

CONSEJO PROFESIONAL DE CIENCIAS ECONÓMICAS DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES

Cuadernos Profesionales

Gestión de Continuidad del Negocio

Estrategias y acciones básicas para mejorar la resiliencia en las organizaciones

Compromiso

Calidad

Supervivencia



EDICON
FONDO EDITORIAL CONSEJO



consejo

Profesional de Ciencias Económicas
de la Ciudad Autónoma de Buenos Aires

- > Gestión de Continuidad del Negocio**
Estrategias y acciones básicas para mejorar la resiliencia en las organizaciones

Consejo Profesional de Ciencias Económicas de la Ciudad Autónoma de Buenos Aires

Gestión de continuidad del negocio : estrategias y acciones básicas para mejorar la resiliencia en las organizaciones / coordinación general de Ricardo José María Pahlen Acuña.- 1a ed.- Ciudad Autónoma de Buenos Aires : Consejo Profesional de Ciencias Económicas de la Ciudad Autónoma de Buenos Aires, 2022.

Libro digital, PDF - (Cuadernos profesionales / 128)

Archivo Digital: descarga

ISBN 978-987-660-367-6

1. Administración de Empresas. I. Pahlen Acuña, Ricardo José María, coord. II. Título.
CDD 658.001

ISBN 978-987-660-367-6

1ra. Edición

Hecho el depósito que marca la Ley 11.723.

Prohibida su reproducción total o parcial
por cualquier medio sin autorización previa del autor o del CPCECABA.

EDICON Fondo Editorial Consejo

Consejo Profesional de Ciencias Económicas de la
Ciudad Autónoma de Buenos Aires

Viamonte 1549 - CABA

Tel. 5382-9200

www.consejo.org.ar

www.edicon.org.ar

> Cuadernos Profesionales

○ Agradecimiento

La elaboración de los contenidos de la presente publicación se ha encontrado a cargo de los **Dres. Ricardo Guillermo Otero, Eduardo Jorge Ochagavía, Fabián Canoni, Gabriel López Calleri, Roberto Iván Quiroga Cangiano, Jorge García Chiesa, Rita Marcela Sotomayor y Marta Chiban**, quienes se desempeñan como miembros de la Comisión de Actuación Profesional – Licenciados en Administración de este Consejo Profesional.

Agradecemos a ellos esta nueva colaboración con la Institución.

Dr. Ricardo Pahlen Acuña
Coordinador del Comité de Dirección
del Fondo Editorial del CPCECABA
Diciembre de 2022

→ **Cuadernos Profesionales**
Últimos números:

Nº 102 Manual de Gobierno Corporativo.

Nº 103 Impuesto a las Ganancias, Impuesto a la Ganancia Mínima Presunta e Impuesto sobre los Bienes Personales.

Nº 104 Impuesto a las Ganancias, Impuesto sobre los Bienes Personales e Impuesto a la Ganancia Mínima Presunta.

Nº 105 Sociedad por Acciones Simplificada (SAS).

Nº 106 Actos societarios vinculados a la emisión y aprobación de estados contables anuales.

Nº 107 El rol del profesional mayor graduado en Ciencias Económicas. Un medio de vida o un modo de vida.

Nº 108 Ajuste por inflación impositivo.

Nº 109 Factura de Crédito Electrónica (Ley 27.440). Herramientas e Instrumentos Financieros para PyME.

Nº 110 Régimen de retención del Impuesto a las Ganancias sobre rentas del trabajo personal en relación de dependencia, jubilaciones, pensiones, etc.

Nº 111 Régimen Simplificado para Pequeños Contribuyentes. Monotributo.

Nº 112 Impuesto a las Ganancias e Impuesto sobre los Bienes Personales - Acciones y Participaciones Societarias.

Nº 113 Impuesto a las Ganancias, Impuesto sobre los Bienes Personales.

Nº 114 Régimen Simplificado para Pequeños Contribuyentes. Monotributo.

Nº 115 La Responsabilidad Social Profesional del matriculado en el CPCECABA.

Nº 116 Envejecimiento y Edadismo.

Nº 117 Impuesto a las Ganancias e Impuesto sobre los Bienes Personales - Acciones y Participaciones Societarias.

Nº 118 Impuesto a las Ganancias, Impuesto sobre los Bienes Personales. Personas humanas y sucesiones indivisas. Período Fiscal 2020.

Nº 119 Práctica pericial: Aspectos teóricos y prácticos.

Nº 120 Mercado de Capitales y Financiero. Vehículo para el ahorro, la inversión y el financiamiento productivo.

Nº 121 El impacto tecnológico en las pericias contables.

Nº 122 PyMEs: Programas y Beneficios para Empresas.

Nº 123 Régimen Simplificado para Pequeños Contribuyentes. Monotributo. Nº 124 Impuesto a las Ganancias e Impuesto sobre los Bienes Personales - Acciones y Participaciones Societarias.

Nº 124 Impuesto a las Ganancias e Impuesto sobre los Bienes Personales - Acciones y Participaciones Societarias. Personas Jurídicas. Período Fiscal 2021.

Nº 125 Régimen de retención del Impuesto a las Ganancias sobre rentas del trabajo personal en relación de dependencia, jubilaciones, pensiones, etc.

Nº 126 Impuesto a las Ganancias, Impuesto sobre los Bienes Personales. Personas humanas y sucesiones indivisas. Período Fiscal 2021.

Nº 127 Actuación Judicial: Teoría y práctica

Gestión de Continuidad del Negocio

Estrategias y acciones básicas para mejorar la resiliencia en las organizaciones

○ Índice

1	○ Reseña	7
2	○ Introducción	9
3	○ Glosario	11
4	○ Formato del presente cuaderno	15
	4.1 Conocimiento de la organización respecto de cuál y cómo es	15
	4.2 Identificación de riesgos disruptivos	17
	4.3 Análisis de impacto	17
	4.4 Análisis y definición de estrategias de continuidad	18
	4.5 Respuestas a emergencias y operatividad	18
	4.6 Desarrollo e implementación de protocolos de acción (Plan de Continuidad)	18
	4.7 Toma de conciencia, capacitación y entrenamiento	19
	4.8 Ejercicios y mantenimiento	19
	4.9 Comunicaciones durante la crisis	19
	4.10 Relación con entidades externas	20
	4.11 Monitoreo de la madurez del programa	20
	4.12 Planes de Continuidad en PyMEs (experiencias, casos, lecciones aprendidas)	20
	4.13 Posibles formularios “tipo”	21
	4.14 Material de interés	21
5	○ Anexos	23
	ANEXO 1 – Contenidos básicos sugeridos para una Matriz de riesgos disruptivos	23
	ANEXO 2 – Contenidos básicos sugeridos para un relevamiento de Análisis de Impactos	25
	ANEXO 3 – Contenidos básicos sugeridos para un Informe de Impactos	27
	ANEXO 4 – Opciones básicas sugeridas como estrategias de contención	29
	ANEXO 5 – Contenidos básicos sugeridos para un Plan de Continuidad	30
	ANEXO 6 – Contenidos básicos sugeridos para un manual de comunicaciones	31

○ 1. Reseña

El objetivo de este material es brindar ayuda a nuestros Licenciados en Administración para la implementación del proceso de mejora continua referido a la Gestión de Continuidad del Negocio (GCN).

