre y aéreo, equipamiento de seguridad para equipos de respuesta, alimentos, entre otros.

Todos estos antecedentes sugieren que existe una oportunidad importante de desarrollar y/o reforzar la gestión de riesgos y de continuidad de negocios en las empresas chilenas de todos los sectores y tamaños y que, al someterlas a daños e impactos que se materializan en pérdidas económicas, podría ser una necesidad permanente en cualquier empresa.

4.2. Marco Conceptual

A continuación, se describen algunas definiciones principales derivadas de las normas vigentes relacionadas con el alcance de esta tesis en términos de gestión de riesgos, continuidad de negocios y respuesta ante crisis.

4.2.1. Gestión de Riesgos

Cualquier evento puede tener un impacto negativo, positivo o ambos. Eventos con un impacto negativo representan riesgos que pueden evitar la creación de valor o erosionar el valor existente. Oportunidad es la posibilidad de que un evento ocurrirá y afectará positivamente el cumplimiento de objetivos (Fuente: COSO Framework, 2004)

Un riesgo puede definirse como "el efecto de la incertidumbre en la consecución de objetivos" (Fuente: ISO 31000:2009) de lo que se desprende que un "efecto" será cualquier desviación respecto a la situación esperada (positiva o negativamente) Desde un punto de vista económico, todos los agentes de la economía incluyendo el Estado, las instituciones públicas, la comunidad y las empresas privadas están sujetos a diversos tipos riesgos. El

riesgo cero no existe, y cualquier actividad siempre estará sujeto a amenazas o riesgos de tipo natural, antrópico, tecnológico, etc. y contará con cierto nivel de vulnerabilidad intrínseco a tales riesgos.

Es por ello que, para no quedar a merced de la incertidumbre, los riesgos a nivel empresarial deben gestionarse. En este contexto surge el concepto de Gestión o Administración de Riesgos definida como "una serie de actividades y métodos coordinados utilizados para dirigir una organización y controlar los muchos riesgos que pueden afectar su capacidad de alcanzar los objetivos" (ISO 31000:2009) Esta misma norma indica que "la gestión del riesgo contribuye de manera tangible al logro de los objetivos y a la mejora del desempeño, por ejemplo, en lo referente a la salud y seguridad de las personas, a la conformidad con los requisitos legales y conformidad con los requisitos legales y reglamentos, a la aceptación por el público, a la protección ambiental, a la calidad del producto, a la gestión del proyecto, a la eficacia en las operaciones, y a su gobierno y reputación", y hace referencia a tres estrategias fundamentales de gestión del riesgo:

1. Eliminar: implica no realizar o evitar la actividad, proceso, decisión sujeta a riesgo de forma de evitarlo completamente. Para ello existen metodologías de Risk Avoidance cuyo objetivo es desviar completamente la mayor cantidad de amenazas posible y evitar sus efectos o consecuencias. Sin embargo, siempre existirá un nivel de riesgo inherente a cualquier actividad, por lo que no siempre se podrá eliminar completamente la amenaza de un riesgo.
2. Transferir: que un tercero asuma parte o todo el riesgo, de lo cual surgen principalmente las estrategias de contratación de seguros.
3. Reducir: tomar medidas que permitan mitigar el riesgo reduciendo la probabilidad de ocurrencia o el impacto que pueda producir.

Una premisa fundamental para la administración de riesgos empresariales es que cualquier entidad o compañía existe para entregar valor a sus *stakeholders*. Y dado que toda entidad debe enfrentar incertidumbre en todo su actuar, el desafío está en determinar cuánta incertidumbre aceptar para hacer crecer el valor para sus *stakeholders*. Es por ello que la gestión de los riesgos empresariales incluye la determinación fundamental del apetito de riesgo que es la cantidad y tipo de riesgo para el cual una organización está preparada para aceptar, tolerar o perseguir (ISO 22301: 2012)

4.2.2. Continuidad de Negocios

La gestión de la continuidad de negocios se define como un proceso holístico de gestión para asegurar que las operaciones continúan y que los productos y servicios son entregados bajo niveles predefinidos, que la marca y las

actividades que crean valor están protegidas, y que la reputación y los intereses de los *stakeholders* clave están protegidos cuando sea que un incidente disruptivo ocurra. Esto es alcanzable identificando las amenazas potenciales, analizando posibles impactos, y tomando medidas para construir resiliencia organizacional (un proceso holístico es aquél que enfatiza la importancia del proceso en su conjunto y la interdependencia de las partes que lo conforman) (Fuente: ISO 22301:2012)

Además, la continuidad de negocio busca tener un plan para enfrentar situaciones difíciles, de manera que la organización pueda continuar funcionando con la menor disrupción posible (Fuente: Business Continuity Institute)

4.2.3. Recuperación ante Desastres

Por su parte la recuperación ante desastres es descrita como una serie de estrategias y planes de recuperación y restauración de las organizaciones en términos de infraestructura tecnológica y capacidad después de una interrupción grave (Fuente: NFPA 1600)

La recuperación ante desastres es un concepto que nace en el mundo informático como el proceso de guardar y almacenar datos con el simple propósito de poder recuperarlos luego de un evento de desastre, y corresponde a una parte dentro de todo el campo de Continuidad de Negocios.

(Fuente: <http://www.datacenterknowledge.com/archives/2013/01/04/disaster-recovery-is-not-business-continuity>)

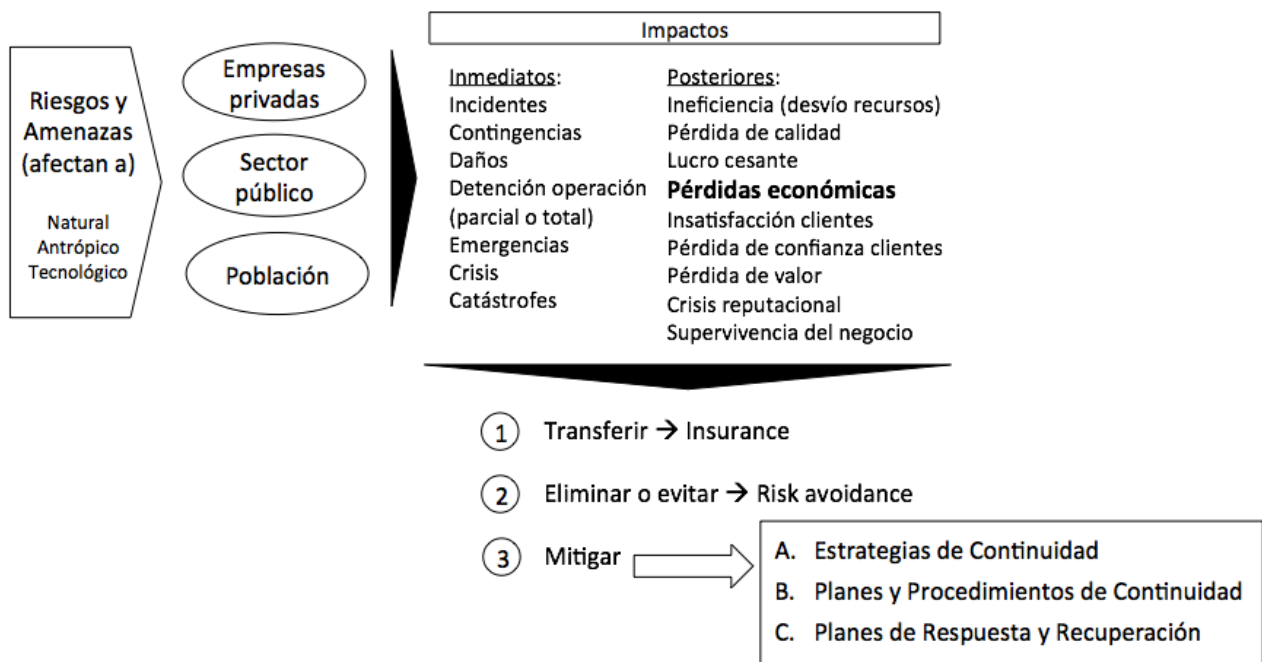
4.2.4. Gestión de Crisis

Es el proceso por el cual una organización enfrenta un evento disruptivo e inesperado que amenaza con dañar a la organización o a sus *stakeholders*. La capacidad de administrar las crisis es uno más de los aspectos de una organización resiliente. La resiliencia requiere de una gestión de crisis efectiva, la cual requiere ser comprendida, desarrollada, aplicada y validada en el contexto de un rango de disciplinas relacionadas con la gestión del riesgo. Estas incluyen la gestión del riesgo, de la continuidad de negocios y la seguridad. La gestión de crisis no puede simplemente ser postergada hasta que una organización sea golpeada por una crisis, esperando que ella nunca ocurra. Requiere de un enfoque sistemático y con visión de futuro que crea estructuras, entrena a las personas y es evaluado y desarrollado en

forma continua, rigurosa y significativa. El desarrollo de las competencias para la gestión de crisis necesita ser una actividad regular y que es proporcional al tamaño y capacidad de una organización (Fuente: BS 11200, 2014)

A modo de resumen, el siguiente diagrama grafica el panorama de gestión de riesgos, continuidad de negocios y crisis sobre la base de las definiciones anteriores:

Figura 7. Panorama general de Gestión de Riesgos, Continuidad de Negocios y Crisis



Fuente: Elaboración propia

- Riesgos y amenazas de tipo natural, tecnológico o antrópico afectan a la población, y las organizaciones de cualquier tipo no se encuentran exentas a esta realidad.
- Estos riesgos pueden materializarse en impactos de corto plazo, generalmente mencionados como incidentes, contingencias, pérdidas de continuidad, emergencias, crisis o catástrofes. Y en el largo plazo se traducen finalmente en pérdidas económicas derivadas de diversas fuentes: ineficiencia por desvío de recursos para atender los incidentes, degradación en la calidad de los productos/servicios, lucro cesante, empeoramiento de los tiempos de entrega, clientes insatisfechos, pérdida de confianza de *stakeholders*, degradación de la reputación y valoración de marca y, finalmente, arriesga la supervivencia de la organización.

- La forma de abordar o gestionar estos riesgos es a través de 3 estrategias fundamentales: transferir, evitar, mitigar.
- En particular, las estrategias de mitigación pueden ser concretadas en estrategias, planes y procedimientos de continuidad, respuesta y recuperación.

5. MODELOS Y ESTÁNDARES VIGENTES

Una revisión general del panorama de normas y estándares internacionales asociados a gestión de riesgos, continuidad de negocios y respuesta ante crisis, arroja los siguientes hallazgos:

- Estándares Británicos, agrupados en el British Standard Institute (BSI)
- Normas y certificaciones creadas por la International Organization for Standardization (ISO)
- Estándares Norteamericanos y de otras fuentes

La siguiente tabla resume algunos de los estándares principales en cada uno de los ámbitos mencionados y si es posible certificar empresas y procesos o sólo sirven como manuales y guías de buenas prácticas:

Tabla 5. Resumen de estándares y guías

Campo	Norma o Estándar	Condición de certificación
Gestión de Riesgos	BS 31100 (2011) ISO 31000 (2018) COSO Framework	Código de buenas prácticas Certificable Certificable
Gestión de Continuidad de Negocios	BS 25999 (2007) ISO 22301 (2014) ISO 27001 (2011)	Certificable Certificable Certificable
Respuesta ante Emergencias e Incidentes	NFPA 1600 (2012) BS 12999 (2015) NIMS, Fema	Guía de buenas prácticas Código de buenas prácticas Guía de buenas prácticas
Crisis y Resiliencia	BS 65000 (2014) ISO 22316 (2017) BS 11200 (2014)	Guía de buenas prácticas Certificable Guía de buenas prácticas

Fuente: Elaboración propia

5.1. BS 31100 (2011) – Gestión de Riesgos

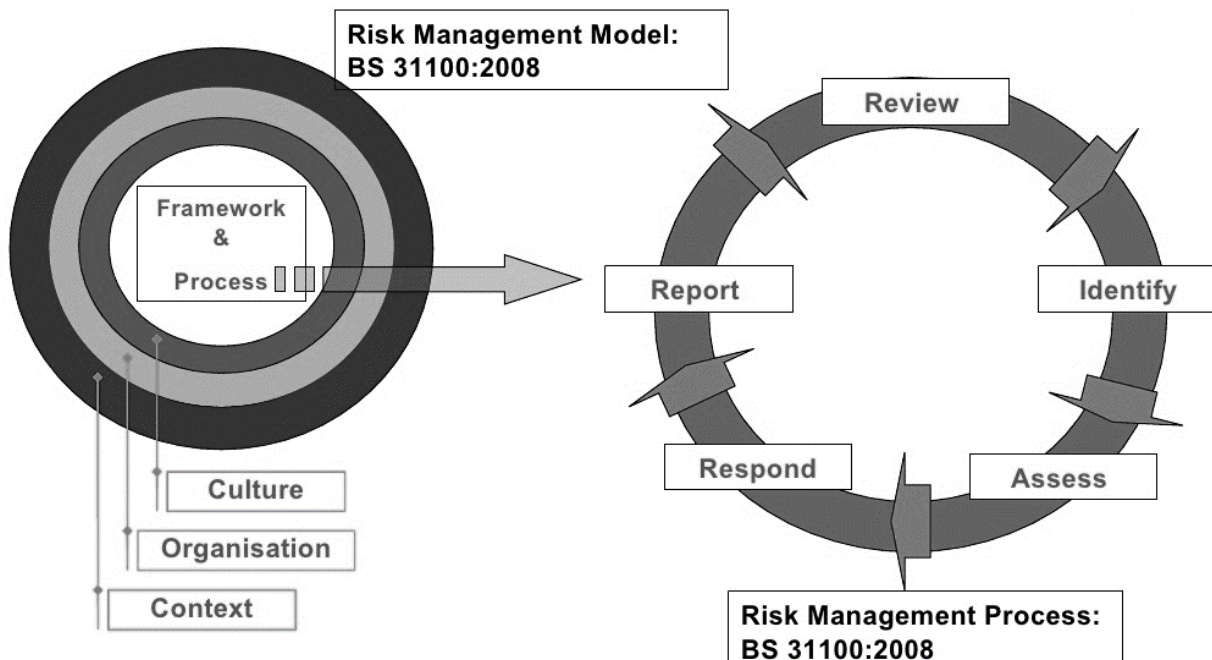
Describe un proceso de gestión del riesgo que puede ser usado e interpretado de tal forma que cada grupo dentro de la organización trabaja de una manera que incrementa la consistencia y comunicación en todo el negocio.

Basada en el consenso de los expertos del comité británico de gestión del riesgo, esta norma provee recomendaciones prácticas y específicas en cómo implementar los principios clave específicamente a la medida de la organización.

La BS 31100: 2011 está basada en la información disponible más actualizada en gestión del riesgo y puede actuar como una parte integral de todos los procesos organizacionales facilitando la mejora continua del negocio. Provee recomendaciones específicas y prácticas sobre cómo implementar los principios clave de la gestión del riesgo tal como se especifica en ISO 31000.

El siguiente diagrama ilustra los principios clave planteados por la BS 311000 para una adecuada gestión del riesgo: Revisar – Identificar – Evaluar – Responder – Reportar.

Figura 8. BS 31100 (2011) framework



Fuente: BSI Group.

5.2. ISO 31000 (2018) – Gestión de Riesgos

Es un estándar internacional genérico de gestión del riesgo, que sugiere una serie de lineamientos descritos en las siguientes secciones: Principios de gestión del riesgo; Marco para la gestión del riesgo; Proceso de gestión del riesgo.

Esta norma reconoce que las organizaciones operan en un mundo incierto. Cualquiera sea la forma que éstas traten de alcanzar un objetivo, existirá siempre la probabilidad de que las cosas no ocurran de acuerdo a lo planeado, y cada paso que se dé en alcanzar un objetivo involucra incertidumbre y riesgo, el cual debe ser gestionado. De acuerdo a esta norma, es posible reducir la incertidumbre y gestionar el riesgo utilizando un enfoque sistemático de gestión del riesgo.

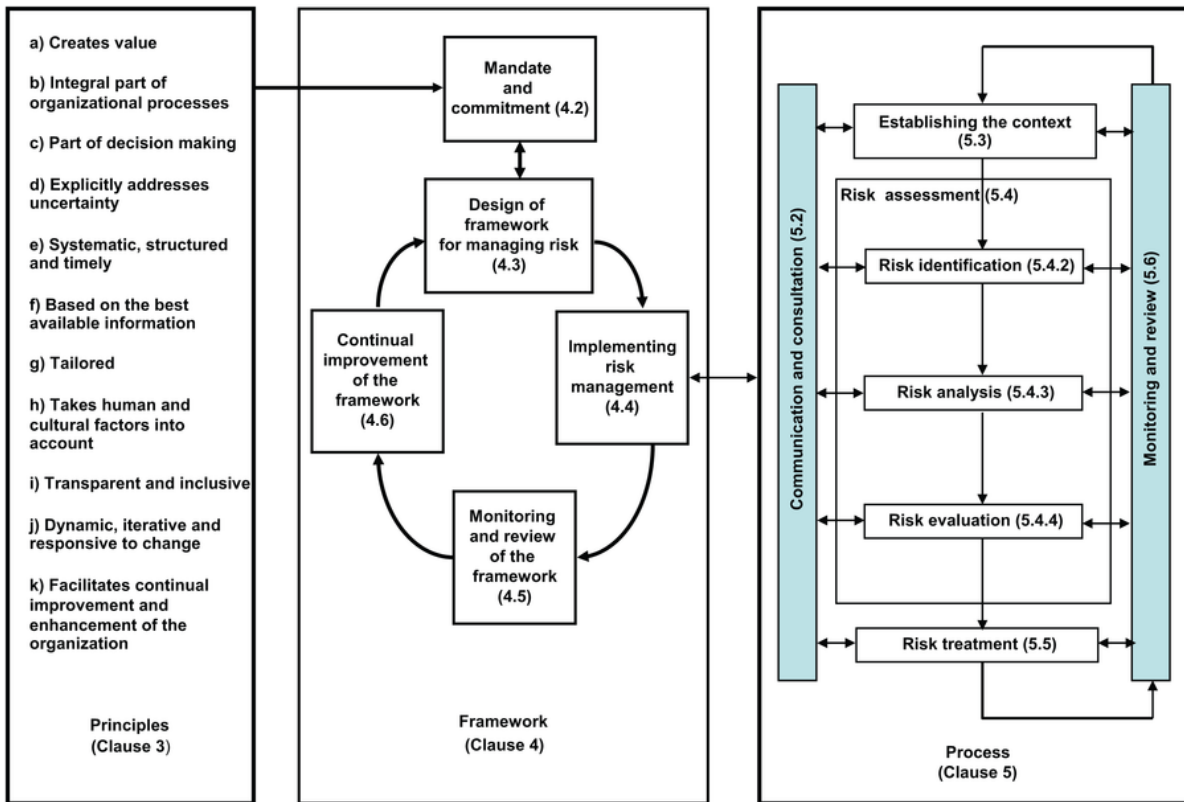
Este estándar puede ser usado por cualquier tipo organización independientemente de su tamaño o sector, tanto públicas como privadas, grupos, asociaciones y empresas de todo tipo, y para cualquier tipo de riesgo. Puede ser a nivel estratégico para apoyar la toma de decisiones y la gestión de procesos, operaciones, funciones, proyectos, programas, productos, servicios, y activos. Sin embargo, el cómo aplicar la norma dependerá de las necesidades, objetivos y desafíos de cada organización.

La norma ISO 31000 bien aplicada puede ayudar a una organización a:

- Incrementar la probabilidad de cumplimiento de objetivos
- Mejorar la habilidad de identificar amenazas y oportunidades
- Alocar y utilizar los recursos de tratamiento del riesgo
- Mejorar la resiliencia global de la organización
- Mejorar la efectividad y eficiencia operacional
- Ayudar a reducir pérdidas
- Mejorar los controles de gestión del riesgo
- Cumplir con requisitos legales y regulatorios
- Mejorar la prevención de pérdidas y la gestión de incidentes
- Mejorar la confianza de los *stakeholders*
- Entre otras

La siguiente figura muestra la relación entre los principios de gestión de riesgos, el marco de referencia en el que ocurren, y el proceso de gestión del riesgo descrito por este estándar internacional

Figura 9. ISO 31000 (2018) framework



Fuente: www.iso.org

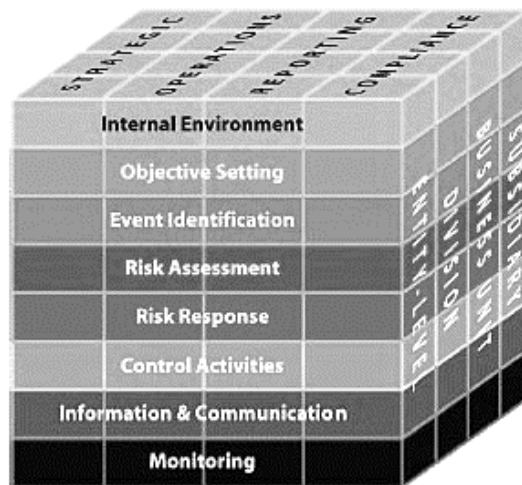
5.3. COSO Framework

Es una iniciativa colectiva dedicada a proveer liderazgo a través del desarrollo de marcos de referencia y directrices en la Gestión del Riesgo Empresarial, control interno y prevención del fraude.

En particular la Gestión del Riesgo Empresarial identifica las siguientes componentes interrelacionadas y asociadas a cada una de estas gestiones: Ambiente interno; Fijación de objetivos; Identificación de eventos; Evaluación de riesgos; Respuesta ante riesgos; Actividades de control; Información y comunicación; Monitoreo.

Además, está dirigida a cumplir los objetivos de la organización en cuatro categorías: Estratégico, Operacional, Reporting, Cumplimiento.

Figura 10. COSO framework



Fuente: www.coso.org

5.4. BS 25999 (2007) – Gestión de la Continuidad de Negocios

Introducido en el Reino Unido para proveer de un estándar con el cual las organizaciones podían obtener por primera vez certificación acreditada en Continuidad de Negocios. Es considerada una norma predecesora y reemplazada por la actual ISO 22301 (2012), y fue la primera norma británica para la gestión de continuidad y fue concebida con el fin de ayudar a minimizar el riesgo a las interrupciones, como un siniestro o una catástrofe.

(Fuente: <https://www.iso.org/news/2012/06/Ref1602.html>)

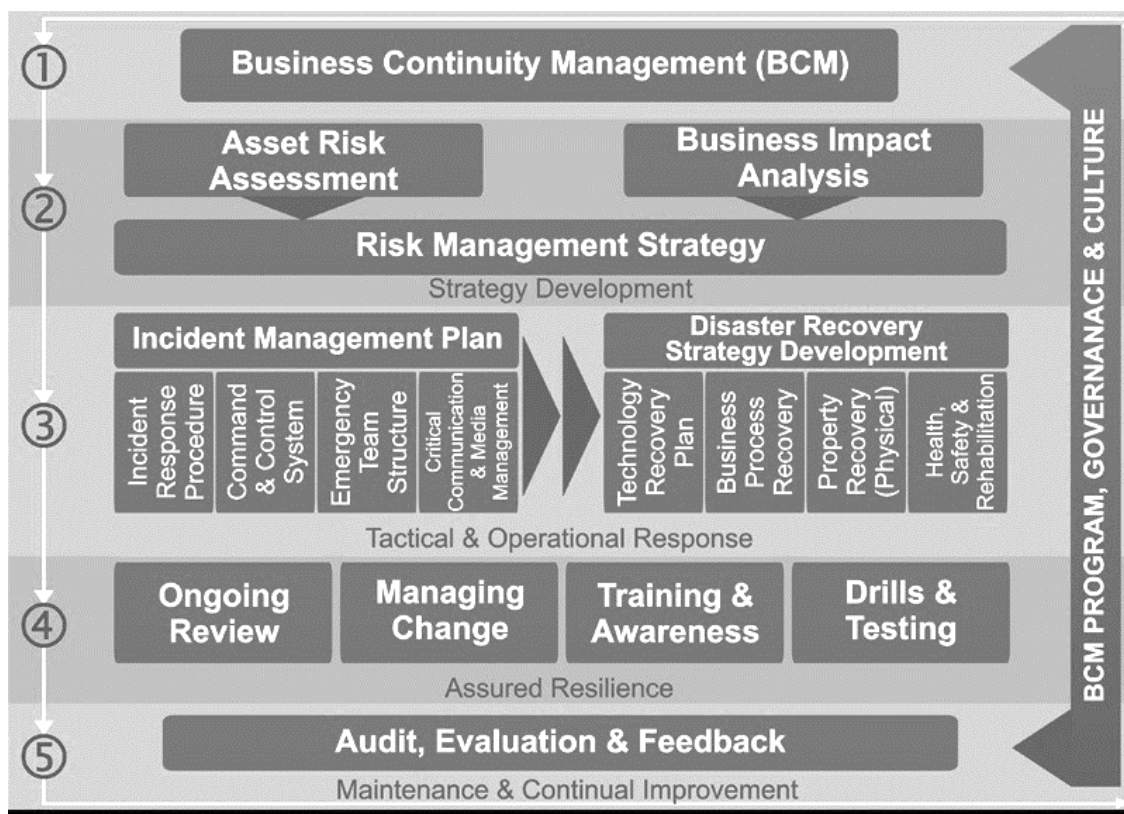
5.5. ISO 22301: 2014 – Sistemas para la Gestión de la Continuidad de Negocios

Es un estándar en Gestión de la Continuidad de Negocios que puede ser usado en organizaciones de todos los tipos y tamaños para ayudarles a protegerse, prepararse, responder, y recuperarse cuando una interrupción de cualquier tipo ocurra, asegurando que podrán responder frente a cualquier incidente y continuar sus operaciones. Las empresas pueden obtener certificación acreditada basada en este estándar y por ende les permite demostrar a distintos *stakeholders* y partes interesadas que la organización adhiere a buenas prácticas en Gestión de Continuidad de Negocios. Este

estándar también puede ser usado al interior de una organización para medirse en comparación a buenas prácticas en la materia, en cuyo caso la influencia de esta norma será mucho mayor que para aquellas que simplemente eligen la certificación.

ISO 22301 provee un marco para planificar, establecer, implementar, operar, monitorear, revisar, mantener y mejorar continuamente un Sistema de Gestión de la Continuidad de Negocios, y su objetivo es dar continuidad al negocio. Se centra en las constantes pruebas para demostrar la "fortaleza" del plan y su implementación. Su marco de gestión se puede resumir en la siguiente figura:

Figura 11. ISO 22301 (2014) framework



Fuente: www.iso.org

5.6. ISO 27001 (2011) – Gestión de la Seguridad de la Información

Es el estándar más conocido como parte de la familia de estándares ISO 27000, que ayuda a las organizaciones a mantener los activos de información seguros, tales como información financiera, propiedad intelectual, detalles de empleados o información confiada por terceros a la organización.

En particular la ISO 27001 provee los requerimientos para un Sistema de Gestión de Seguridad de la Información.

(Fuente: www.iso.org)

5.7. NFPA 1600 – Estándar en Gestión de Desastres/Emergencias y Programas de Continuidad de Negocios

Establece una base de normalización para el planeamiento y operaciones de manejo de desastres/emergencias al brindar elementos comunes del programa, técnicas, y procedimientos enfocados en su totalidad en el programa. Su objetivo es dar continuidad al negocio formando parte de un plan de gestión de emergencia a nivel global y estableciendo un sistema de gestión de incidentes basado en un Centro de Operaciones de Emergencia y una estructura jerárquica de actuación o Sistema de Manejo de Incidentes.

Es parte del sistema nacional de gestión de incidentes y el sistema de comando de incidentes de EEUU (NIMS/ICS) y el marco de acción se enmarca en la recuperación y restauración de los requisitos del sistema de gestión.

Algunos de los elementos más importantes mencionados son:

- Identificación de peligros, evaluación de riesgos y su mitigación: La evaluación de riesgos debe cuantificar la probabilidad de incidentes y la gravedad de sus consecuencias, cuantificando el impacto que tendría un desastre en sus activos y las consecuencias financieras directas o indirectas. El análisis del impacto debe cuantificar las emergencias potenciales de un riesgo, que permita evaluar el costo-beneficio por los esfuerzos de investigación y determinar cuánto invertir en planes de mitigación, respuesta y recuperación.
- Administración de recursos: Los recursos necesarios deben ser catalogados para su recuperación, y el acceso a éstos debe disponerse con anterioridad. Cualquier limitación debe ser identificada para que fallas puedan ser corregidas.
- Planificación: Todas las organizaciones deben tener un plan que cumpla con el reglamento, este debe contar con estrategias de mitigación a corto y largo plazo, una lista de funciones críticas, en orden de prioridades, un análisis de impacto, un programa de respuesta y recuperación total y un plan de evacuación.
- Dirección, control y coordinación: Toda organización debe contar con un sistema de administración de incidentes (IMS) y procedimientos para el control constante de incidentes.

En resumen, es una norma que establece un conjunto común de criterios para la mitigación, preparación, respuesta y recuperación ante desastres y emergencias, y ha sido aprobada por el Instituto Americano Nacional de Normas

(Fuente: National Fire Protection Association - <http://www.nfpa.org/>)

5.8. BS 12999 (2015) – Gestión de daños

Este estándar está diseñado para ayudar a las personas a responder efectivamente cuando un accidente o crimen ha causado daño a la propiedad o a los activos. Aplica a un amplio rango de tipos de incidente incluyendo, incendios, inundaciones, contaminación y explosiones. No propone tecnologías o metodologías específicas, pero identifica procesos genéricos aplicables a todos estos incidentes. Está alineada con las buenas prácticas de gestión del riesgo y está dirigida a profesionales u organizaciones de gestión de daños, entre ellos aseguradoras, equipos de respuesta a emergencias, instituciones de gobierno, autoridades locales, entre otros.

Describe cómo restablecer la propiedad y activos; las mejores prácticas para estabilizar, mitigar, remediar y restaurar los daños; un método simple para establecer si estas actividades han sido conducidas de forma adecuada; y una guía para la comunicación entre las partes que deberían estar conscientes del estado de un incidente

(Fuente: BSI Group)

5.9. NIMS: National Incident Management System (FEMA, Estados Unidos, 2018)

Es el sistema de gestión utilizado en Estados Unidos que busca dar una coordinación general para el tratamiento de incidentes de cualquier nivel de complejidad, proponiendo para ello procedimientos y estructuras.

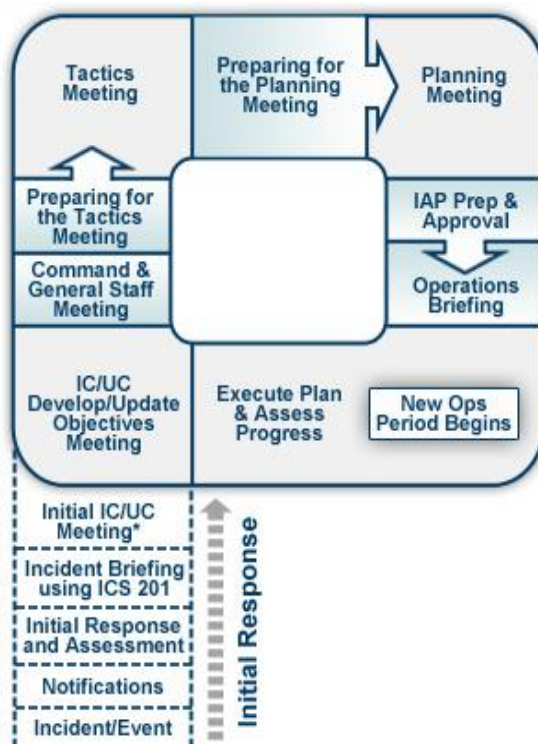
Nace a partir de los atentados de septiembre de 2001 y los huracanes del año 2004. Integra una estructura de gestión utilizada por más de 30 años en Estados Unidos en Gestión de Emergencias, denominada *Incident Command System*.

Se caracteriza porque su modelo puede utilizarse en cualquier tipo de organización, tales como:

- Dependientes del Estado
- Hospitales
- Empresas del Sector Privado
- ONGs
- Otros

Es un estándar de actualización y publicación permanente, disponible en el sitio web de Fema para toda la comunidad, y que plantea el siguiente ciclo de planeación denominado Planificación "P" que establece un continuo para la Planificación de Acciones frente a Incidentes (PAI) durante emergencias o incluso fuera de éstas

Figura 12. NIMS framework



Fuente: www.fema.gov

5.10. BS 65000 (2014) – Guía para la Resiliencia Organizacional

Describe la naturaleza de la resiliencia y las formas de construir y potenciar la resiliencia organizacional. Es un estándar dirigido a la Alta Dirección y a cualquier responsable por construir resiliencia en una organización: Gerentes

de Riesgo, profesionales de gestión de continuidad, gobierno, responsables de la gestión de emergencias y cadena de suministro.