Haciendo pie en normas internacionales, en buenas prácticas que surgen desde distintos institutos especializados, y sumando nuestra propia experiencia, nos hemos propuesto acercar este tema para que pueda ser fácilmente aplicado en nuestra querida Argentina.

Dado que en nuestro país, más del 70% de los empleos es generado por mipymes y pymes, hemos intentado focalizar la temática de GCN, ajustándola a requerimientos básicos de este tipo de empresas, de forma tal que permitan la formación de protocolos de acción para continuar con sus operaciones.

Es cada vez más solicitado que las organizaciones tengan una resiliencia tal que les permita sobrevivir en distintos escenarios, y desde nuestra profesión estamos convencidos de que contamos con las herramientas necesarias para lograr ese objetivo.

Adicionalmente, tenemos que facilitar la generación de evidencias que puedan dar testimonio frente a las entidades externas que lo requieran (prospectos, clientes, bancos, reguladores, accionistas, etc.).

La lectura de este material y su puesta en marcha facilitarán llegar en buenos términos a mejorar la resiliencia de las organizaciones donde GCN sea aplicada.

¡Les deseamos lo mejor!

○ 2. Introducción

Son de público conocimiento los impactos que la pandemia causada por el COVID-19 ha provocado mundialmente y, obviamente, también en nuestro país.

El COVID-19 es **solo una de entre muchas otras amenazas** que, con origen en la naturaleza, el mercado, comportamientos sociales, etc., irrumpen cada día de manera más virulenta y globalizada en la sociedad.

La Argentina no escapa a estas amenazas que, de concretarse, degradan su industria, su comercio, sus actividades (aun aquellas sin fines de lucro o públicas), y hasta interrumpen su producción, su oferta y su distribución. Algunas organizaciones que se han visto afectadas han podido permanecer con vida y, generalmente, para lograrlo, han tenido que degradar sus servicios o productos, achicarse en muchos aspectos (inclusive a nivel de recursos humanos), y otras, lamentablemente, debieron cerrar sus puertas.

Esta problemática ha sido abordada de varias formas por diferentes tipos de organizaciones.

Existen empresas que son parte de cadenas productivas en otras empresas. Es así como aquellas empresas que son ejecutoras de la mayor parte de dichas cadenas productivas y de mayor valor agregado no pueden permitirse depender de empresas de baja resiliencia.

Si a esto sumamos una competitividad global aumentada por la pandemia, se ha generado una fuerte necesidad de acelerar su adaptación a la situación (madurando su transformación digital, identificando sus debilidades en sus cadenas de valor, inclusive sus dependencias en sus propios proveedores, etc.).

Un hecho macroeconómico y sanitario destacable es que, estando la Argentina en el hemisferio Sur, se ubica a contrafase de los ciclos climáticos, sanitarios (pandémicos) y económicos respecto al hemisferio Norte. Esto se hace aún más evidente cuando los mercados objetivos están determinados no solo por cercanía física/geográfica, sino por cercanía digital en las interacciones económicas.

Generalmente, el nivel de resiliencia promedio (capacidad de recuperación que demuestra todo ente ante situaciones de máxima criticidad que permiten su subsistencia en el futuro) con que contamos en la Argentina no resulta suficientemente maduro como para asegurar o, por lo menos, aumentar razonablemente las probabilidades de supervivencia. No es materia de análisis determinar por qué esto es así, pero claramente nos vemos en la necesidad de proponer un marco de trabajo para que esta madurez pueda ser recorrida y alcanzada siguiendo una disciplina profesional avalada por nuestro Consejo.

De entre las herramientas que orbitan con este objetivo, entendemos que el “PLAN DE CONTINUIDAD” es el que sobresale tanto por su contenido como por las habilidades que genera diseñarlo, implementarlo, probarlo y mantenerlo.

Reconocemos que además resulta sumamente necesario que la asignación de recursos en la formación de este PLAN DE CONTINUIDAD sea valorada y retribuida. Es común que no se identifique el valor agregado que estas actitudes en la organización logran con su implementación.

Es así como aquellas organizaciones que puedan contar con esta herramienta certificada profesionalmente podrán ofrecer mejores expectativas sobre la continuidad de sus servicios y productos, lo que claramente podrá concebirse como una ventaja competitiva sobre aquellas que no la gestionen. Esta ventaja, además, podrá establecerse no solo en el ámbito local, sino también en el internacional.

Fundamentalmente, los clientes podrán entender si la organización de quienes se están proveyendo está en condiciones de enfrentar desastres o incluso interrupciones que pongan en riesgo la provisión requerida, de la cual muchas veces dependen sus propias cadenas productivas. Los punitivos u otras penalidades al proveedor generalmente no llegan a cubrirlas, por lo que no resulta suficiente sostenerse en “la letra” de los contratos u otros acuerdos de servicios (Service Level Agreement, SLA).

Por otra parte, aunque existen normas internacionales y guías de buenas prácticas que facilitan la formación de estos PLANES DE CONTINUIDAD, también resulta imprescindible dimensionar sus contenidos para Pequeñas y Medianas Empresas (PyMEs), y así lograr el enriquecimiento de estas al acceder a esta disciplina adaptada a su propia realidad, tomando contenidos, formas, técnicas que ya existen y fueron generalmente adoptadas por grandes empresas o países con economías mayores.

Urge por lo tanto concientizar y equipar a los profesionales en Ciencias Económicas con herramientas y pautas que definan las expectativas de actuación en su carácter de profesionales independientes; y a la vez es fundamental concientizar y educar al mercado en la oferta de estos servicios profesionales, que consolidan e incrementan el valor de las empresas.

Entendemos que los Licenciados en Administración están cabalmente formados, capacitados y entrenados para entender y aplicar los conceptos del presente cuaderno, y, por ello, facultados para emitir opinión por sí mismos e inclusive incluyendo a otros profesionales de distintas disciplinas que participan en la formación de PLANES DE CONTINUIDAD. Esta certificación les otorgará a dichos planes una importante presunción de fiabilidad para que los interesados puedan afianzarse institucionalmente sobre su contenido.

○ 3. Glosario

Queremos remarcar tres aspectos importantes respecto a este punto:

1. NO DESESTIMAR el lenguaje y los significados de las palabras que se utilizan en esta disciplina. Suele suceder que, AUN DENTRO DEL MISMO PROYECTO, la gente que participa pretende entender por sí misma conceptos básicos y aplica sus propias definiciones y nomenclaturas. Esto es peligroso, dado que puede (y suele) ocurrir que, al concluir los relevamientos, se hayan aplicado distintos conceptos, lo que puede invalidar (total o parcialmente) el trabajo realizado. Conclusión: es muy importante que, al hablar de esta disciplina, estén todos alineados, tanto el profesional a cargo como el personal relevado.
2. UTILIZAR EL GLOSARIO GENERALMENTE ACEPTADO, que es el que se incluye en la norma ISO 22301 (*“Social Security - Business Continuity Management Systems - Requirements”*).
3. Intentaremos dar ejemplos y “alertas” sobre algunos conceptos, de manera tal que la definición contenida en dicho glosario internacional pueda ser asimilada más fácilmente al traerla a realidades más cercanas no solo de nuestra profesión, sino del usuario final de nuestro trabajo. Estos ejemplos, aunque discutibles, quizás puedan ser utilizados para el armado de parte de un curso introductorio en la organización donde se va a realizar este proyecto.

Ejemplos adaptados:

1. **Actividad (Activity*)**: El proyecto terminará generando (o aprovechando si ya existiese) una nómina de actividades con sus prioridades de recuperación, de acuerdo con su criticidad para la supervivencia del negocio. Hay que tener especial cuidado, no solo en averiguar desde un inicio si el mismo cuenta con un inventario de actividades, sino, además, si el personal (cualquiera sea su nivel) tiene internalizado el concepto de “actividad” (o proceso). Cualquier falta al respecto de estas dos variables va a significar sin duda alguna mayores tiempos en su ejecución. Puede suceder que la organización NO SEPA que trabaja “por procesos”, y esto implica hacer un trabajo de capacitación al respecto.
2. **Auditoría (Audit*)**: Es importante que quede claro que el relevamiento NO APUNTA a revisar si las actividades se hacen bien o no (tipo evaluación de auditoría) porque es necesario capturar la verdad de lo que estamos relevando. Aquí no se desea desestimar ni personal ni actividades que puedan dejar de hacerse en el día a día. Habrá que prestar especial cuidado en considerar si la organización ha realizado recientemente o, aún peor, está haciendo en ese mismo momento, algún proyecto de “reingeniería de procesos” porque puede canibalizar a nuestro proyecto.
3. **Gerenciamiento de Continuidad del Negocio (Business Continuity Management*)**: El proyecto trata de esto. Primero lo hace identificando los riesgos que amenazan a la organización (incluyendo no solo aquellos operativos); qué actividades deben retomarse; en cuánto tiempo y orden. La intención final es contar con protocolos y recursos alineados a estos para efectuar dicha recuperación. Es importante que el personal comprenda que, si la organización para la cual trabaja no puede retomar su negocio, es muy probable que ese fin de mes no pueda cobrar su honorario, sueldo, comisión, etc. La Interrupción NO es de alguien fuera de la vida del personal, sino que tiene impactos directos en la vida de cada persona que dependa de esa organización.

4. **Sistema de Gerenciamiento de Continuidad del Negocio (*Business Continuity Management System**)**: Es más amplio que el punto anterior porque pretende monitorearlo. Este tema es un proyecto en sí mismo y, si bien puede postergarse para más adelante (es decir, una vez implementada la GCN), no puede dejar de hacerse, pues deberemos estar atentos a cómo va madurando la GCN en la organización.
5. **Plan de Continuidad del Negocio (*Business Continuity Plan**)**: Son los procedimientos o protocolos específicos que armaremos para continuar las actividades que se han visto interrumpidas. Es muy importante preestablecer el nivel de detalle en que se desea describir y bajo qué supuestos se hará dicha descripción. No es lo mismo indicar un protocolo de actuación para gente que sabe de qué se está hablando que a otros que no tienen noción de lo que se tiene que hacer.
6. **Programa de Continuidad del Negocio (*Business Continuity Programme**)**: Monitoreos que se desean (y deseamos que se realicen) por parte de la Alta Gerencia para evaluar la madurez a la que está arribando la organización. Es importante preestablecer un nivel “objetivo” al que se desea llegar, el cual será más o menos ambicioso dependiendo de la penetración que este tema tenga en la organización, así como la repetitividad con que se esté haciendo (¿1era. vez? ¿2da. vez?, etc.).
7. **Mejora continua (*Continual Improvement**)**: Es importante saber que abandonar el proyecto no solo durante su ejecución, sino también una vez concluido (y no volver a tocar nada), implica que, al retomarlo, habrá que empezar NO DESDE CERO, sino DESDE MENOS QUE CERO, pues la gente que participará en su formación fácilmente detectará que lo que se está haciendo NO fue lo suficientemente importante para la alta gerencia como para mantenerlo funcionando. Esto implica que la atención que pondrá sobre el mismo irá decayendo vez tras vez.
8. **Infraestructura (*Infrastructure**)**: Facilidades que se utilizan (sean propias o contratadas) para realizar las actividades. No se refieren únicamente a temas tecnológicos (servidores, enlaces, *firewalls*, etc.), sino a TODO tipo de infraestructura (comunicaciones, edificaciones, agua, luz, gas, energías alternativas, ascensores, etc.).
9. **Partes Interesadas (*Interested Party Stakeholder**)**: Es importantísimo detenerse AL INICIO del proyecto para enumerar QUIÉNES son las partes (internas, externas, regulatorias, clientes, proveedores, accionistas...) que tienen interés en que la organización sobreviva. Obviamente, requiere mantenerse bajo observación durante toda la ejecución del proyecto para detectar posibles altas, bajas y modificaciones.
10. **Máximo tiempo tolerable de salida de servicio (*Maximum Tolerable Period Of Disruption- MTPD**)**: ¿Cuánto tiempo soporta el negocio antes de que empiecen a existir efectos adversos inaceptables por la interrupción del negocio? Raramente podrá suceder que NO haya efectos, pues estos tiempos requerirán ser “retados” (*challenger*) antes de determinarlos como finales. Cualquier atraso para llegar a ese momento tiene impactos negativos.
11. **Objetivo mínimo para continuar el negocio (*Minimum Business Continuity Objective MBCO**)**: ¿Cuál es el nivel de calidad del producto o de servicio mínimo que se puede ofrecer al continuar con el negocio, dado que no se cuenta con recursos para retomarlo plenamente?
12. **Organización (*Organization**)**: Se refiere a la gente que tendrá responsabilidad para que la organización retome sus actividades. No necesariamente son las mismas responsabilidades que se tienen en su día a día. Pueden ser roles distintos en el momento de la crisis respecto del momento habitual de trabajo.