Este estándar define la resiliencia organizacional como la habilidad de anticipar, prepararse, responder y adaptarse a los eventos – tanto shocks repentinos como cambios graduales. Esto implica ser flexible, competitivo, ágil y robusto.

Una forma de mejorar la resiliencia es integrando y coordinando las variadas disciplinas operacionales en una organización, por ello este estándar recurre a otros estándares relacionados con estas disciplinas. La mayoría de las organizaciones funcionan al interior de complejas redes de interacciones. Este estándar reconoce que esto es esencial para construir resiliencia no sólo al interior de una organización, sino que a lo largo de redes y en colaboración con otros. Usando la terminología fijada por este estándar:

- permite clarificar el significado de resiliencia
- destaca los componentes clave de la resiliencia
- ayuda a una organización a medir su resiliencia y realizar mejoras
- identifica las buenas prácticas encontradas en otras disciplinas y definidas en estándares existentes.

(Fuente: BSI Group)

5.11. ISO 22316 (2017) – Seguridad y Resiliencia

Entrega directrices para mejorar la resiliencia organizacional para organizaciones de cualquier tamaño y tipo. No aplica a alguna industria o sector en particular. Establece los principios para la resiliencia organizacional, identifica los atributos y las actividades que apoyan la mejora en la resiliencia de una organización. Incluye:

- Los principios que entregan las bases para mejorar la resiliencia de una organización
- Los atributos que describen las características de una organización que permite los principios anteriores sean adoptados
- Las actividades que guían la utilización, evaluación y mejora de tales atributos

(Fuente: www.iso.org)

5.12. BS 11200 (2014) – Gestión de Crisis (Directrices y buenas prácticas)

Esta guía de buenas prácticas ofrece directrices para ayudar a la administración a planificar, establecer, operar, mantener y mejorar las capacidades de gestión de crisis de las organizaciones. Esta guía es aplicable a cualquier organización independientemente de su localización, tamaño, tipo, industria o sector. Sus contenidos son:

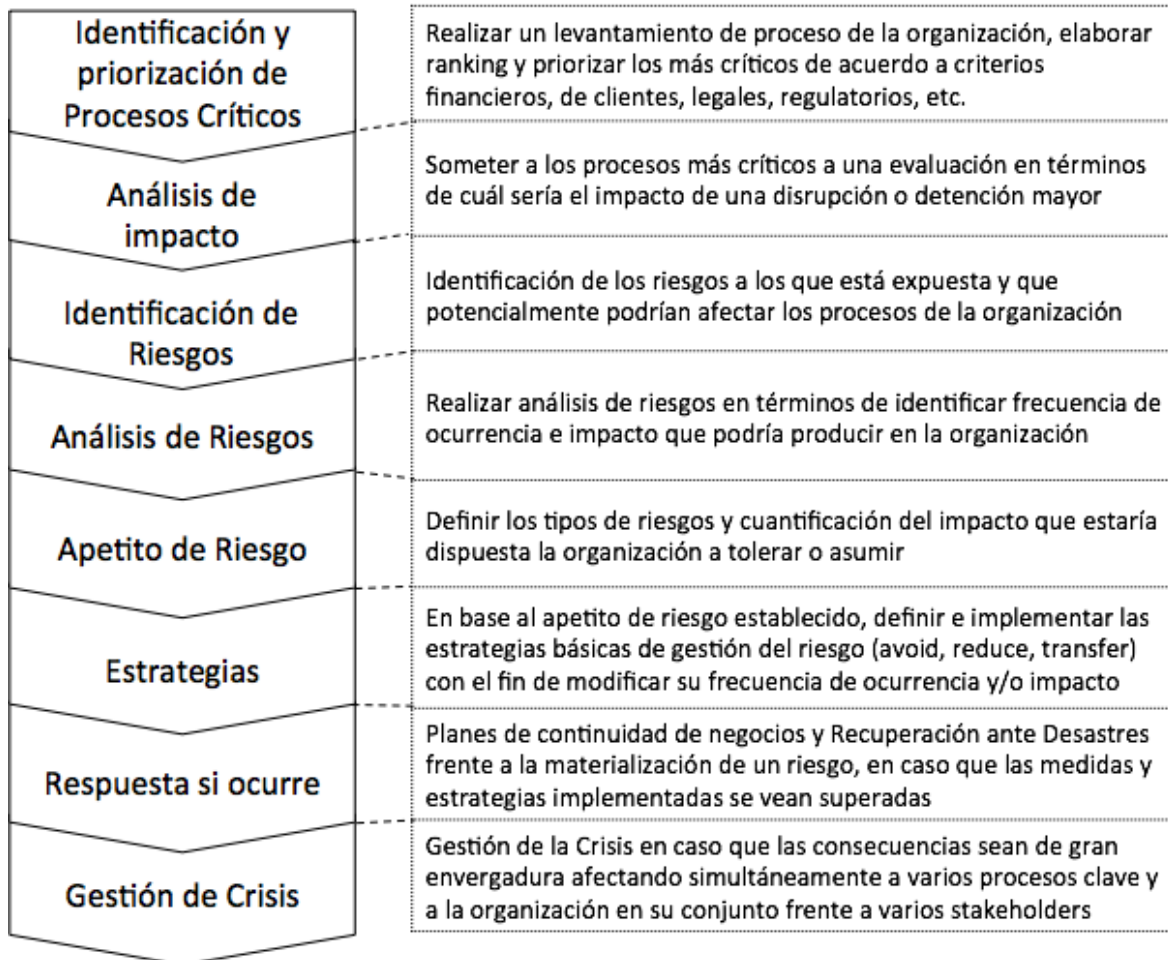
1. Introducción
2. Alcance
3. Términos y definiciones
4. Gestión de Crisis: conceptos centrales, principios y desarrollo de capacidad
5. Construyendo capacidad para la gestión de crisis
6. Liderazgo durante la crisis
7. Toma de decisiones estratégica durante la crisis
8. Comunicaciones durante la crisis
9. Entrenamiento, ejercicio y aprendizaje de las crisis

(Fuente: BSI Group)

5.13. Oportunidades de los modelos y estándares existentes

Un resumen general y secuencial de lo expuesto por las normas y estándares vigentes puede describirse en la siguiente figura, el cual describe el enfoque metodológico que debiese seguir secuencialmente cualquier organización que pretenda abordar la gestión de riesgos, continuidad de negocios y crisis en forma integral:

Figura 13. Resumen del enfoque de gestión de riesgos, continuidad de negocios y gestión de crisis



Fuente: Elaboración propia

Sin embargo, considerando el panorama actual de amenazas y vulnerabilidades descrito en la sección 4.1., y la urgencia porque las organizaciones aborden adecuadamente la continuidad de sus procesos y sean capaces de gestionar una crisis, es que este modelo integrado exhibe algunas limitaciones de cara a una efectividad máxima:

1. **Podría requerir un esfuerzo demandante en tiempo y costo, directamente proporcional al tamaño de la organización.** La identificación de la cadena de valor y los procesos críticos puede ser un desafío y proyecto en sí mismo, dependiente además del nivel de madurez de la organización en gestión de procesos o la existencia de alguna certificación en este campo (por ejemplo, ISO 9001) Más aún si deben incorporarse las etapas de identificación, análisis y gestión de riesgos, antes de llegar a establecer algún plan de respuesta frente a algún incidente puntual o una crisis mayor para toda la organización.

2. **Podría requerir apartar gran cantidad de recursos humanos y financieros para su consecución.** El levantamiento de la situación actual y la implementación de las nuevas prácticas podrá ser abordada mediante el uso de personal y recursos interno, los cuales deberán ser destinados al menos parcialmente a esta función, pero más probablemente requiera incorporar conocimiento especializado desde el exterior de la organización a través de la contratación de servicios de asesorías y consultoría.
3. **La organización podría verse enfrentada a un incidente o crisis durante este proceso.** El punto más relevante es que, a la luz de los antecedentes expuestos en la sección 4.1., un incidente mayor o una crisis que involucre y exponga a toda la organización con consecuencias graves e irreversibles podrían ocurrir durante la implementación de tales actividades y antes de llegar a la fase de Respuesta, exponiendo a la organización a tener que enfrentar el evento sin la existencia de planes mínimos de preparación y respuesta ni un adecuado entrenamiento.

Por ello es urgente abordar la oportunidad de plantear un modelo que integre esta gestión en forma integral, pero sin posponer los elementos necesarios para atender una crisis mayor con exposición comunicacional y de reputación para las organizaciones, un modelo que además permita rápidamente asegurar un resguardo mínimo de la organización frente a disrupciones mayores.

6. DISEÑO DEL MODELO PROPUESTO

Entre los fundamentos conceptuales de cualquier modelo de gestión de la continuidad de negocios, reside la necesidad de crear las medidas, estrategias, planes o procedimientos de mitigación necesarias para evitar que una amenaza latente pueda convertirse en un incidente real y, en caso que éste se manifieste, pueda evitar que se transforme en una disrupción mayor a la continuidad del negocio o en una declaración de crisis real. Por esto, en términos prácticos, para asegurar la continuidad del negocio y minimizar las pérdidas el modelo propuesto busca dar respuesta a dos temas fundamentales:

- I. Cómo asegurar la continuidad habitual del negocio de modo que, independientemente del nivel de impacto y sus consecuencias, ningún incidente o amenaza se traduzca en una paralización de las actividades.
- II. Cómo dar respuesta a incidentes mayores que superen las medidas de mitigación existentes, que tengan como consecuencia una paralización importante de al menos una de las actividades principales de negocio, y que incluso pueda derivar en una emergencia, crisis o catástrofe con implicaciones mayores para la sostenibilidad del negocio en el largo plazo.

El modelo propuesto abordará estas inquietudes usando e integrando elementos de los estándares vigentes ya descritos, pero sugiriendo una reformulación a la luz del panorama actual de riesgos y amenazas al cual puede estar expuesta cualquier organización.

En este contexto el modelo se basa en tres claves fundamentales, pero también requiere del planteamiento de algunos supuestos que se describen a continuación.

6.1. Supuestos

Los supuestos básicos del modelo son:

- Los riesgos podrían ser infinitos, así como también sus causas (endógenas o exógenas) por lo tanto cualquier proceso de *Risk Management* podría dejar fuera un espacio indeterminado de riesgos no identificados ni menos evaluados.

- Los efectos de un incidente debidos a cualquier riesgo son absolutamente impredecibles, por ende, cualquier proceso de evaluación de riesgos puede omitir un espacio no determinado de impactos posibles.
- El desarrollo de un incidente es un proceso no lineal, complejo e impredecible que puede iniciarse en una escala menor, pero derivar rápidamente en un problema de continuidad de negocios severo o incluso una crisis profunda.

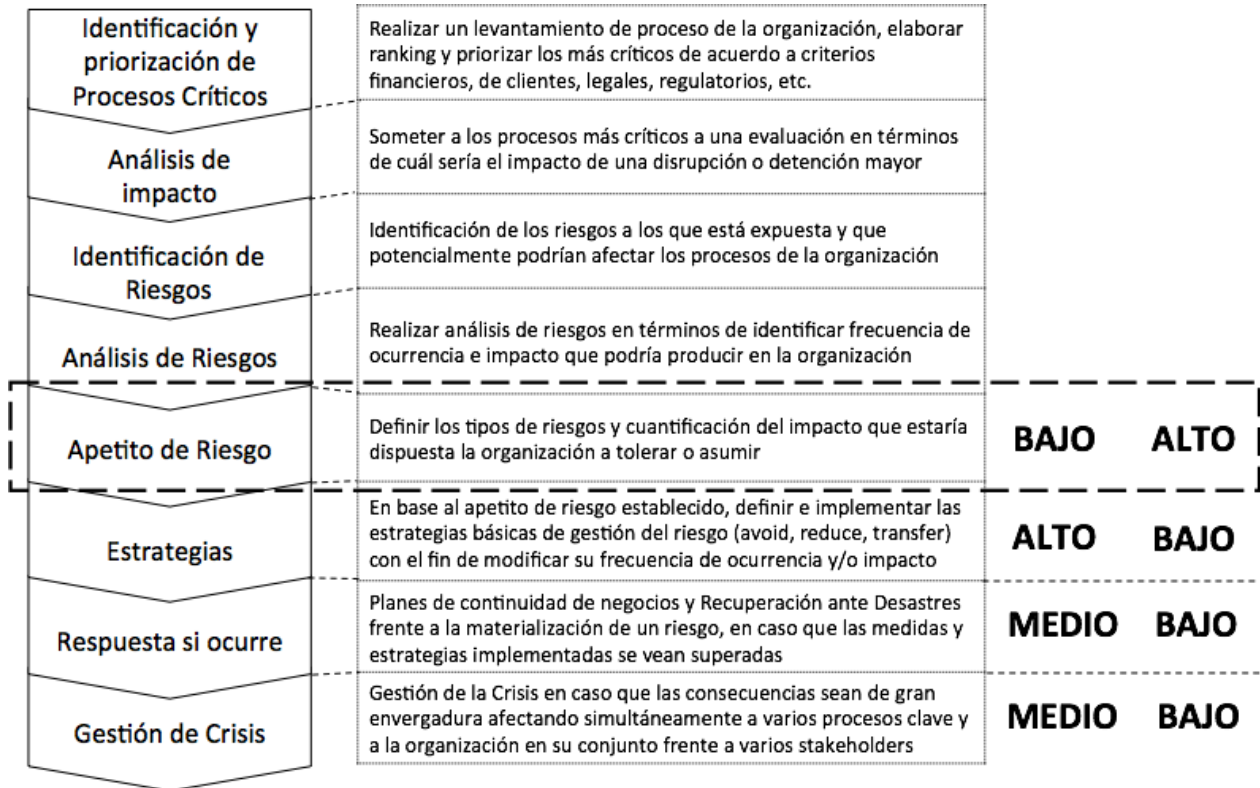
6.2. Las tres claves fundamentales

Además de constituir los elementos centrales del modelo, estas claves constituyen en sí decisiones estratégicas que deben ser asumidas e impulsadas por el nivel ejecutivo de la organización.

6.2.1. Definir claramente el apetito de riesgo.

El primer paso es entender el apetito de riesgo como una variable clave que determinará un *trade off* entre la cantidad y calidad de recursos a destinar en estrategias o en planes de continuidad y respuesta. Cuánto riesgo esté dispuesta a asumir la organización determinará cuántos recursos destinar en estrategias o planes.

Figura 14. Apetito de riesgo en el enfoque de gestión de riesgos, continuidad de negocios y gestión de crisis



Fuente: Elaboración propia

Como puede observarse en la figura, el apetito de riesgo definido por la organización como variable clave, ya que existirá un *trade off* entre las estrategias de gestión del riesgo y los planes de continuidad a establecer. Más aún, es este concepto el que vincula los tres campos Gestión de Riesgos, Continuidad de Negocios y Respuesta ante Crisis, ya que en base al apetito o nivel de riesgo aceptado es que dependerá la intensidad, profundidad y destinación de recursos para la implementación de estrategias y planes de continuidad tendientes a mitigar los impactos del riesgo aceptado. Así, para un nivel de aceptación del riesgo ALTO, menor será el incentivo por realizar una adecuada gestión de los mismos, al igual que para preparar las estrategias y planes de continuidad. De forma inversa, un nivel BAJO de aceptación del riesgo derivará en un foco importante e inmediato en asegurar las estrategias para evitar, transferir y por sobre todo en mitigar el riesgo, incluso por sobre la elaboración de planes de respuesta. Sin embargo, es relevante no perder el foco en, independientemente de lo robustas y efectivas que sean las medidas de mitigación, asegurar las acciones de respuesta frente a incidentes puntuales o crisis mayores, debido a los supuestos planteados en la sección 6.1 de este capítulo.

6.2.2. Priorizar la preparación y respuesta para el peor escenario.

La segunda decisión clave, y la más relevante, es la de modificar la secuencia derivada de las metodologías tradicionales para comenzar definiendo y diseñando la estrategia de respuesta de la organización en las situaciones más extremas y de impacto transversal, en lugar de iniciar la extensa secuencia expuesta en el punto 5.12 anterior en forma secuencial desde la primer fase, asumiendo que en cualquier momento un evento disruptivo mayor podría llevar a la organización a tener que enfrentar un escenario crítico de excepción.