13. **Política (Policy*)**: Está compuesta por los altos lineamientos que la Dirección suministra como marco al proyecto. Generalmente no se sabe qué lineamientos dar con excepción de dos o tres conceptos de supervivencia. Sin embargo, resulta muy importante que uno de los primeros pasos en la implementación de la GCN sea la publicación de una Política de Gestión de Continuidad del Negocio. El profesional actuante deberá componer las partes de esta política indicando en ellas los supuestos estratégicos del trabajo que va a desarrollar (estructura, organización, alcances, matriz de autorizaciones, etc.) a modo de acuerdo (a través de su publicación) con la Dirección.
14. **Productos y Servicios (Products and Services*)**: Son todos aquellos que la organización provee. Suele desestimarse aquellos productos que a ojos vista no tienen gran participación en la rentabilidad de la organización, pero eso puede cambiar y conviene que quede claro que han sido vistos, analizados y desestimados bajo qué motivos. Así, si estos motivos cambian, se podrá volver a analizar su posible inclusión en la supervivencia de la organización.
15. **Registros (Record*)**: Resulta por lo menos interesante que se establezca un modo de medir los avances que el proyecto de GCN vaya teniendo, dado que son proyectos de duración media (1 año o más si se comienza desde cero). Y no solo hay que considerar las variables para determinar el estado del mismo, sino, además, cómo agregar o quitar variables en el modelo de medición.
16. **Punto objetivo de recuperación (Recovery Point Objective RPO*)**: Hay que considerar en qué momento se necesita tener la información cuando todo esté en condiciones de retomar actividades. Es importante acordar con quienes utilizan información y considerar que además tengan claro que deberán estar en condiciones de reconstruir lo que suceda entre dicho momento y el de la caída. Esto puede obligar a contar con información diaria que quizás NUNCA sea utilizada, pero que resulta más económico mantenerla que forzar un RPO más potente (cercano al momento de la crisis).
17. **Tiempo objetivo de recuperación (Recovery Time Objective RTO*)**: Lapso en el que se debe iniciar las actividades prediseñadas de recuperación para poder llegar al máximo período de interrupción tolerable, en condiciones de actividad.
18. **Riesgo (Risk*)**: Más allá de la inmensa provisión de estándares que rigen la gestión de riesgos, se sugiere, mínima e inicialmente, trabajar sobre:
 - a. Pérdida del procesamiento de datos.
 - b. Pérdida del sitio habitual de trabajo.
 - c. Pérdida del personal clave.
 - d. Pérdida de los proveedores clave.

Y así, tomando de a uno, priorizarlo no solo por la importancia, sino por el nivel de madurez que tenga la organización para atenderlo. Adicionalmente, es muy probable que, a causa de que sea más probable un evento menor, se desee incluir riesgos “menores” pero que, a raíz de su habitualidad, se desee resolverlos urgentemente. Esto también puede servir para lograr una primera internalización de esta disciplina (GCN) en la organización.

* Glosario en ISO 22301 - **Societal Security – Business Continuity Management Systems – Requirements**

○ 4. Formato del presente cuaderno

El dictamen del profesional será su opinión formal sobre un trabajo específico realizado previamente y por otro/s profesional/es, en cuanto a que en el mismo se ha incluido cada uno de los siguientes pasos metodológicos:

4.1 Conocimiento de la organización respecto de cuál y cómo es

1. Su madurez administrativa

Es el relevamiento de ubicación o diagnóstico inicial analizando el tamaño y tipo de organización de que se trate, cómo gestiona sus operaciones, sus procesos (productivos y de servicios, administrativos, digitales, decisorios, etc.), y la relación entre ambas características (tamaño y tipo). También se debe analizar el organigrama escalar con inclusión referencial de misiones y funciones principales para ver si están establecidas manifiestamente las responsabilidades de las partes actuantes.

2. Su apetito y gestión de riesgos

Perfil de la organización respecto a los riesgos (aversión, propensión, neutral) que enfrenta, como: de precios, de mercado, de cartera de clientes, de créditos, riesgos operativos etc. Además, saber si consideró la existencia de una metodología con que se gestionan dichos riesgos, y si dicha gestión está alineada con el perfil de la organización.

3. Sus perspectivas del negocio

Movimientos estratégicos que la organización está pensando hacer como política de empresa. ¿Hacia dónde va la empresa? ¿Qué está haciendo? ¿Qué proyectos tiene en curso? ¿Con qué negocios subsiste? La visión que tiene la organización sobre sí misma; macroeconomías relacionadas; potencialidad de su mercado; posibles o potenciales fusiones, etc.

4. Su competencia

Si la organización tiene claramente identificada a su competencia y si monitorea cuál es su resiliencia. Debería haber analizado si dicha capacidad genera una ventaja/desventaja competitiva de la organización respecto a sus competidores.

5. El perfil de su cliente

Considerar lo siguiente: Cuán flexible es el cliente a aceptar demoras en los servicios/productos. Cuán fiel es a la empresa bajo análisis. Qué busca en el producto o servicio que le adquiere (calidad, precio, etc.). Detectar cuán crítica es la empresa para los procesos productivos o de comercialización del cliente.

6. La comunidad interesada en la organización (*stakeholders*)

Ver si ha identificado el contexto interesado en la empresa (accionistas, vecinos, personal propio y contratado, proveedores, clientes potenciales, el público, otros posibles consumidores, mercado y otras comunidades interesadas -afectadas directa o indirectamente- en general).

7. Los productos y servicios que genera

Identificación del producto/servicio/s “estrella” y aporte en la rentabilidad de la empresa. Estacionalidades relacionadas con el consumo y con las materias primas que se utilizan.

Adicionalmente, la existencia de un mapeo de procesos que incluya el denominado “Diagrama de flujo de procesos”, que permita facilitar la identificación y análisis de situaciones de criticidad en la operatividad de los procesos núcleo y de soporte.

8. El gobierno de su tecnología

Cuán fuerte es para soportar incidentes, qué ejercicio tiene. El nivel de monitoreos que efectúa, el nivel de madurez que tiene su ciclo de desarrollo de sistemas.

La existencia de planes de acción implementados para casos de interrupciones severas en la automatización regular de los datos, a través de una contención adecuada (por ejemplo: la suplantación por medios informáticos y/o manuales), hasta su solución.

9. Las regulaciones y leyes que le son aplicables

Esto tiene que ver con la vigilancia que la organización recibe de parte de regulaciones y leyes que deba cumplir. También deberá haber identificado posibles mandatos de casas matrices.

10. La madurez de su Responsabilidad Social Empresaria (RSE o CSR, *Corporate Social Responsibility*) y de sus Comunicaciones (internas, externas, formales, informales)

Qué nivel de madurez tiene la organización para comunicarse y para comprender lo que le está aconteciendo.

11. La madurez en su gestión de la seguridad (física, digital)

Cómo relaciona sus medidas de seguridad con un análisis de riesgos previo y sus niveles de implementación y monitoreo de las soluciones diseñadas a tal efecto.

12. La gestión de sus instalaciones

En cuanto a la responsabilidad que tiene la empresa sobre sus propias instalaciones (edificio, locales, facilidades, etc.) y cómo las ejerce (monitoreos, resolución de incidentes, seguros, etc.). Posibles instalaciones compartidas con otras organizaciones y distribución de la responsabilidad sobre las mismas (ejemplo: consorcios de copropietarios).

13. Los principales activos a ser protegidos

Cuáles son y si existe alineamiento de su valoración entre los distintos niveles y responsables en la organización.

14. Los esquemas contables y de imputación de pérdidas operativas

En cuanto a si la responsabilidad sobre las gestiones administrativas de la organización es claramente identificada frente a las pérdidas o si estas se diluyen evitando un posible tratamiento *postmortem* de la misma. Adicionalmente, la madurez presupuestaría que tenga la organización y, de existir, cuál ha sido la asignación de recursos para mejorar su resiliencia.

4.2 Identificación de riesgos disruptivos

El profesional actuante ha identificado los principales riesgos disruptivos que amenazan a la organización y los ha evaluado de acuerdo con una metodología aprobada por las máximas autoridades de la misma.

Mínimamente, los 4 escenarios que debieron haberse analizado son:

- a) Pérdida de las facilidades para el procesamiento de datos u otras facilidades tecnológicas en uso, incluyendo la confidencialidad e integridad de los datos e información que la organización tiene bajo su responsabilidad.
- b) Pérdida de las facilidades donde se realiza el trabajo (edificio, trabajos remotos, etc.).
- c) Pérdida del personal clave.
- d) Pérdida de proveedores clave.

De ser posible, en el caso de que la dimensión del proyecto inicialmente autorizada lo hubiese incluido, debieron también identificarse riesgos parciales o combinatorios, los cuales, si bien son de impactos más específicos y quizás de menor tamaño, seguramente será mucho más probable que ocurran.

Adicionalmente, es importante que se haya evaluado el grado de madurez que tiene el nivel operativo de la organización para gestionar este tipo de riesgos (si es o no proclive a identificarlos, evaluarlos y tratarlos), así como también sobre si existe capacitación, entrenamiento y difusión para la toma de conciencia y así madurar dicha gestión operativa. Por último, se debió analizar si esta gestión está alineada con el apetito al riesgo definido desde las más altas autoridades.

4.3 Análisis de impacto

El profesional actuante ha identificado los principales productos y servicios que permiten sobrevivir a la organización en crisis, con sus procesos y recursos asociados, de manera tal de priorizar qué deberá mantenerse funcionando durante la contingencia y a qué nivel de calidad.

Un punto a considerar consiste en evaluar si el profesional actuante ha analizado los recursos hasta un nivel de identificación tal que permita accionar **sobre** los responsables de los mismos. Si los recursos son identificados sin mayor detalle, será más complicado asignar responsabilidad sobre quién deberá gestionar cambios en los mismos.

Durante el análisis de impactos que las interrupciones operativas puedan generar en la organización, es muy importante determinar cuáles son los tiempos “soportables”, dado que, a mayor apuro en la solución, mayores serán seguramente los costos asociados a conseguir dicha rapidez. Una vez identificados los procesos críticos y los tiempos en que deben ser retomados luego de su interrupción, también deben analizarse las relaciones entre ellos y los recursos que utilizan, ya que puede suceder que un recurso que se usa para un proceso crítico también sea empleado para otro no tan crítico. De esa manera, al hacer sobrevivir dicho recurso, estarán sosteniéndose ambos procesos, siendo que el segundo no genera un gasto adicional al primero.

Este análisis debió ser obtenido en el nivel operativo, pero ha de ser validado por las gerencias intermedias y, de ser posible, por la Alta Gerencia también. Es muy normal que esta etapa metodológica detecte “ruidos” entre las capas de la organización identificando valoraciones que disientan entre las mismas sobre un mismo proceso.

Por último, debe considerarse que los Impactos pueden recaer fuera de la organización y aun también en varias “capas” a posteriori de los clientes directos de la misma (efecto “cascada”).

4.4 Análisis y definición de estrategias de continuidad

Una vez identificados, y priorizada la recuperación de los procesos, debe establecer claramente cuál será el tiempo objetivo de recuperación. Determinar en qué momento deben iniciarse las actividades de re-establecimiento, de manera tal de “llegar” a cubrir los procesos que deben retomarse, y cuáles/cuántos pueden dejarse sin cubrir (dado que requieren tal premura en forma puntual que no resulta económico a la organización llevar toda su recuperación a ese tiempo, y por lo tanto, se deberán retomar “de otra manera” hasta tanto el grupo mayor de recursos esté disponible).

Es una buena práctica analizar si el tiempo objetivo al que se ha arribado es coherente con los niveles actuales de custodia con que cuenta la organización. Nos referimos a, por ejemplo, si la organización determina que no puede estar más de dos horas sin operar determinados procesos, y, sin embargo, en su giro habitual de negocio, no cuenta con guardias que custodien dicho lapso, puede ser que, o bien deba implementar dicha guardia o que las dos horas son demasiado estresantes y en realidad no es necesario semejante nivel de respuesta.

De existir varias alternativas de recuperación, debieron haberse analizado mediante distintas herramientas (por ejemplo: FODA, matrices de decisión, etc.) para determinar cuál es la que mejor se adapta a la organización. Como en todas las cosas, el crecimiento y la madurez de cada ente deben ser armoniosos, por lo que no tiene sentido invertir para obtener tiempos sumamente estrechos y que la organización se mantenga con debilidades administrativas, o incluso de recursos humanos que no aseguren razonablemente la implementación de este tiempo.

Demás está decir que se debe tener en cuenta que todas las definiciones y/o alternativas de recuperación a implementar deben ser consistentes con la ecuación costo-beneficio que debe analizarse sobre cada una de estas. Obviamente, toda la información recogida al conocer la organización debe ser utilizada durante este análisis, quizás como en ningún otro punto metodológico.

4.5 Respuestas a emergencias y operatividad

Una vez determinada la estrategia de cómo la organización decidió abordar el problema y solucionarlo, cabe avanzar con protocolos de emergencia que sean los que deberán llevarse a cabo en el momento del impacto y posteriores.

Estas “respuestas” son a modo de “RCP” (Reanimación Cardiopulmonar) de la organización y debieron haberse armado por evento a cubrir, activo en cuestión, momentos de ocurrencia, etc.