Figura 15. Priorización de la respuesta



Fuente: Elaboración propia

Esta decisión aborda la oportunidad de mantener preparada a la organización en su conjunto para un escenario de crisis mayor que requiera la respuesta de todas las funciones de la cadena de valor, tanto procesos críticos como los de apoyo, en el menor tiempo posible considerando la ocurrencia de tal evento en cualquier momento.

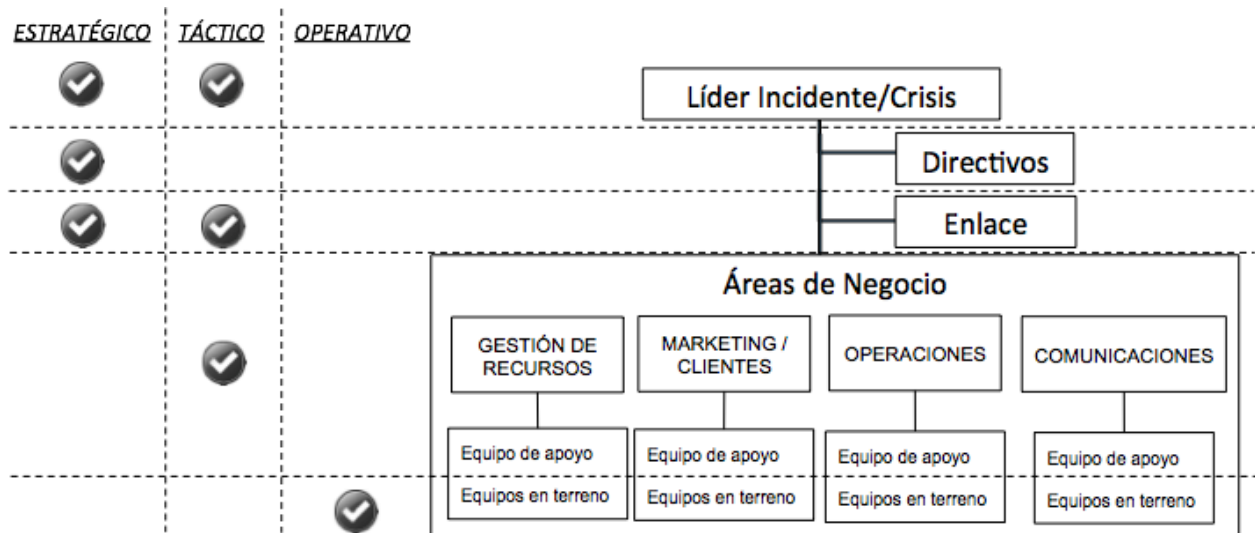
Para abarcar a toda la organización, el modelo de preparación y respuesta requerirá de dos elementos que deberán cruzar los niveles estratégico, táctico y operacional de la organización: una estructura y definiciones para una orgánica de funcionamiento.

6.2.2.1. Estructura de respuesta

Es la estructura organizativa destinada a ser activada una vez declarado el estado de excepción para la organización, que se deberá constituir específicamente para abordar y dar respuesta a los incidentes, contingencias, emergencias, crisis o catástrofes, y cuyo objetivo será velar por la continuidad de todos los procesos de la organización retornando lo antes posible a la normalidad o al nivel de funcionamiento mínimo aceptado, el cual deberá ser definido por el nivel táctico y aprobado por el nivel estratégico. Esta estructura podrá utilizar los recursos humanos, técnicos, logísticos y financieros disponibles en la organización y/o podrá recurrir a la contratación y adquisición de recursos adicionales para tales fines.

La siguiente es una propuesta de estructura simplificada y que rescata e integra los modelos expuestos en el capítulo 5, señalando además si cada función atiende a un enfoque estratégico, táctico u operativo durante la actuación:

Figura 16. Estructura de respuesta



Fuente: Elaboración propia

Líder del Incidente/Crisis: responsable máximo por la vuelta a la normalidad desde iniciado el incidente, monitorea la evolución del estado de la organización durante el incidente, lidera al Equipo de Respuesta global mientras no se alcancen los RPO exigidos, y mantiene informada a la línea Directiva sobre la evolución e impactos del incidente.

Línea Directiva/Alta Gerencia: es el equipo Directivo de la organización que, durante el incidente, asume un rol supervisor e instancia de escalamiento para decisiones de alto nivel que se requieran durante el evento.

Función de Enlace: presta apoyo al Líder del Incidente, integra la gestión global durante el incidente, realiza seguimiento, coordina actividades entre los equipos de respuesta funcionales, Gestión de Recursos:

Gestión de Recursos: provee de todos los recursos necesarios durante el incidente: financieros, equipos, materiales, herramientas, etc.; en fases previas, anticipa necesidades y asegura stock de recursos necesarios en el próximo evento para garantizar máxima disponibilidad.

Marketing/Gestión de Clientes: asegura un impacto mínimo en la satisfacción de los clientes durante el incidente, evalúa la aplicabilidad de las políticas

comerciales y campañas en curso, provee de información de mercado y afectación en clientes al Líder del Incidente, mantiene canal de comunicación con clientes afectados.

Operaciones: asegura la vuelta a la normalidad de todos los procesos de operación afectados ejecutando planes de continuidad y respuesta definidos en fases previas al incidente. Será el dueño del proceso de operación afectado por el incidente el que, a partir de la ejecución de las acciones de restitución y continuidad, abrirá las pautas de ejecución que deberán desarrollar las demás funciones de respuesta.

Comunicaciones: función esencial durante la crisis (sobre todo en grandes corporaciones), toma el control de toda la comunicación emitida por la organización, atiende las necesidades de comunicación de la prensa, medios, entidades estatales y de gobierno, clientes, Equipos de Apoyo: cada función de negocio está compuesta por un equipo de apoyo a nivel táctico que es el que coordina y asegura las actividades descritas anteriormente.

Equipos en Terreno: cada función de negocio está compuesta por un equipo de apoyo a nivel operativo que es el que ejecuta las actividades descritas anteriormente.

La estructura debe incluir la definición de roles claros por cada función, el objetivo a cumplir antes, durante y después del incidente y deberá estar soportada por una lista o nómina de personal que ocupará cada rol o función, listado que deberá ser mantenido y actualizado regularmente, y al que llamaremos Equipo de Respuesta.

Un fundamento esencial consiste en que la estructura a establecer para la continuidad y respuesta debe ser definida para estos fines y no tiene que ser necesariamente la misma responsable de la operación regular del negocio o en condiciones de normalidad. Más aún, esta estructura podría requerir de profesionales de la organización que cuenten con roles y perfiles psicológicos que permitan una toma de decisiones en momentos en los que no se cuenta con el tiempo ni la información suficientes, en otras palabras, liderazgo en tiempo de crisis. Esta definición es clave, incluso porque la línea ejecutiva no necesariamente asume un rol de liderazgo de la crisis a nivel global, sino que supervisa el desempeño del Líder del Incidente/Emergencia/Crisis y asume una función de escalamiento en caso que éste necesite la aprobación de alguna decisión más allá de sus atribuciones durante el incidente como por ejemplo la aprobación de recursos extraordinarios.

Particularmente esencial es la función de comunicaciones, sobre todo en grandes corporaciones y organizaciones para las que la continuidad es esencial ya sea por poseer una gran base de clientes distribuida en una amplia zona de territorio geográfico, por proveer de servicios básicos

esenciales para la población, o por poseer infraestructura crítica para la nación. Esta función debe asumir la comunicación oficial frente a *stakeholders* y será la principal encargada de asegurar un impacto mínimo en la reputación y valoración de marca de la organización. Para ello debe considerar acciones de comunicación proactivas y realizar acciones de contención comunicacional con medios, prensa y redes sociales con el fin de evitar una escalada de la crisis por la ausencia o deficiente comunicación. Este tema ha sido ampliamente desarrollado por el campo denominado "Comunicación en Crisis" y cuya explicación con mayor detalle se encuentra fuera del alcance de esta tesis.

6.2.2.2. Definiciones necesarias de funcionamiento

El Plan Integral de Respuesta estará conformado por definiciones, procedimientos e instrucciones de trabajo, asumiendo un evento disruptivo mayor y que tiene por consecuencia la afectación o paralización parcial o total de la organización en su conjunto o de una o varias de las funciones más críticas. Los elementos de este Plan son:

- a) Definición de los estados de normalidad, alerta, emergencia y crisis, y los criterios para definir bajo cuál de estos escenarios se encuentra la organización en todo momento.

Esta definición incluirá obligatoriamente la determinación de los criterios por los cuales se declara a la organización en un estado u otro, los cuales podrán ser una composición de variables financieras, de procesos de operación, de satisfacción de clientes, pero principalmente de la definición de los RTO y RPO globales (RTO: Recovery Time Objective; RPO: Recovery Point Objective)

Definición de estados:

<i>Normalidad</i>	
<i>Alerta</i>	
<i>Emergencia</i>	
<i>Crisis</i>	

La cantidad de niveles y su definición dependerá de cada organización. Se recomienda establecer primero los estados de normalidad y crisis, para luego identificar escenarios intermedios, y también alinear la cantidad y definición de niveles a los que ya han creado los organismos de emergencia locales (ONEMI en el caso chileno)

La definición de estos estados y criterios permitirá:

- Definir cuándo se deberá activar a la organización en forma total o parcial para ejecutar los planes de continuidad y respuesta que correspondan. Es por ello que esta definición conlleva inevitablemente a identificar los procesos más críticos dentro de

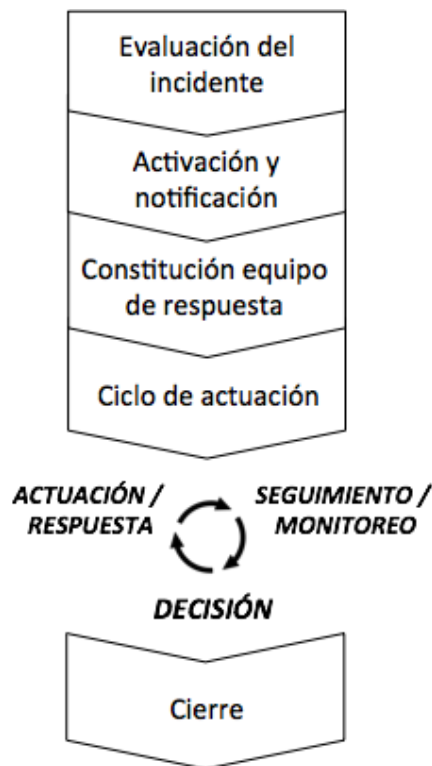
la cadena de valor de la organización, asumiendo una afectación importante en ellos.

- Decidir cuándo la organización sale de la fase de alerta, emergencia o crisis y se desactiva el estado de excepción pasando a la completa normalidad.

b) Declaración de las distintas fases desde el momento de tomada la decisión de activación hasta la determinación de cierre.

En forma genérica estas siguen las siguientes etapas:

Figura 17. Fases para la respuesta



La evaluación del incidente estará guiada por los parámetros y criterios definidos en la sección a) anterior. Si los criterios sugieren una activación, se inicia un proceso de notificación a los equipos de respuesta, actuación en terreno por el personal operativo, y la constitución de las funciones estratégica y táctica. Esto inicia un ciclo de ejecución de cada plan de respuesta definido, un seguimiento y monitoreo con información disponible del estado de la organización en base a los criterios ya definidos que guiará la toma de decisiones en términos de corregir cursos de acción, excluir o incorporar nuevas acciones, decretar el término y cierre del incidente.

Fuente: Elaboración propia

c) Definición de los cursos de acción a alto nivel de acuerdo al tipo de evento ocurrido, las actuaciones inmediatas y aquellas que puedan estar sujetas a evaluación del evento.

Si bien cada evento es diferente, existirán acciones de respuesta que deberán tomarse desde el minuto inicial de ocurrido cualquier evento, sin esperar ninguna autorización o comunicación formal. Ejemplo de ello es la contratación de recursos adicionales tanto materiales como humanos que además deberán estar previamente acordados y comprometidos contractualmente tanto con proveedores habituales como con aquellos que se requieran exclusivamente durante el incidente. Nuevamente es posible visualizar que consecuentemente con

la definición de un plan de respuesta global se estará revisando y definiendo planes de mitigación que también resultan útiles para incidentes menores o cuyo alcance sea sólo de algunos procesos puntuales.

- d) Definición de las actividades que deberán ejecutarse por cada una de las funciones de la estructura de respuesta.
En las fases previas a la ocurrencia de cualquier incidente o crisis (cuando la organización no se encuentre sometida a algún evento) todas las áreas de negocio deberán establecer planes de respuesta locales para sus procesos, asumiendo una situación de discontinuidad extrema o paralización total. Si bien la elaboración de estos planes no necesariamente se alinearán a los procesos secuenciales que indican los modelos vigentes descritos en el capítulo
- e) Los KPIs sobre los cuales se medirá la efectividad de cada función, y que contribuirán a mejorar los indicadores globales que llevarán a la organización a pasar de un estado de alerta y/crisis al de normalidad.
El nivel de efectividad de las acciones ejecutadas tendrá un resultado que acercará a la organización a alcanzar los RPO y RTO definidos para transitar entre los estados de crisis, emergencia, alerta y normalidad. Para ello cada función debe establecer los KPIs que permitan medir el estado en el que se encuentren las principales acciones ejecutadas, así como la contribución al cumplimiento de los RPO y RTO globales.
- f) Las instancias de reunión y seguimiento a la evolución del estado en el que se encuentra la organización, en los tres niveles de decisión (estratégico, táctico, operacional)
Las reuniones de reporte y seguimiento del Líder de Incidente con los equipos de respuesta deberán estar establecidas, asegurando que la primera tras ocurrido cualquier evento ocurra lo antes posible.
- g) Las acciones de mediano y largo plazo correspondientes a reconstrucción y reversa.
Esto es fundamental ya que el estado de excepción coloca a la organización en una posición diferente a la de normalidad en términos de recursos técnicos y humanos movilizados a terreno, decisiones de excepción ejecutadas con el personal interno, clientes, proveedores, etc. las que requerirán volver atrás a su condición inicial o de no excepción
- h) Sistemas de información que permitan contar con la mayor cantidad de datos e información que faciliten la toma de decisiones y la movilización de los recursos para atender el incidente.
La gestión de información en emergencia y crisis, en forma agregada y detalle, suficiente, disponible en oportunidad, consistente y clara,



juega un papel central. Directamente proporcional al tamaño de la organización serán los equipos de respuesta y la cantidad de información que éstos generen, procesen, publiquen y distribuyan por lo que una mala gestión de la información podría agravar los efectos del evento conduciendo a decisiones equivocadas por no contar con la información adecuada en tiempo y forma. Para ello existen plataformas que permiten la gestión de información en emergencia o crisis, tema cuya profundización no forma parte del alcance de esta tesis.

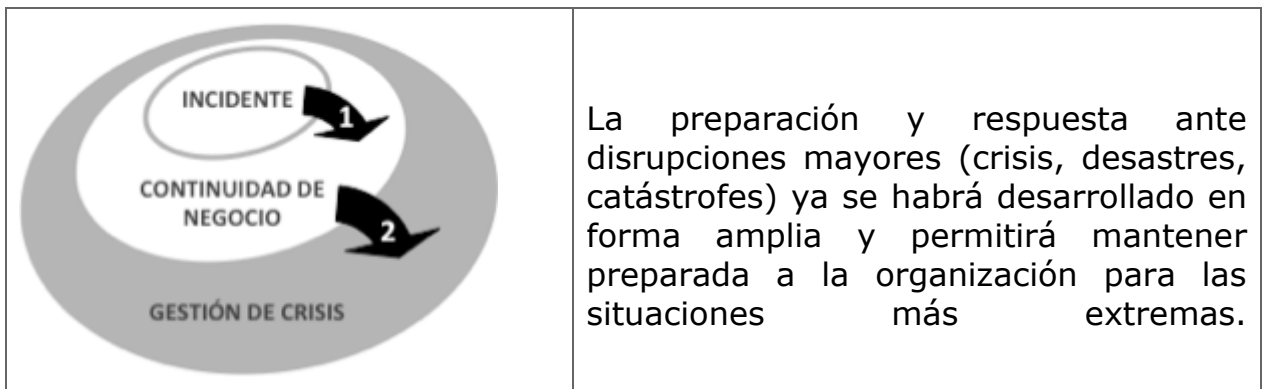
- i) Un Plan de Entrenamiento para todo el personal involucrado acerca del Plan Integral de Respuesta definido.
- a) Tanto el entrenamiento como la capacitación permiten promover e instalar una cultura de conciencia por la gestión del riesgo, continuidad de negocios y respuesta a crisis, por lo que todo el diseño de modelos y planes que implemente la organización, quedarán estáticos en el papel si no se ejercita, refuerza y mejora permanentemente. En este sentido, la práctica de pruebas periódicas a través de simulaciones de activaciones (simulacros) es pieza clave para asegurar la mejora continua del modelo implementado ya que permitirá retroalimentar y robustecer el modelo en los tres niveles organizacionales.
- j) Un Plan de revisión y mejoras, al menos anual.
Ello con el fin de asegurar la identificación e incorporación de nuevos planes de respuesta a las nuevas amenazas y riesgos a los que se podría ver enfrentada la organización, y también para integrar las mejoras identificadas tanto en los entrenamientos realizados como de los eventos reales vividos.