Ha de haberse definido no solo *script* de comunicaciones, sino, además, responsables, formatos, tiempos de actualización, resultados esperados.

4.6 Desarrollo e implementación de protocolos de acción (Plan de Continuidad)

Las instrucciones a seguir para recuperar la operación de la organización, más allá de los primeros protocolos de emergencia, deben haberse diseñado cubriendo los tiempos objetivos de recuperación, los momentos en los que la información deberá ser hallada para dicha recuperación, responsables, cadenas de mando, encadenado de pasos a seguir, tiempos esperados de ejecución, recolección de errores y problemas para generar “lecciones aprendidas”, puntos de control intermedios, rendiciones de avances a comités de trabajo creados a tal efecto (fundamentalmente, el Comité de gerenciamento de la crisis).

4.7 Toma de conciencia, capacitación y entrenamiento

La existencia de un plan de capacitación y entrenamiento de la gente, indicando alcance de la capacitación y cantidad de colaboradores involucrados, es un requisito para coadyuvar a la continuidad del funcionamiento de la entidad. La evidencia de capacitaciones y simulaciones de casos será parte importante del informe de Gestión de Continuidad.

Es más, será un punto importante para evaluar el compromiso del personal y, sobre todo, DE LA DIRECCIÓN, pues la asignación de recursos que les den a estos temas es una muestra de la presencia que tiene este tema en la mente de la Alta Gerencia.

La continuidad del negocio es responsabilidad de todos los miembros de una organización.

Enumeramos aquí algunos ítems a evaluar de la capacitación o entrenamiento (enumeración no taxativa):

- Departamentos capacitados (cobertura de áreas de la organización).
- Porcentaje de personas entrenadas en función de la nómina, del nivel jerárquico, etc.
- Frecuencia de las capacitaciones.
- Registros/evidencia de ellas y de que la gente que ha asistido ha entendido el tema.
- Temas tratados.

4.8 Ejercicios y mantenimiento

Así como son habituales por normas de seguridad e higiene los simulacros de incendio, efectuar simulaciones de situaciones críticas para probar los procedimientos de contingencia es una forma de hacer eficientes las respuestas preestablecidas.

Confirmar la existencia y conocimiento práctico de aquellos que los deben llevar adelante, de procedimientos de resguardos de base de datos, su locación alternativa, tiempos que se demora en dejarlos disponibles, si los usuarios están en condiciones de reconstruir registros y desde qué momento, y cuánto tardan en dicha reconstrucción, aspectos legales asociados al mantenimiento de dichos resguardos, etc.

Es requisito asimismo contar, a modo de evidencia, con un registro del resultado de estos entrenamientos (impactos evidenciados en los riesgos analizados, verificación o modificación del riesgo residual estimado, etc.)

4.9 Comunicaciones durante la crisis

Este ítem comprende, a modo preventivo, no solo la previsión y provisión de canales de comunicación para los períodos de crisis, sino también la comunicación en sí.

En otras palabras, es el análisis de la disponibilidad de las vías de comunicación y de la existencia de la comunicación en sí misma. Los recursos humanos (dentro y fuera de la organización) son el principal activo de una organización (colaboradores, clientes, proveedores, inversores, etc.), y como tal se debe garantizar la mejor comunicación posible.

El informe deberá contener el detalle de la existencia de plan de comunicaciones, y simulaciones de uso en caso de haberse realizado, salvaguardando la confidencialidad pertinente en la organización.

Es importante incluir la posibilidad de comunicaciones “fuera de banda” para los casos en que las comunicaciones de formato habitual y conocido no sean posibles. Entendemos por aquellas la disponibilidad de canales alternativos para comunicaciones de emergencia, que son conocidos por el personal, pero que sólo serán utilizados en situaciones de emergencia. Si quisiésemos indicar un ejemplo, podríamos referirnos a crear perfiles normalmente durmientes en redes sociales públicas, pero que se usan para comunicar al personal en situaciones críticas, y que estos saben reconocer como canales autorizados de la organización. La idea es doble: por un lado, contar con un canal alternativo y, por el otro, que ante una situación de emergencia donde los canales formales de comunicación no estén disponibles, el personal sufra *phishing*, manipulación, confusión y/o otra comunicación fraudulenta por información que les llega por canales públicos que PRETENDEN provenir de la organización.

4.10 Relación con entidades externas

Como se expresó más arriba, la organización no actúa sola, sino que lo hace en un contexto (sociedad, mercado, etc.), en el que interactúa con otras organizaciones y personas (competidores, proveedores, organismos públicos, bancos, etc.), con las cuales debe mantener comunicación aun (y especialmente) en situaciones de crisis.

El informe del profesional debe incluir los planes de continuidad de comunicación con terceros para minimizar el riesgo de cortes de cadenas de pagos (proveedores, salarios, etc.), de entrega de productos o servicios, de provisión de insumos, etc.

4.11 Monitoreo de la madurez del programa

Existen modelos que permiten evaluar objetivamente el estado de la organización respecto a la GCN. Estos modelos pueden además sistematizarse utilizando herramientas de OFIMÁTICA que permitan aplicarlos más fácilmente y obtener valores comparativos en el tiempo para detectar avances/retrocesos en el programa.

También nos permitirá responder las siguientes preguntas clave que provengan de la Alta Dirección de las empresas:

1. ¿Dónde estamos hoy? (¿Qué nivel de madurez del programa Continuidad del Negocio poseemos?)
2. ¿Cuál es el objetivo que buscamos? (¿Qué nivel de madurez del programa de Continuidad del Negocio necesitamos tener?)
3. ¿Cuál es el camino de madurez por el que debemos transitar para llegar ahí? (¿Cómo debemos progresar más efectivamente al siguiente nivel? Por ejemplo, primero avancemos lentamente, después caminemos y finalmente corramos)

4.12 Planes de Continuidad en PyMEs (experiencias, casos, lecciones aprendidas)

La implementación de un programa de Gestión de Continuidad del Negocio tiene idénticos retos, amenazas, objetivos, protagonistas, etc., tanto en grandes empresas como en PyMEs. Sólo que el “tamaño” de cada uno de ellos es diferente y claramente asociado al tamaño de la organización de que se trate.

Un punto en común es que este tipo de proyectos evidencia OTRAS DEBILIDADES ADMINISTRATIVAS, que si bien no tienen que ver con esta disciplina, le impactan directamente. Por ejemplo: si una organización no tiene un buen gobierno de su propia tecnología y, por lo tanto, entre otras debilidades, no cuenta con buenos resguardos de información, esta debilidad impedirá certezas al momento de recuperarse frente a

una crisis. Es por ello que estos proyectos pueden ser “reveladores” y muchas veces “antipáticos” para la organización.

Dicho esto, es importante dejar en claro desde un principio que los objetivos a alcanzar deben ser claros, concretos y de alcance limitado/razonable para el nivel de madurez INTEGRAL que tenga la organización.

Además, puede aprovecharse este proyecto para introducir mejoras en otras disciplinas a medida que vayan surgiendo las debilidades (sobre todo durante el diagnóstico inicial).

Es fundamental e ineludible que el proyecto esté apadrinado desde la Alta Gerencia y con un nombre visible, tanto en reuniones como en comunicaciones al personal y evaluaciones de su desempeño durante su realización.

Otra experiencia habitual es que a veces se pretende que TODO sea importante y, por lo tanto, TODO debe sobrevivir. Esto NO puede ser cierto o por lo menos NO puede ser aceptado. A lo sumo, deberán plantearse objetivos de menor alcance pero realizables (“Los elefantes se comen de a poco” o, como diríamos en términos de capacidades, “mejor lisiado que muerto”).

4.13 Posibles formularios “tipo”

- a) Contenidos básicos sugeridos para una Matriz de riesgos disruptivos (Ver Anexo 1).
- b) Análisis de Impactos (Ver Anexo 2).
- c) Contenidos básicos sugeridos para un Informe de impactos (Ver Anexo 3).
- d) Opciones básicas sugeridas como estrategias de contención (Ver Anexo 4).
- e) Contenidos básicos sugeridos para un Plan de Continuidad (Ver Anexo 5).
- f) Contenidos básicos sugeridos para un manual de Comunicaciones (Ver Anexo 6).

4.14 Material de interés

TIPO	NOMBRE	SITIO
NORMAS	ISO 22301 - Societal Security - Business Continuity Management	www.iso.org
NORMAS	ISO 22313 - Security And Resilience — Business Continuity Management Systems — Guidance On The Use of ISO 22301	www.iso.org
NORMAS	ISO 22316 - Security and Resilience — Organizational Resilience — Principles and Attributes	www.iso.org
NORMAS	ISO 22317 - Societal security – Business continuity management systems – Business impact analysis	www.iso.org
NORMAS	ISO 22318 - Security And Resilience — Business Continuity Management Systems — Guidelines For Supply Chain Continuity Management	www.iso.org

TIPO	NOMBRE	SITIO
NORMAS	ISO 22319 - Security And Resilience — Community Resilience — Guidelines For Planning The Involvement of Spontaneous Volunteers	www.iso.org
NORMAS	ISO 22320 - Gestión de emergencias - Respuesta a incidentes	www.iso.org
REGULACIÓN	BCRA - COM "A" 4609 Requisitos Mínimos de Gestión, Implementación y Control de los Riesgos Relacionados con Tecnología Informática, Sistemas de Información y Recursos Asociados para las Entidades Financieras	www.bcra.org.ar
REGULACIÓN	BCRA - COM "A" 4793 Lineamientos para la gestión del riesgo operacional en las entidades financieras	www.bcra.org.ar
SITIO	Asociación Latinoamericana de Continuidad	www.alcont.org
SITIO	Banco Interamericano de Desarrollo www iadb org/countries	www.iadb.org/intal
SITIO	Banco Mundial	www.worldbank.org
SITIO	British Standard Institution	www.bsigroup.com
SITIO	Business Continuity Institute	www.thebci.org
SITIO	Centro de Información Química para Emergencia	www.ciquime.org.ar
SITIO	Comisión Económica para América Latina y el Caribe (CEPAL)	www.cepal.org/argentina
SITIO	Comité Internacional de la Cruz Roja	www.cicr.org
SITIO	Cruz Roja Argentina	www.cruzroja.org.ar
SITIO	Dirección Nacional de Emergencias Sanitarias	www.msal.gov.ar/dinesa
SITIO	Dirección Nacional de Protección Civil	www.proteccioncivil.org.ar
SITIO	Disaster Recovery Institute International	www.drii.org
SITIO	Federación Internacional de Sociedades de la Cruz Roja	www.ifrc.org
SITIO	Fondo de las Naciones Unidas para la Infancia (UNICEF)	www.unicef.org/argentina
SITIO	Instituto de Racionalización de Materiales	www.iram.org.ar
SITIO	Instituto Nacional de Prevención Sísmica	www.inpres.gov.ar
SITIO	Oficina de la Secretaría General de la Organización de los Estados Americanos (OEA)	www.oas.org
SITIO	Organización de Estandarización Internacional	www.iso.org
SITIO	Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO)	www.unesco.org
SITIO	Organización Panamericana de la Salud (OPS-OMS)	www.ops.org.ar
SITIO	Programa de Naciones Unidas para el Desarrollo	www.undp.org.ar
SITIO	Red Toxicológica Argentina	www.msal.gov.ar/redartox
SITIO	Sistema de Atención Médica de Emergencia	www.same.gov.ar

○ 5. Anexos

ANEXO 1 – Contenidos básicos sugeridos para una Matriz de riesgos disruptivos

El objetivo de esta matriz es volcar en ella en forma metodológica (en el formato y método que utilice la organización para la gestión de todos sus riesgos) aquellos riesgos disruptivos que se hayan identificado y sus características.

RIESGO DISRUPTIVO	TOTAL O DEL SECTOR (PARCIAL)	IMPACTO	FRECUENCIA	RIESGO INHERENTE	NÓMINA DE MITIGANTES ACTUALES	CONTROL	RIESGO RESIDUAL	MARCA DE EXIGENCIA REGULATORIA	MITIGACIONES ADICIONALES A ANALIZAR	ESCENARIO QUE GENERA	PLANES DE ACCIÓN (*)	ESTRATEGIA DE CONTENCIÓN ASOCIADA AL ESCENARIO
FUEGO, EXPLOSIONES	TOTAL	ALTO	RARO	MODERADAMENTE ALTO	Contamos con: 1. Detectores de humo. 2. Matafuegos. 3. Red de Incendios. 4. Pulsadores de alarmas. 5. Bomberos de piso. 6. Alarma con bomberos de la zona. 7. Ejercicios y testeos habituales. 8. Bomberos de la Policía Federal. 9. Manual de evacuaciones del edificio y de acciones frente al fuego y otras amenazas.	FUERTE	MODERADAMENTE BAJO	SÍ	Guardias nocturnas sobre zonas de alto riesgo. Monitoreos habituales de los sensores y otros elementos de lucha contra el fuego.	Dependiendo del lugar del incendio, la pérdida del recinto y hasta todo el edificio	NO	Establecer sitios alternativos de trabajo de concretarse el riesgo, incluyendo la posibilidad de trabajo remoto.
Tormentas, huracanes y vientos fuertes												
Inundaciones, diluvios												
Terremotos												
Pandemias												
Ausentismo/interrupción del transporte público, piquetes												
Paro general del personal de la organización												
Terrorismo, amenazas químicas o biológicas												
Ciberataques												
Falta de energía eléctrica												
Caída del data center primario												
Pérdida de las telecomunicaciones												
Falla en el sistema principal de la organización												

Corte del suministro de Internet
Salida del servicio de la impresora del sector
Pérdida del sitio de trabajo
Robo y daños intencionales

(*) Se define que deberá contener plan de acción aquel riesgo cuyo valor residual se considere “ALTO” o bien, cuando existan exigencias regulatorias que indiquen la obligatoriedad de su armado.