6.2.3. Integrar apetito y estrategia de respuesta, iniciando un proceso de evaluación más detallado.

Los puntos 6.3.1. y 6.3.2. anteriores entregan una ventaja importante en cualquier organización en términos del nivel de preparación global frente a cualquier evento disruptivo, porque el plan de gestión de crisis ya estará en gran medida elaborado. Sin embargo, se debe continuar profundizando y detallando los planes generales usando la información ya levantada en el desarrollo del plan de respuesta, ahora con más holgura para seguir las fases tradicionales de gestión del riesgo y continuidad de negocios expuestas en el capítulo 5 de este documento. Para ello una guía interesante es considerar el siguiente modelo:

Figura 18. Dinámica de escalamiento de eventos

	<p>La dinámica de escalamiento de cualquier evento sigue la siguiente secuencia:</p> <ol style="list-style-type: none"> 1. Una amenaza puede provocar una interrupción, incidente o emergencia menor, y las medidas de mitigación podrían controlar el evento y evitar que se transforme en un problema de continuidad de la operación. 2. Sin embargo, si las medidas y planes de mitigación no son suficientes o no son ejecutados de acuerdo a lo previsto, pueden derivar en problemas serios de continuidad en algún proceso clave. 3. Si las medidas para abordar a pérdida parcial de continuidad no existen, son mal ejecutadas o se ven superadas por el evento, la organización podría verse enfrentada a un problema de crisis, catástrofe o desastre afectando a la organización en su conjunto.
	<p>Ya con un plan de respuesta ampliamente desarrollado, será posible profundizar en los hallazgos estableciendo las estrategias de gestión del riesgo y planes de respuesta frente a pérdidas de continuidad para procesos de criticidad alta y media, consolidando una definición cualitativa y cuantitativa para la pérdida de continuidad (RTO y RPO por proceso)</p>



Fuente: Elaboración propia

6.3. Beneficios e impacto del modelo propuesto

6.3.1. Beneficios generales y contraste con modelos vigentes

Los estándares expuestos en el capítulo 5 derivan en modelos que guían la implementación de sistemas y procesos para abordar la gestión del riesgo, de la continuidad de negocios, de la respuesta ante emergencias, y de la resiliencia organizacional. Por su parte, el modelo propuesto no contraviene, rechaza ni refuta ninguno de los elementos planteados por tales modelos, sino que plantea un enfoque complementario e integrador enfatizando algunos aspectos. La siguiente tabla expone los principales elementos de comparación entre tales estándares y el modelo propuesto.

Tabla 6. Comparación entre estándares vigentes y modelo propuesto

Estándares vigentes	Modelo propuesto
Cada uno se enfoca en alguno de los tópicos: gestión de riesgos, continuidad de negocios, respuesta ante emergencias, resiliencia organizacional.	Integra y plantea a alto nivel los elementos esenciales, destacando los más relevantes.
Algunas describen el Apetito de Riesgo como uno de sus elementos.	Destaca la definición del Apetito de Riesgo como decisión estratégica para determinar el esfuerzo de implementación a comprometer.
Algunas sugieren la secuencia de desarrollo: > Priorización de Procesos Críticos > Análisis de impacto > Identificación y análisis de Riesgos > Estrategias de gestión del Riesgo > Respuesta y Recuperación > Gestión de Crisis	Propone la secuencia: > Definición de Apetito de Riesgo > Respuesta y Recuperación > Gestión de Crisis > Priorización de Procesos Críticos > Análisis de impacto > Identificación y análisis de Riesgos > Estrategias de gestión del Riesgo

Este planteamiento permite que el modelo propuesto en este documento ofrezca los siguientes beneficios para las organizaciones:

- a) Da acceso a una comprensión conceptual simplificada para cualquier organización de cualquier sector y tamaño que vea valor en iniciar una gestión robusta de riesgos, continuidad y crisis.
- b) Les permitirá integrar transversalmente (*end to end*) los principales elementos de los modelos vigentes para todo el ciclo Riesgo – Continuidad – Respuesta – Resiliencia, lo cual podrá encontrarse de manera independiente en los estándares vigentes.
- c) Evita el desarrollo de la secuencia más extensa sugerida por los estándares vigentes, con el riesgo de ver a la organización enfrentada a la próxima emergencia o crisis sin haber llegado al desarrollo de la fase de Respuesta y Recuperación.
- d) Otorga a la organización una ventaja competitiva de cara a sus clientes ya que da mayores garantías de continuidad en la entrega de los productos y/o servicios respecto de aquellas que no cuenten con un modelo similar, lo que puede ser expuesto como antecedente en cualquier proceso de licitación.
- e) Otorga seguridad y tranquilidad a la organización de contar con un mecanismo de respuesta listo para atender y minimizar las pérdidas del próximo evento.

- f) Puede ser implementada con recursos humanos internos, no requiere necesariamente de la contratación de consultorías o asesorías externas.
- g) Su implementación constituye una base y entrega una ventaja de cara a una certificación en alguna de las normas y estándares descritos en el capítulo 5.
- h) Constituye un antecedente frente a entidades financieras que da solidez y respaldo al momento de requerir financiamiento, como con compañías aseguradoras para re negociación de los costos de primas de seguros.
- i) Para empresas de menor tamaño, contribuye a crear en los *stakeholders* una imagen de empresa profesional y responsable en el desarrollo del negocio.

En resumen, la implementación del modelo propuesto otorgará a la organización al menos beneficios económicos como los descritos en la figura 6 de la sección 4.1. y cualitativos como los expuestos en la figura 7 de la sección 4.2.4., alineados a los que garantizan los modelos vigentes, pero en menor tiempo y con foco en atender cualquier evento inminente. Como se expone en el capítulo 7, empresas de diversos tamaños y sectores pueden beneficiarse de estas ventajas.

6.3.2. Beneficios de poner énfasis en el Apetito de Riesgo

El énfasis en determinar el apetito de riesgo real (ver sección 6.2.1.), obliga a la organización a cuantificar los beneficios esperados en términos de pérdidas evitadas por riesgos, amenazas y eventos ocurridos, así como también planificar el nivel de esfuerzo e inversión necesarios en estrategias y planes de mitigación, respuesta y recuperación. La cuantificación tanto del beneficio como del esfuerzo requerido para obtenerlo permitirá a la organización decidir el balance entre ambas variables, constituyendo una decisión estratégica clave.

6.3.3. Beneficios de priorizar la Estrategia de Respuesta

Asumir un enfoque que sugiere iniciar el diseño e implementación en la fase de Respuesta (ver sección 6.2.2.) puede parecer arriesgado, sin embargo, posee varias ventajas:

- b) Abstrae inicialmente a la organización de realizar una revisión exhaustiva de innumerables escenarios o tipos de riesgo por proceso,

al asumir un escenario extremo o límite bajo el cual pensar el plan para la organización como un todo.

- c) Permite a la organización estar preparada en corto tiempo para enfrentar eventos disruptivos mayores, independiente de las medidas de mitigación en los procesos más críticos.
- d) Integra los elementos de los campos gestiones de riesgo, continuidad de negocios, y crisis, ya que inevitablemente la definición y diseño de la estructura y plan de respuesta global obligará a realizar un revisión y formalización de:
 - los procesos críticos en los niveles estratégico, táctico y operacional
 - los riesgos principales en los tres niveles
 - las medidas de mitigación existentes y las necesarias de implementar
 - la creación de planes de respuesta por área de negocio y/o para los procesos más relevantes de la cadena de valor, empoderando a los dueños de tales procesos y a sus equipos de trabajo.
- e) Coloca a la organización en ventaja para abordar una gestión de riesgos, continuidad y resiliencia más profunda y detallada con la tranquilidad de contar con un plan de respuesta inmediato frente a cualquier evento disruptivo en el corto plazo (ver sección 6.2.3.)
- f) Establece una estructura especializada en la respuesta que se constituye sólo para estos fines incluso como entidad adyacente al organigrama habitual del negocio, permite focalizar recursos y esfuerzo en la respuesta mientras la estructura organizacional habitual mantiene el foco en las decisiones diarias.
- g) Prioriza y robustece la función de comunicaciones como función clave durante la emergencia o crisis, permitiendo minimizar los impactos en reputación debidos a la crisis misma o a un mal manejo de ella, de cara a clientes, opinión pública, entidades reguladoras y del estado, empleados y accionistas. Además asegura la tranquilidad y tiempo necesario a los equipos de respuesta y a la organización completa para continuar las acciones y dar prontitud al cierre de la crisis.

A la luz de los antecedentes y estadísticas expuestas en la sección 4.1., anteponer la estrategia de Respuesta a la secuencia habitual que exhiben los estándares vigentes, evita que emergencias y crisis erosionen los activos y el capital de una organización poco preparada, y contribuye con ello a asegurar la viabilidad del negocio en el corto y largo plazo.

6.4. Limitaciones del modelo

Algunas limitaciones del modelo, y que exponen su real alcance, son:

1. **No constituye una guía para la identificación de eventos potenciales ni futuros.** El modelo plantea una estrategia de abordaje de corto plazo para mantener a cualquier organización preparada a dar respuesta a variados tipos de eventos que deberán ser identificados y revisados por la organización, pero la revisión para llevar a cabo tal proceso dependerá de cada organización de acuerdo al sector o industria a la que pertenezca, y a los tipos de riesgo a los que este expuesta. La identificación precisa de todos los riesgos existentes para una organización es un input para el modelo, el cual no asegura que el 100% de ellos sean claramente identificados, ni tampoco la aparición de nuevas amenazas. Ello obliga a mantener un proceso sistemático y periódico de identificación de riesgos y amenazas.
2. **No entrega lineamientos para determinar el apetito de riesgo de una organización.** El modelo plantea como uno de los tres elementos clave, la determinación por parte de la organización del apetito de riesgo, pero no es parte del alcance de este documento el guiar la definición cualitativa y/o cuantitativa de tal variable. Para ello se recomienda profundizar en modelos y marcos de referencia para su determinación.
3. **No predice ni garantiza un umbral máximo de pérdidas.** La ocurrencia de un evento de alto impacto que además alcance el impacto máximo en un lapso de tiempo muy acotado, puede irremediablemente llevar a una organización a su desaparición, frente a lo cual ningún plan de respuesta resultará efectivo. Además el modelo podrá ser implementado asumiendo ciertos niveles de frecuencia e impacto de los riesgos identificados, para determinar el apetito de riesgo y las estrategias de respuesta y recuperación, y cualquier variabilidad en tales niveles puede derivar en pérdidas que superen los supuestos originales. Nuevamente, un proceso periódico de revisión de riesgos permitirá abordar esta debilidad.
4. **No plantea lineamientos para la reconstrucción o restauración.** El modelo se hace cargo de las acciones principales para dar respuesta y contener los efectos de los eventos revisados y estudiados previamente por la organización, pero no describe las actividades propias de la reconstrucción o restauración del daño sufrido por los activos físicos e intangibles de la organización, cuyo esfuerzo será función directa del nivel de daño y la criticidad del activo afectado. Para ello se sugiere profundizar en estrategias y planes de Recuperación y Restauración.
5. **No cuantifica el esfuerzo económico ni financiero de las acciones de respuesta, ni menos su optimización.** Si bien la implementación del modelo se justifica por las pérdidas potenciales que cualquier organización enfrentada a un evento sin la preparación para la respuesta podría evitar, el modelo no expone una cuantificación del esfuerzo

económico y financiero que tal dinámica de respuesta conlleva, tanto durante la ocurrencia de un evento como previo a su materialización. Toda acción de respuesta implicará uso de recursos de la organización para atender un incidente o evento en forma coordinada, y la optimización de tal uso constituirá una segunda fase de mayor especialización dentro del programa de continuidad de negocios de cualquier organización. Sin embargo, a juzgar por los beneficios en términos de impactos y pérdidas evitadas como las expuestas en la figura 7 de la sección 4.2.4., cualquier esfuerzo de esta índole arrojará un caso de negocio positivo que validará su realización.

6. **No incluye elementos concretos que guíen la toma de decisiones durante un incidente.** Este desafío es más ambicioso y escapa al alcance inicial del modelo propuesto. Sin embargo, es posible predeterminar y entrenar (simular) cursos de acción para el set de amenazas analizadas por la organización, entendiendo que siempre quedará un espacio a la improvisación por tratarse de procesos no lineales. En este sentido es clave la existencia de sistemas de información disponibles que provean de la mayor cantidad de información posible para las instancias de toma de decisión durante el incidente, más aún cuando se trata de una crisis, y que las primeras acciones de alerta, constitución y reporte sean definidas y entrenadas regularmente para que su funcionamiento sea autónomo y autosuficiente. El campo "toma de decisiones durante una crisis" podrá ser estudiado como complemento a este documento.

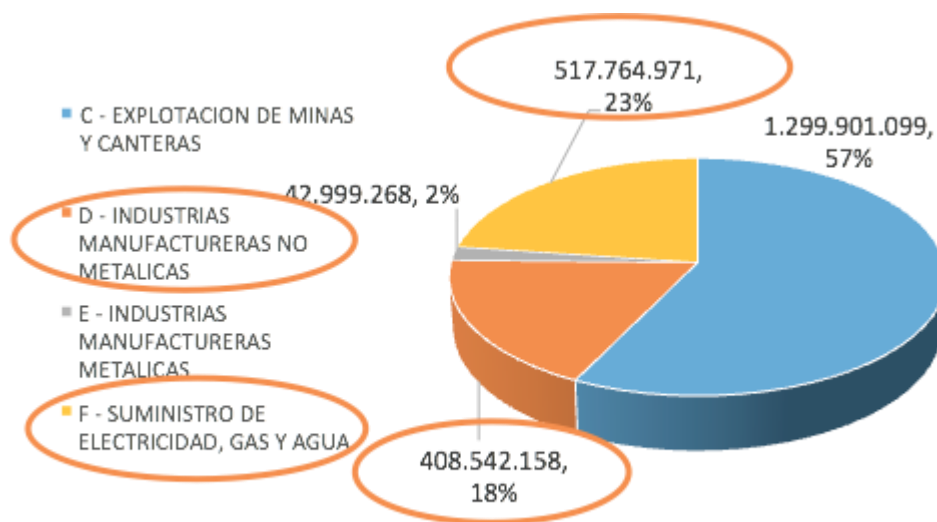
7. SEGMENTACIÓN DE MERCADO POTENCIAL

Si bien para cualquier organización y sector económico la continuidad de negocios debe ser un campo relevante de desarrollar, más importante aún es identificar aquellos para los cuales sea especialmente relevante. Para ello se iniciará un análisis de información de facturación de empresas en Chile, ya sean de carácter público, privado o mixto, que contribuya a identificar la criticidad de una adecuada gestión de continuidad tanto por la naturaleza del sector al que pertenece como por el volumen de recursos que podría estar expuesto a pérdidas económicas. Esto se revisará más adelante con una definición de variables de segmentación específicas.

7.1. Desafíos para las Grandes Corporaciones

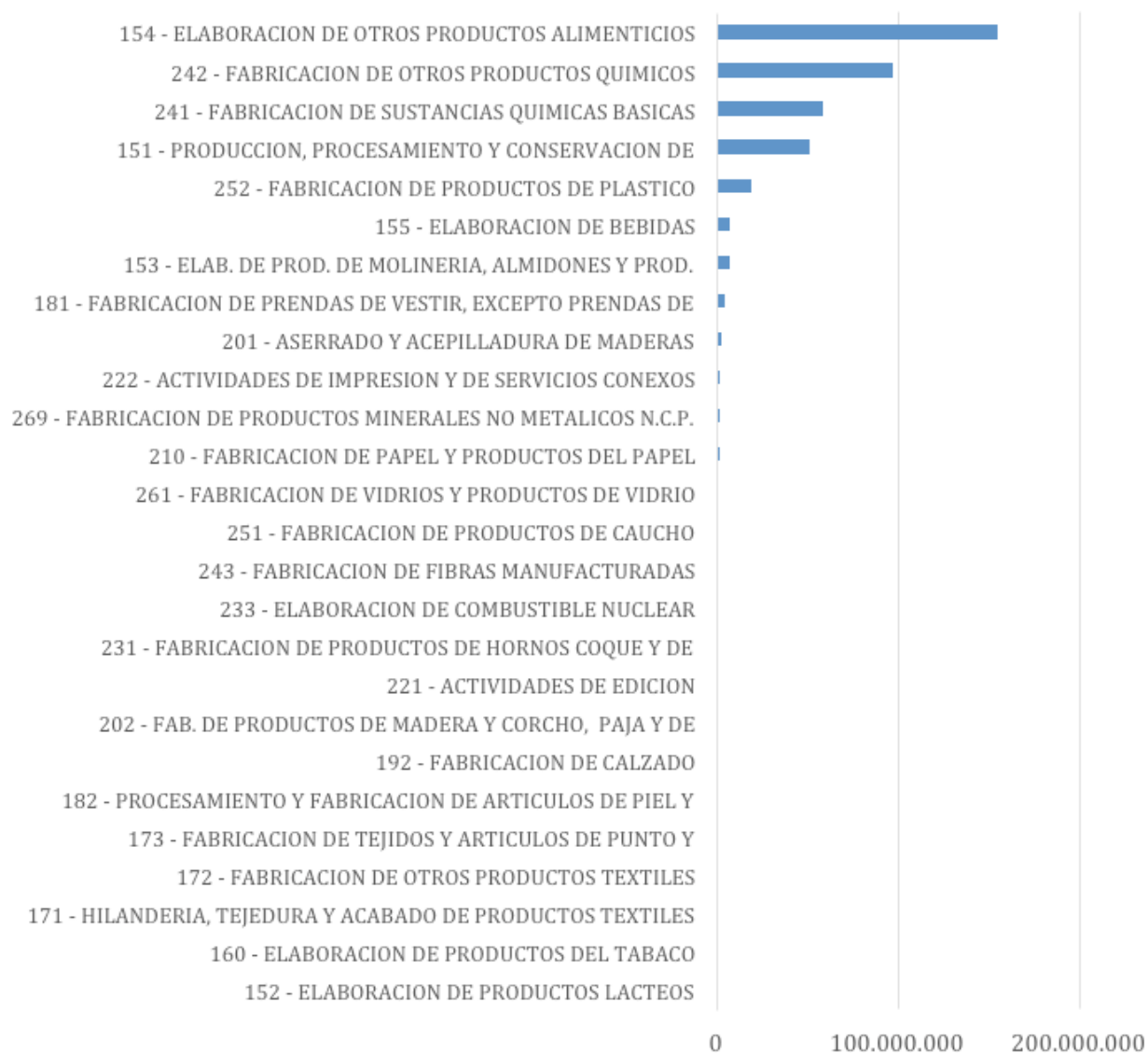
A nivel de Grandes empresas, si bien es evidente apreciar la relevancia de la continuidad de negocios en la actividad de explotación minera por su magnitud en flujo de recursos, en general se trata de un sector homogéneo en términos de procesos y el producto resultante de su actividad. Por ello se centrará el foco en identificar otros sectores bajo la categoría más heterogénea de "Industrias Manufactureras no Metálicas", en particular los sectores "Elaboración de Producto Alimenticios" y "Fabricación de Productos Químicos".

Figura 19. Sectores económicos en segmento Grandes Empresas



Fuente: *Estadísticas de Empresas por Tramo según Ventas, Rubro, Subrubro y Actividad Económica, Servicio de Impuestos Internos, 2016.*

Figura 19. Sub-sectores económicos en sector “Industrias Manufactureras no Metálicas”



Fuente: Estadísticas de Empresas por Tramo según Ventas, Rubro, Sub rubro y Actividad Económica, Servicio de Impuestos Internos, 2016.

Por otra parte, especialmente relevante es el sector que agrupa el suministro de electricidad, agua y gas, por tratarse de empresas proveedoras de servicios básicos para la comunidad, por lo que las empresas de este sector tienen una alta exposición a reclamos y comentarios de la opinión pública, prensa, medios de comunicación y de la comunidad en general que hoy tiene acceso al uso masivo de redes sociales.

Pueden identificarse beneficios para las grandes organizaciones como contar con una ventaja competitiva en términos de time to market competitivo, reducción de ineficiencias y desvío de recursos, evitar pago de sanciones y multas económicas por incumplimiento, obliga a la revisión, mejora y comunicación de procesos entre áreas de la organización, entrenamiento y desarrollo profesional a ejecutivos y profesionales internos, favorece la comunicación, coordinación y trabajo colaborativo inter áreas, capitalizable en las tareas regulares del negocio.

Este contexto expone a estas empresas a que una paralización en sus operaciones pueda transformarse no sólo en pérdidas económicas, sino que en una crisis de reputación severa en cuestión de horas. Ejemplos de situaciones de este tipo de ocurrencia reciente en el país se exponen a continuación:

- **Crisis Enel por nevadas en Región Metropolitana (Julio, 2017)**

En Julio de 2017 la principal compañía distribuidora de energía eléctrica de la Región Metropolitana se vio enfrentada a una crisis de más de 3 días debido a un evento que superó los pronósticos iniciales en términos de impacto, y a un manejo de la emergencia que derivó en una crisis de reputación. Este caso será desarrollado en el capítulo 8.

Figura 20. Notas de prensa crisis Enel, Julio 2017

Enel: radiografía de una crisis

Dos apagones en un mes. Clientes furiosos, barricadas en el sector oriente, dos nuevas formulaciones de cargos, sanciones que podrían llegar a US\$ 16 millones, pago de compensaciones por cerca de US\$ 5 millones, una imagen reputacional por el suelo y una billetera obligada a abrirse para evitar que la situación se repita. Esta es la bitácora de la última crisis de Enel.



Crisis de Enel: ven fuerte daño a la reputación de la compañía y 98% de los encuestados espera una mayor regulación

por EL MOSTRADOR MERCADOS | 25 julio, 2017



Fuente: Diario La Tercera, 23 de Julio de 2017; Diario El Mostrador, 25 de Julio de 2017.

- **Aguas Andinas por rotura de matriz en Providencia, Junio de 2017**

El 9 de junio de 2016, la rotura de una matriz de agua durante la madrugada, provocó un socavón en una de las principales avenidas de la capital, la inundación y paralización del tren subterráneo y el corte de tránsito en el sector. La situación generó una crisis de reputación para la compañía con menciones directas en medios de comunicación y redes sociales, y pérdidas económicas para la empresa por concepto de reparaciones y pago de multas.

Figura 21. Notas de prensa crisis Aguas Andinas,

NACIONAL

Santiago colapsado por rotura de matriz de Aguas Andinas

Cerca de las 4 de la mañana, la rotura de una matriz de agua en calle Seminario con Avenida Providencia afectó el servicio de Metro y cortó el tránsito de la arteria capitalina, además de obligar a suspender la restricción vehicular contemplada por la preemergencia ambiental.

Diario Uchile Jueves 9 de junio 2016 10:45 hrs.

matriz

Me Gusta



G+

Compartir



El Servicio Nacional del Consumidor (Sernac) oficiará a Aguas Andinas por la rotura de matriz de agua potable en la comuna de Providencia, que causó una inundación que interrumpió el tránsito vehicular en avenida Providencia y que mantiene la línea 1 del Metro cerrada entre los Héroes y Tobalaba, ocasionando problemas a las miles de personas que se dirigen a sus lugares de trabajo o estudio.

Superintendencia formula cargos contra Aguas Andinas por rotura de matriz de agua en Providencia

El hecho ocurrido en junio del año pasado generó cortes de tránsito, un socavón en Avenida Providencia e inundaciones en el Metro y el Museo Tajamar.

04 de Agosto de 2017 16:45



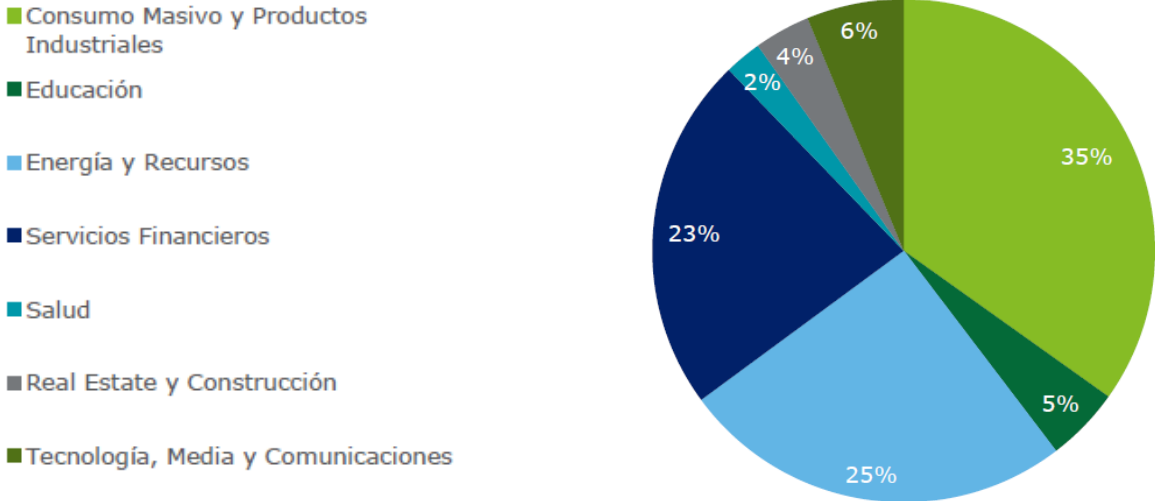
Fuente: Diario UChile, 9 de Junio de 2016,

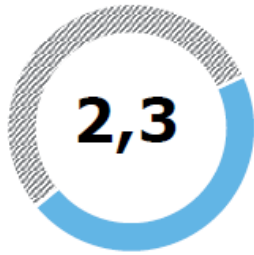
Como se planteó en el punto 2.3., una de las hipótesis que se busca validar es si las empresas poseen un nivel de conocimiento y gestión sólo parcial de la administración de riesgos, continuidad de negocios y crisis. Y que para aquellas que poseen algún nivel de madurez, lo han desarrollado sólo para aquellos procesos y ámbitos que la regulación y legislación vigente les exige sin un nivel de revisión más amplio o integral.

Una revisión de datos y estadísticas disponibles en Chile, arroja cierta información sobre la gestión de riesgos, pero muy escasa respecto a la continuidad de negocios y menos aún sobre gestión de crisis, indicando que el conocimiento y tratamiento de estos campos en Chile es parcial o limitado.

Los siguientes antecedentes derivados de una encuesta realizada a ejecutivos de 80 empresas de diversas industrias a nivel nacional sobre sus niveles de madurez sólo a nivel de gestión del riesgo, confirman la oportunidad de desarrollo en el segmento grandes empresas en Chile no sólo de este campo, sino que de los de continuidad y gestión de crisis, además de la implementación de modelos como el expuesto en esta tesis.

Figura 22. Distribución de industrias para organizaciones entrevistadas y nivel de madurez





Nivel promedio de madurez de la gestión de riesgos a nivel nacional.

En una escala de 1 (nivel de madurez "Inicial") a 5 (nivel de madurez "Óptimo"), se concluyó que el nivel de madurez de la gestión de riesgos promedio de organizaciones encuestadas corresponde a un 2,3 reflejando

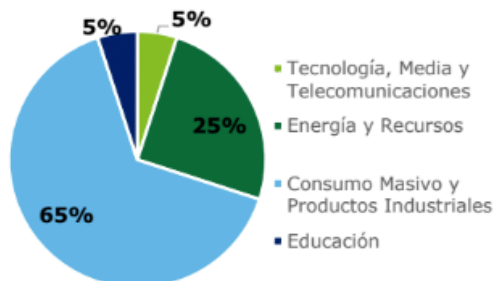
- trabajo por silos
- en vías de implementar o definir un lenguaje común
- uso de nuevos estándares
- obligaciones de nuevas regulaciones

Fuente: Primer Estudio del nivel de madurez de la gestión de riesgos, Deloitte, octubre 2017

El estudio arrojó que en promedio el nivel de madurez de las compañías encuestadas fue de 2,3 en una escala de 1 a 5 considerando el nivel 5 como óptimo.

Figura 21. Principales resultados Encuesta

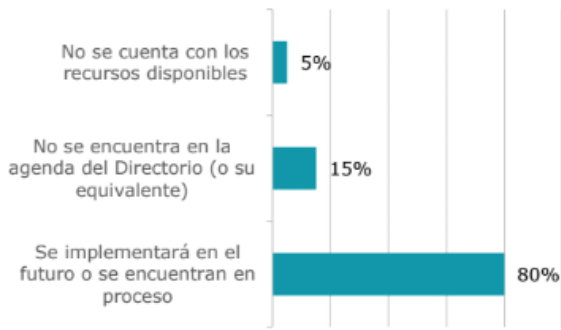
Las industrias de las organizaciones que no poseen un modelo son:



La mayor parte de las organizaciones que no poseen un modelo de gestión de riesgos (65%) provienen de la industria de Consumo Masivo y Productos Industriales, seguido por Energía y Recursos (25%). Cabe destacar que ninguna de las organizaciones que respondieron del sector de educación, posee un modelo de gestión de riesgos.

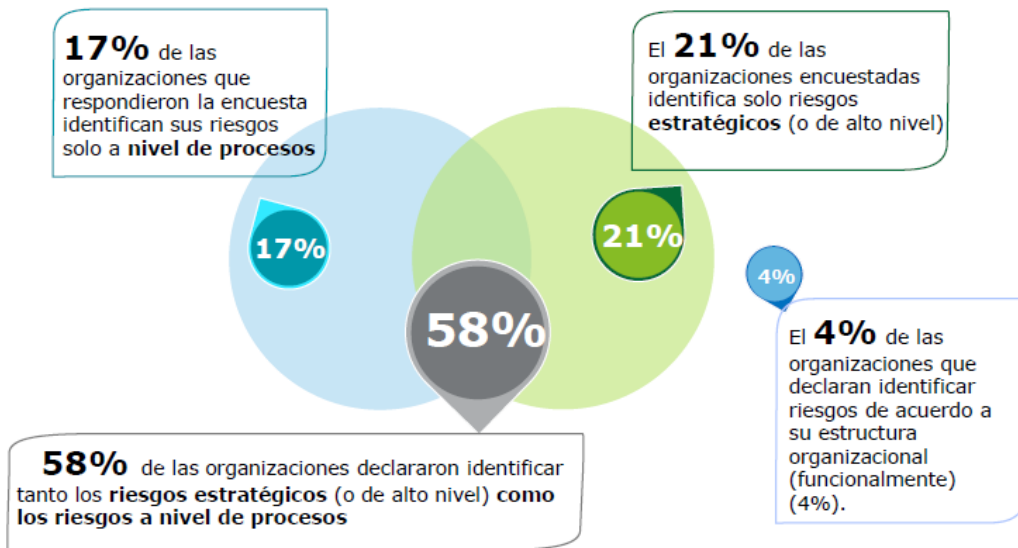
Fuente: Primer Estudio del nivel de madurez de la gestión de riesgos, Deloitte, Octubre 2017

¿Por qué las organizaciones no cuentan con un modelo de gestión de riesgos?



De las organizaciones que no poseen un modelo (25%), podemos destacar que en su mayoría se encuentran en proceso o se implementará en un futuro (80%).

23% de las organizaciones encuestadas que no posee una definición del apetito al riesgo, existiendo una variedad de enfoques disponibles para determinarlo, tanto cualitativamente como cuantitativamente:



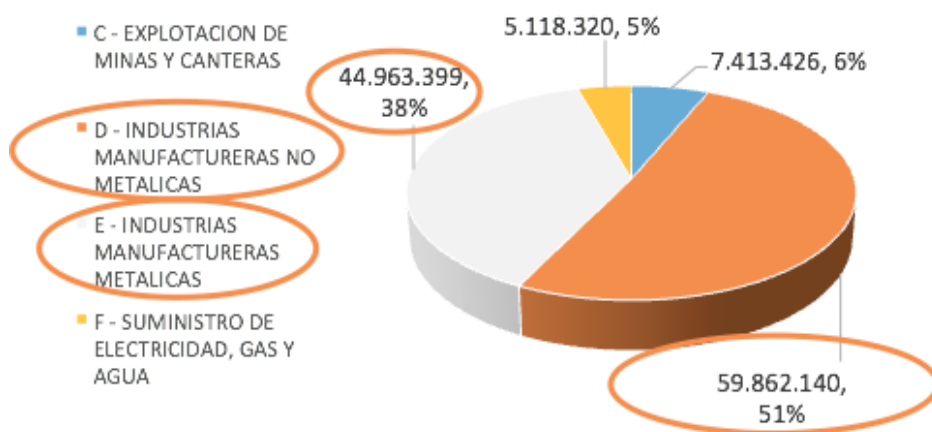
Fuente: Primer Estudio del nivel de madurez de la gestión de riesgos, Deloitte, Octubre 2017

Los resultados de esta encuesta muestran que el primer eslabón de la problemática planteada en este documento (la gestión de riesgos) es limitada en el segmento, para el cual se esperaría una gestión más avanzada considerando su robustez nivel de procesos y disponibilidad de recursos para atender una gestión tan elemental como la de riesgos.

7.2. Desafíos para las Empresas Medianas

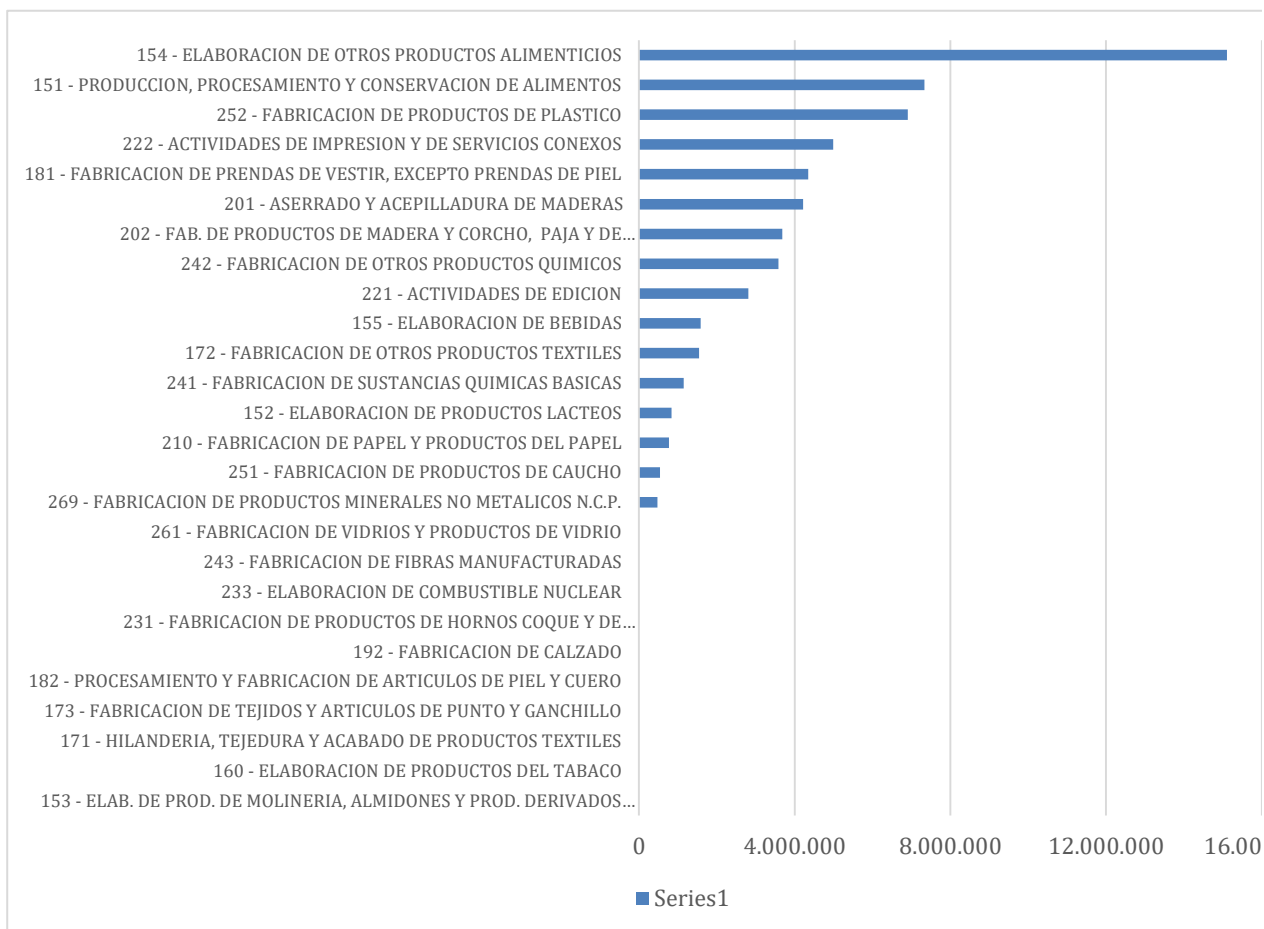
Figura 23. Sectores económicos en segmento Medianas Empresas

En el caso de empresas medianas, si bien la presencia a nivel facturación es menos relevante para los sectores vinculados a la minería y al suministro de electricidad, gas y agua, debe considerarse que se trata de empresas proveedoras de servicios para grandes empresas de estos sectores, por lo que la gestión de riesgos y continuidad es igualmente relevante en empresas de este tamaño.



Fuente: Estadísticas de Empresas por Tramo según Ventas, Rubro, Sub rubro y Actividad Económica, Servicio de Impuestos Internos, 2016.

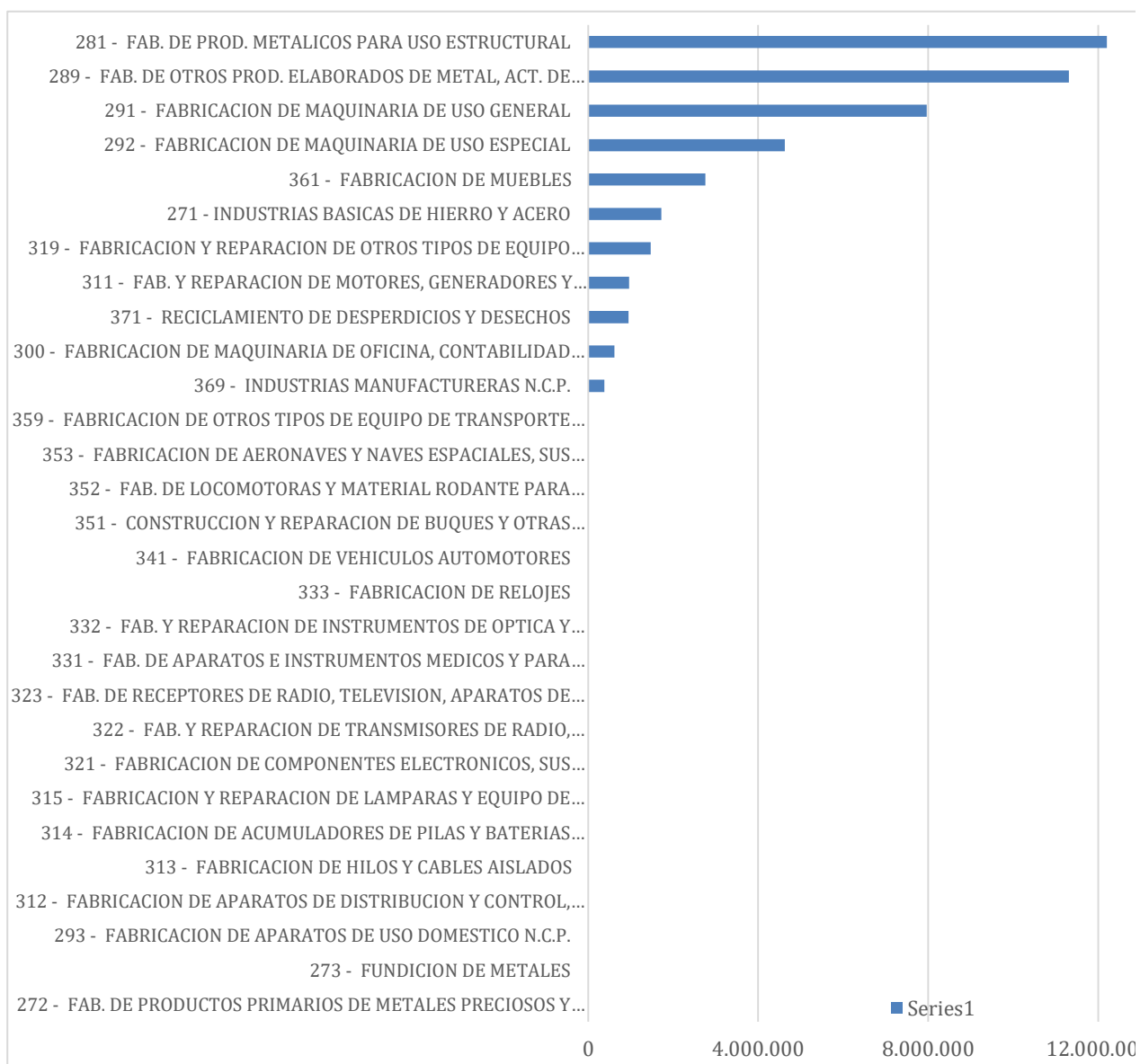
Figura 24. Sub-sectores económicos en sector “Industrias Manufactureras no Metálicas”



Fuente: Estadísticas de Empresas por Tramo según Ventas, Rubro, Sub rubro y Actividad Económica, Servicio de Impuestos Internos, 2016.

A nivel de Medianas empresas, es posible identificar sectores relevantes bajo la categoría “Industrias Manufactureras no Metálicas” e “Industrias Manufactureras Metálicas”, en particular los sectores “Elaboración de Producto Alimenticios” y “Fabricación de Productos de Plástico”.

Figura 25. Sub-sectores económicos en sector “Industrias Manufactureras Metálicas”



Fuente: Estadísticas de Empresas por Tramo según Ventas, Rubro, Sub rubro y Actividad Económica, Servicio de Impuestos Internos, 2016.

Para empresas medianas los beneficios también van en la línea de constituir un antecedente importante frente a sus propios clientes (garantía de continuidad para incorporar en contratos) lo cual constituye una ventaja competitiva real y factible de valorar económicamente, que profesionaliza y posiciona a la empresa para competir con importaciones; es un antecedente frente a la banca gracias a que apoya la garantía de los flujos operacional y

económico; constituye un antecedente frente a compañía de seguros para mejorar costo primas; es sinónimo de profesionalismo, confianza y seriedad para los *stakeholders*; y desarrolla las capacidades de prevención y respuesta internamente, dejando a los seguros como la última instancia.

Sin embargo, pueden existir resistencias o dificultades para que el segmento de medianas empresas pueda abordar y desarrollar este campo, algunos de ellos con:

- Que el tema no sea prioridad en empresas medianas, debido a la existencia de otros desafíos antes que esto: certificaciones de calidad, acceso a financiamiento, brechas en productividad, asegurar flujo de caja y capital de trabajo, competir con importaciones en el mercado interno, acceder a los mercados internacionales
- Fuerte dependencia y vulnerabilidad en empresas medianas respecto al desempeño de la macroeconomía y los ciclos del mercado interno. Medianas representan el 80% de las exportaciones de las pymes, luego cuentan con factor adicional de diversificación.
- Empresas medianas aún deben abordar etapas más tempranas de la gestión de riesgos (legales: laboral, seguridad en el trabajo)

7.3 Propuesta segmentos clave para la continuidad de negocios.

Para establecer una priorización de sectores de la economía para los cuales sería más relevante y urgente la gestión de riesgos, continuidad y crisis, se utilizarán los criterios:

7. Nivel de vulnerabilidad o exposición a riesgos y amenazas
8. Prioridad estratégica para el país debido a la naturaleza del producto o servicio y/o por la criticidad de la infraestructura involucrada en la elaboración del mismo
9. Obligación legal o regulatoria

Y a partir de una lista resumida de los sectores identificados con la información de facturación de empresas, se propone la siguiente priorización de sectores marcados en gris:

Figura 26. Resumen de recomendación de segmentos

Sector	Subsector	Nivel de vulnerabilidad	Prioridad estratégica país	Obligación legal/regulatoria
Extracción	Minería, pesca, agricultura		ALTA	ALTA
Industria/fabril	Alimentos		ALTA	ALTA
	Metalmecánico	ALTA		
	Químico	ALTA		ALTA
	Bebidas y tabaco			ALTA
	Refinación petróleo	ALTA		ALTA
	Celulosa, papel, imprenta			
	Maderas y muebles	ALTA		
	Minería no metálico			
	Textil y calzado			
	Construcción	ALTA		
	Suministro electricidad, gas, agua	ALTA	ALTA	ALTA
Comercial	Comercial			
Financiero	Banca, financieras	ALTA	ALTA	ALTA
Servicios	Hoteles y restaurantes			
	Transporte y comunicaciones	ALTA	ALTA	ALTA
	Inmobiliario			
	Admin. Pública y defensa			
	Educación		ALTA	
	Servicios sociales y de salud		ALTA	ALTA

Fuente: Elaboración propia

Los sectores marcados en gris tanto de empresas Medianas y Grandes en Chile deben abordar la oportunidad de asegurar su reputación y supervivencia. Esto ya sea por motivos de regulación, prioridad estratégica para la nación y la población, o por encontrarse en un contexto de mayor exposición al riesgo, frecuencia de amenazas, y vulnerabilidad.

En resumen, podemos identificar como segmentos objetivo a aquellos sectores de la economía en Chile en que legislación y/o regulación exige tratamiento del tema, así como también sectores para los que se proyectan modificaciones en términos de mayor rigurosidad regulatoria o legislativa.

Ejemplos de ello son los proveedores de empresas de servicios básicos o de empresas estratégicas, que en la actual discusión sobre la legislación laboral han sido declaradas como empresas estratégicas obligando a asegurar sus servicios mínimos (para la supervivencia del negocio) y profesionalizar sus

equipos de emergencia, lo que refuerza la relevancia de la continuidad de servicios no sólo para estas empresas y sus recursos internos, sino que también para sus proveedores.

Otro ejemplo son empresas proveedoras de bienes o servicios requeridos durante la ocurrencia de emergencias o catástrofes a nivel nacional, las que son rápidamente requeridas al decretarse el estado de emergencia o excepción exigiendo su respuesta inmediata con presupuestos adicionales aprobados para estos fines. Ejemplo de ello son empresas de combustibles, transporte terrestre, transporte aéreo, equipamiento de emergencia para personas, entre otros.

Otra variable de segmentación está referida a la antigüedad y madurez de la gestión de la empresa, en el sentido de que ya cuenten con procesos y operaciones establecidos y en régimen productivo por muchos años (no empresas con puesta en marcha reciente), incluso con la posibilidad de contar con una certificación ISO 9001. Esto permitiría ya contarían con un mapeo inicial procesos de acuerdo a un estándar internacional facilitando la implantación del modelo propuesto en esta tesis. Esto contempla a los segmentos de medianas y grandes empresas; en particular las del segmento medianas son de menor envergadura con cadenas de valor más pequeñas por lo tanto más factible de abordar un mapeo de procesos y desarrollar planes de continuidad y respuesta. Los beneficios estatales para Pymes para el cofinanciamiento también pueden facilitar el desarrollo del campo en este segmento.

Adicionalmente, la legislación laboral chilena se encuentra en un proceso de reforma (Reforma Laboral del año 2017, Ley 20.940) el cual entre otros aspectos, considera:

- La prohibición de reemplazar trabajadores en huelga legal
- Que una huelga puede ser indefinida
- Definir y asegurar "servicios mínimos" ente empresa y sindicatos
- Que los huelguistas deben asegurar "servicios mínimos" (equipos de emergencia)

La definición de "servicios mínimos" implica:

- Proteger bienes e instalaciones de la empresa
- Prevenir accidentes
- Garantizar servicios de utilidad pública/necesidades básicas
- Garantizar prevención daños ambientales y sanitarios

Este contexto desafía a las empresas a buscar alternativas para reducir riesgos y asegurar la continuidad mediante:

- Externalización (mandante puede caducar contrato de empresa externa en huelga, y contratar nueva)
- Administrar procesos de soporte de manera continua: Planes de continuidad/emergencia
- Obliga a sindicatos a desarrollar planes de continuidad/respuesta/emergencia

Estos antecedentes también crean un ambiente propicio para el tratamiento serio de la gestión de riesgos, continuidad de negocios y gestión de crisis en las organizaciones.

8. EXTRAPOLACIÓN A UN CASO REAL

A través del siguiente caso, se pretende justificar que la aplicación de un modelo como el expuesto en ese documento, permitiría a las empresas reducir pérdidas económicas y mitigar impactos negativos en la reputación al verse enfrentadas a un incidente que implique pérdida de continuidad pero que también derive en una crisis de reputación para la organización.

El caso aborda la situación vivida por una gran empresa del sector de distribución de energía eléctrica en Chile, y la principal de la Región Metropolitana abarcando 3 comunas, que se vio enfrentada a una crisis a partir de una situación climática de excepción en la zona central del país en julio de 2017.

8.1. Contexto y descripción del caso

El sábado 15 de julio de 2017 la zona central de Chile recibió el paso de un sistema frontal que trajo precipitaciones y una ola de frío de características extremas e inusuales para las últimas décadas. Los días previos todos los informes meteorológicos ya pronosticaban una situación climática extraordinaria: las mayores nevadas en la zona central de la última década. La Dirección Meteorológica de Chile pronosticó un descenso en las temperaturas llegando a mínimas de -3 C° la madrugada del sábado 15 de julio y una acumulación de nieve que podría alcanzar hasta 15 cm.

Bajo este escenario, Enel activó su Plan de Emergencia que incluyó entre las principales medidas el despliegue de cuadrillas de personal en terreno de hasta 8 veces su capacidad habitual de operación, la que además fue incrementada el día sábado.

La caída de nieve se inició durante la madrugada del sábado y provocó los primeros cortes desde las 5 AM superando los pronósticos oficiales y los impactos esperados por la empresa: en algunos sectores se registró más de 40 cm. de nieve; la caída de más de 350 árboles produjo daños y cortes en la red de distribución aérea; a las 8AM más de 310 mil clientes (más de un millón de personas) se encontraban sin suministro en la capital; los cortes impactaron la continuidad del servicio de telecomunicaciones (red móvil), sistemas de bombeo de agua en edificios, calefacción eléctrica, y personas con afecciones de salud y apoyo de equipos electro dependientes.

A las 7AM se constituyó el Comité de Crisis con presencia del Gerente General. Presidente del Directorio en Chile y principales ejecutivos. El actuar durante la crisis se extendió por lapso de varios días e incluyó varias falencias como se describirá en el contraste respecto a la metodología propuesta en este documento. La fuente principal de información para el caso corresponde a los medios de prensa de la época y los comunicados oficiales de la empresa.

Figura 27. Nota de prensa crisis Enel

Enel: radiografía de una crisis

Autor: Sandra Burgos

Dos apagones en un mes. Clientes furiosos, barricadas en el sector oriente, dos nuevas formulaciones de cargos, sanciones que podrían llegar a US\$ 16 millones, pago de compensaciones por cerca de US\$ 5 millones, una imagen reputacional por el suelo y una billetera obligada a abrirse para evitar que la situación se repita. Esta es la bitácora de la última crisis de Enel.



Fuente: La Tercera, sección Negocios, 23 de Julio de 2017

Antecedentes relevantes para el análisis.

1. La ocurrencia del evento era previsible, existían diversos pronósticos coincidentes, concluyentes y oficiales que indicaban la existencia de una amenaza potencial con impacto alto (con registro histórico similar de al menos 10 años)
2. El evento superó los pronósticos oficiales en intensidad e impacto, tratándose finalmente de nevazones que no ocurrían con tales características y en tal región geográfica hace al menos 45 años.
3. La afectación total fue de 337.000 hogares sin suministro de energía eléctrica (más de un millón de personas), afectando a 30 comunas de la Región Metropolitana, por más de 72 horas hasta resolver más del 95%

- de los casos, y con impacto en otros servicios como las redes de comunicación móvil.
4. Durante la ocurrencia del evento, la crisis fue agravada por:
 - poca información a clientes por los canales de atención y comunicación formales, sin indicar sectores afectados, acciones concretas en curso ni tiempos de solución
 - call center desbordado por la cantidad de llamadas recibidas (hasta 100 mil llamados atendidos en 3 días)
 - mensajes en redes sociales de ejecutivos de la compañía haciendo mención a temas ajenos a la emergencia (entre ellos, eventos de la empresa en el extranjero)
 - envío de correos y mensajería automática a clientes con publicidad y productos en oferta
 - reclamos de clientes en redes sociales y notas de prensa con menciones directas a la compañía
 5. Personal que participó directamente en atender la emergencia señaló que existían muchas órdenes cruzadas desde el Gerente General, el Presidente de la compañía en Chile y ejecutivos de la matriz regional.
 6. El Sindicato de Profesionales de la compañía envió una carta a medios de comunicación indicando que una de las causas principales de la crisis era el modelo de gestión actual de la compañía que se basa en operaciones en terreno y de atención a clientes tercerizadas, además planes sostenidos de reducción de costos en tales procesos.
 7. Además de la devolución legal a clientes por días sin suministro, la empresa se comprometió a compensar a los clientes por las extensas horas de servicio no prestado por un monto de hasta \$25.000 por cliente por día sin energía, la que la compañía declaró como una "bonificación adicional, voluntaria y extraordinaria" que en suma alcanzó los 5 millones de dólares.
 8. Las autoridades indicaron que la empresa arriesgaba multas de hasta US\$17 millones pese a la compensación entregada.

8.2. Contraste a partir del modelo propuesto

1. Apetito de riesgo

A la luz de lo ocurrido, no es posible identificar una evidencia formal de que la empresa había realizado una determinación y evaluación del apetito de riesgo que le permitiese determinar el nivel de tolerancia al riesgo y las inversiones necesarias para asegurar la continuidad y calidad de su servicio, tanto en infraestructura como en políticas, procedimientos y planes de respuesta. Para reforzar esta hipótesis, se cuenta con el antecedente de que el propio Sindicato de Profesionales de la empresa indicó a través de una carta dirigida a los medios de comunicación que "la crisis que enfrentaba la compañía era producto de los cambios experimentados en los últimos años

en su gestión y que han buscado una reducción de costos. Primero -en el 2000, cuando estaba en manos de Endesa España- con la tercerización de los servicios operativos en terreno y atención de público, dejando dentro de las empresas del grupo principalmente funciones de administración, quedando un grupo reducido de trabajadores propios dedicados a la operación” (Fuente: diario UChile, 19 de julio de 2017)

Es por ello que, bajo el planteamiento expuesto en la sección 6.2.1., de haber la compañía determinado formalmente su apetito de riesgo, **hubiese asumido la decisión estratégica de reducir costos sólo después de haberse declarado muy tolerante a asumir riesgos o con un apetito de riesgo de nivel bajo** (ver figura 14 en sección 6.2.1.) Esto es absolutamente contradictorio considerando la naturaleza del negocio y servicio que ofrece la compañía, el cual está catalogado como de primera necesidad para la población y que es además soportado por infraestructura crítica para el país. De haber declarado la compañía su apetito de riesgo como BAJO, hubiese comprendido que el esfuerzo a dedicar en planes y estrategias de continuidad debería ser de nivel MEDIO a ALTO.

Este simple ejemplo muestra la importancia estratégica de determinar el apetito de riesgo de una organización como variable que determina el esfuerzo a destinar en estrategias y planes de continuidad y respuesta, así como también de priorizar o des priorizar inversiones o tomar decisiones de reducción de costos.

2. Priorizar la preparación y respuesta

No se cuentan con los antecedentes suficientes para determinar el nivel de madurez que tenía la compañía en gestión de riesgos, continuidad y crisis. Sin embargo es evidente que de haber priorizado el desarrollo de la fase de preparación y respuesta a una emergencia o crisis, hubiese estado preparada y entrenada para atender un evento de estas características como el modelo de este documento propone: **comenzar definiendo y diseñando la estrategia de respuesta de la organización en las situaciones más extremas y de impacto transversal, asumiendo que en cualquier momento un evento disruptivo mayor podría llevar a la organización a tener que enfrentar un escenario crítico de excepción** (ver figura 15 en sección 6.2.2.)

A la fecha de ocurrida la crisis, Enel declaraba en sus memorias anuales:

- La existencia de planes integrales de calidad para las redes de alta, media y baja tensión, como medidas preventivas y de mantención de sus redes
- La existencia de planes de emergencia activados para asegurar la continuidad del servicio frente a eventos puntuales durante el año
- La implementación de Salesforce en call center para la atención de emergencias de clientes

- La existencia de un servicio de auto-atención de emergencias para clientes a través de redes sociales

(fuente: Memoria Anual Enel Distribución Chile 2016)

Sin embargo, la compañía no explicita la existencia de un Plan de Gestión de Crisis global ni de su activación periódica, pruebas o posibles resultados. El desarrollo de su actuar durante la crisis no entrega evidencias de que la empresa había realizado un proceso formal de identificación y análisis de riesgos suficiente, o ésta se encontraba desactualizada o, en caso de existir y haber arrojado riesgos como los del evento de julio de 2017, no fueron desarrolladas adecuadamente las estrategias ni los planes de mitigación, respuesta o contención de crisis.

Respecto a la estructura y orgánica de respuesta, la presencia y constitución de la plana ejecutiva como instancia de respuesta a la crisis no muestra evidencias de que se haya tratado de una situación de constitución formal y previamente declarada. Respecto a la orgánica de funcionamiento, las declaraciones del personal presente en estas reuniones mencionando que las órdenes eran diversas y cruzadas muestra que no existían definidos protocolos de actuación ni decisión ni una estructura clara de mando durante la emergencia. Estos antecedentes hacen más válida aún la necesidad de **contar con una estructura de respuesta formal y adyacente al organigrama habitual** (ver figura 16 de sección 6.2.2.1.), que no utilice los liderazgos del negocio en el día a día para la toma de decisiones a nivel operativo, sino que tenga las competencias para dar respuesta y cierre a las emergencias y crisis de forma efectiva y eficiente, y a la cual se supeditan los ejecutivos de la compañía como instancia de escalamiento y para abordar la crisis en el nivel estratégico.

Y como se expone en el modelo propuesto, en suma, a la priorización de la preparación y respuesta está la relevancia de la función de comunicaciones en compañías de tal nivel de importancia estratégica para el país. En el caso expuesto, el impacto habría sido claramente menor de contado con una función de comunicaciones entrenada para asegurar un impacto mínimo en la reputación y valoración de marca de la organización, con acciones de comunicación proactivas y de contención comunicacional con medios, prensa y redes sociales con el fin de evitar una escalada de la crisis.

8.3. Conclusiones principales

Este caso evidencia la responsabilidad y obligación de las organizaciones en ser efectivos en aquellos casos en los que con antelación se conoce de un riesgo o amenaza potencial. Podrá ser comprensible que un evento supere el nivel de impacto o la probabilidad de ocurrencia estimados, incluso cuando el proceso de evaluación se haya hecho con los antecedentes y evidencias

históricas. Pero menor comprensión habrá si tal proceso de evaluación no se ha realizado, o si frente a la evidencia de una amenaza potencial cercana no se toman las medidas de preparación y simulación asumiendo el escenario más adverso o catastrófico.

Este caso muestra que priorizar la respuesta global y transversal de toda la organización trae beneficios incalculables en términos de pérdidas evitadas. La compañía declaró una compensación adicional económica por US\$5 millones además de las multas a las que podría estar sujeta, lo que podría fijarse como base para determinar una posible pérdida económica evitada en el corto plazo. Sin embargo, la degradación del valor en el mediano y largo plazo en términos de reputación, satisfacción de clientes, presión y tensión organizacional, confianza de los empleados, opinión pública, percepción sobre la solidez del gobierno corporativo, y confianza de los accionistas, es incalculable pero significativamente mayor.

9. CONCLUSIÓN

El tema central de esta tesis ha pretendido sensibilizar a la línea ejecutiva de cualquier organización proponiendo una herramienta de gestión simple y práctica que contribuye a asegurar la viabilidad y sostenibilidad de las organizaciones, motivando a tomar decisiones en la línea de la gestión de riesgos, continuidad de negocios y gestión de crisis que deberán ser impulsadas a alto nivel.

El modelo propuesto rescata los principales elementos de la gestión de riesgos, continuidad de negocios, gestión de crisis y resiliencia, y los integra en una secuencia adaptada al escenario actual al que se puede enfrentar cualquier organización. Pero a la vez valora y responde a la urgencia de cualquier organización de contar rápidamente con medidas de blindaje y respuesta frente a disrupciones mayores, entregando una ventaja y también una base para abordar los modelos y estándares vigentes en mayor profundidad en el mediano plazo. El entendimiento del valor del modelo propuesto está dirigido a la línea ejecutiva de cualquier organización ya que expresa la importancia de asegurar continuidad y sustentabilidad tanto en el corto como el largo plazo, lo cual es finalmente la función principal de los máximos responsables de cualquier organización. La propuesta de valor del modelo se basa en ver la continuidad como un campo a desarrollar de forma integral para toda la organización haciendo foco en acciones tácticas y de rápida implementación con maximización en el uso de los recursos disponibles en la organización.

Algunas limitaciones del modelo sugieren a las organizaciones profundizar en una gestión de riesgos dedicada y que apunte principalmente a identificar el universo de riesgos a los que podría verse enfrentada la organización no sólo a partir de la historia reciente de eventos, sino que también de las tendencias en la aparición de nuevas amenazas o la variación en frecuencia e impacto de los ya conocidos. Establecer las acciones necesarias para una adecuada restauración o reconstrucción de los activos y procesos dañados por el evento, también es parte de los aspectos a revisar por las organizaciones como alcance de un modelo más amplio al expuesto en este documento. Otra dificultad reside en definir lineamientos concretos para la toma de decisiones durante un incidente, emergencia o crisis, lo cual constituye un problema bastante complejo considerando que durante un incidente la situación original de una organización cambia en términos de la disponibilidad o incluso pertenencia y estado de sus recursos, tema que escapa al alcance de este documento, pero se sugiere trabajar en una segunda fase.

Por su simpleza en los conceptos y planteamientos, es un modelo factible de implementar en cualquier organización en Chile de cualquier tamaño, pero tendrá más valor en aquellos sectores de la economía que constituyan una

prioridad estratégica para el país, que presenten altos niveles de vulnerabilidad o exposición a riesgos, y que por normativa o regulación deban contar con modelos y mecanismos que aseguren la continuidad de sus operaciones y el negocio en su conjunto.

El estudio de aplicación de los elementos del modelo a un caso chileno reciente refuerza la simpleza, pero también la fortaleza de los elementos expuestos por el modelo, sugiriendo que su aplicación es perfectamente válida en empresas de gran tamaño en Chile y cuya infraestructura sea estratégica para la nación.

El principal valor del modelo propuesto radica en su simpleza y la capacidad de alinear y movilizar la cultura organizacional de la preparación y respuesta a la vez que permite incrementar las pérdidas evitadas, en ambos casos estará contribuyendo al capital económico, financiero y humano de las organizaciones.

BIBLIOGRAFÍA

AON BENFIELD. 2017. 2016 Annual Global Climate and Catastrophe Report [en línea] <<http://thoughtleadership.aonbenfield.com/Documents/20170117-ab-if-annual-climate-catastrophe-report.pdf>> [consulta: 15 julio 2017]

ASIMET. 2016. Radiografía de la Pyme Industrial ¿Quién es la Pyme Industrial? [en línea] <http://www.asimet.cl/radiografia_pyme_industrial.htm> [consulta: 07 agosto 2017]

ESET. 2017. ESET Security Report Latinoamérica 2017 [en línea] <<https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf>> [consulta: 03 agosto 2017]

Juan Pablo Sarmiento, Gabriela Hoberman, Meenakshi Jerath, & Gustavo Ferreira Jordao. (n.d.). Disaster Risk Management and Business Education: The Case of Small and Medium Enterprises. *AD-minister*, (28), 73-90.

OBSERVATORIO DEL COMERCIO ILÍCITO, CÁMARA NACIONAL DE COMERCIO. 2016. Vulnerabilidad de Empresas en Ciberseguridad [en línea] <<http://www.cnc.cl/wp-content/uploads/2016/12/Informe-Estudio-Vulnerabilidad-de-Empresas-en-Cyberseguridad-dic-2016.pdf>> [consulta: 05 agosto 2017]

Sahebjamnia, Torabi, & Mansouri. (2015). Integrated business continuity and disaster recovery planning: Towards organizational resilience. *European Journal of Operational Research*, 242(1), 261-273.

WORLD ECONOMIC FORUM. 2017. The Global Risks Report 2017. 12th ed., [en línea] Geneva, Switzerland. <http://www3.weforum.org/docs/GRR17_Report_web.pdf> [consulta: 11 julio 2017]