ANEXO 2 – Contenidos básicos sugeridos para un relevamiento de Análisis de Impactos

El objetivo de esta matriz es obtener, a partir de la nómina de productos-procesos-subprocesos de la organización, una evaluación de los impactos que generaría la interrupción del mismo, bajo distintos ejes de análisis (por ejemplo: Financiero, Imagen y Reputación, Comercial, Regulatorio/Legal), para darle un puntaje a cada uno y luego determinar cuáles deben sobrevivir frente a una crisis.

Como esta información seguramente será relevada en cada sector de la organización, deberá considerarse tabulados los que, al momento de tener que integrar toda la información, permitan un análisis uniforme.

ID Proceso	Producto	Proceso	Subproceso	Impacto Financiero		Impacto en Imagen y Reputación		Impacto Comercial		Impacto Regulatorio y Legal		Scoring del proceso en el Sector	Críticidad del proceso	Máximo Período de Interrupción Tolerable (MPIT)
				Descripción	Significado	Descripción	Significado	Descripción	Significado	Descripción	Significado			

A partir de esta nómina, deberá obtenerse la lista de recursos que hacen falta para ejecutar dichos procesos, tales como:

PROVEEDORES QUE INTERVIENEN EN EL PROCESO:

Producto – Proceso - Subproceso	Nombre del Proveedor	¿Tiene Contingencia (BCP)?	¿Fue testeada en los últimos 12 meses?	Nivel de criticidad de la dependencia	Datos del contacto y eventuales horarios	Contacto interno con el proveedor

PERSONAL ASIGNADO:

Nombre y Apellido	ROL	INTERNO / EXTERNO	MARCA DE URGENTE Necesario dentro de los primeros 3 días (D+1 a D+3)	MARCA DE IMPORTANTE Necesario dentro de los siguientes 4 a 10 días (D+4 a D+10)	MARCA DE NECESARIO Necesario a partir de los 10 días y mientras dure la contingencia (>D+10)	Posible personal sustituto (BUP)	¿Tiene recursos para trabajar en forma remota?

PUESTOS DE TRABAJO:

Producto- Proceso- Subproceso	Cantidad total de puestos de trabajo (regulares)	Cantidad mínima de puestos de trabajo (contingencia)	Descripción de puesto de trabajo "especial" que sea necesario explicar	Sitio tentativo donde necesito estos recursos (URS, Domicilio, otro)	# Puestos necesarios el 1er. día (D + 1)	# Puestos necesarios el 2do. día (D + 2)	# Puestos necesarios el 3er. día (D + 3)	# Puestos necesarios del 4to. al 10mo. día (D + 4 al D + 10)	# Puestos necesarios a partir de los 10 días (>D+10)

APLICACIONES:

Producto- Proceso- Subproceso	Nombre de la Aplicación	¿Es CRÍTICA la aplicación para el proceso que soporta?	RTO Aplicación según TI	MPIT Aplicación según usuarios	RPO Aplicación según TI	RPO Aplicación según usuarios	¿Está en el sitio alternativo de procesamiento?	¿ACCESIBLE POR VPN SEGÚN TI?

REGISTROS VITALES:

Producto- Proceso- Subproceso	Identificación del Registro Vital	Medio en que se soporta el registro	Ubicación del Registro Vital	Ruta completa del Registro Vital	¿El registro vital tiene resguardo? ¿Dónde?	¿El personal asignado posee este recurso en su sitio alternativo de trabajo?

OTROS RECURSOS NECESARIOS:

Producto- Proceso- Subproceso	Descripción de Recurso	Criticidad del Recurso	Cantidad Total para afrontar la contingencia	¿El personal asignado posee este recurso en su sitio alternativo de trabajo?

ANEXO 3 – Contenidos básicos sugeridos para un Informe de Impactos

A partir de la información obtenida a través de los BIAs, se deberá efectuar un informe que permita mínimamente responder las siguientes preguntas:

¿Cuáles son los productos/procesos que más y mejor contribuyen en la supervivencia de mi entidad?

Esta pregunta está relacionada con la necesidad de conocer cuáles son los procesos que deben sobrevivir y a qué nivel de calidad, sí o sí, frente a cualquier crisis porque son los que realmente sostienen a la organización. Esto nos servirá para determinar el alcance de nuestra continuidad. Cuanto más amplio sea este alcance, mayores costos tendremos que enfrentar. Así que, cuanto más certeros seamos en definir cuáles son, habrá menores costos.

Se debe obtener una nómina de procesos ordenados por criticidad como para confirmar hasta dónde se desea mantener supérstites en situación de crisis e ir y venir en el *tunning* por esta lista hasta que todos los responsables estén de acuerdo en que son esos y solo esos procesos que haremos sobrevivir y en qué nivel de calidad.

Es conveniente comparar visiones de los procesos entre la Alta Gerencia y las gerencias operativas de manera tal de confirmar que todos “están viendo” la misma organización. Cuando existen visiones diferentes, hay que buscar su alineamiento.

¿Todos los que participan en las actividades de la entidad han entendido y conocen las actividades que se realizan?

Si quienes realizan las actividades de la entidad no reconocen los procesos que se efectúan en ella, podemos tener el serio problema de “estar hablando” de distintas cosas y no darnos cuenta de ello.

Hay que detectar si existen procesos que, se supone, son realizados en la entidad, pero que en realidad NADIE se los ha apropiado; es decir que NADIE dice hacerlos. ¿Son reales? ¿No fueron identificados? ¿Han dejado de hacerse?

¿En cuánto tiempo debo recuperarme y retomar mis actividades para que tenga los menores impactos posibles?

Cuanto más pronto necesite recuperar mis actividades, mayores costos tendré que enfrentar para conseguir llegar a ese punto.

Es importante consultar cuántos procesos y de qué criticidad estaría dejando sin retomar si decido reanudar en un “momento N”. Por ejemplo: si decido retomar en 4 días (no antes), estaré dejando de atender “X” procesos de criticidad, por ejemplo, “alta”. ¿Eso es aceptable? ¿Cuáles son? ¿Dónde se ejecutan?, etc.

De esta manera, podremos decidir el retorno de la mejor manera y decidir si conviene apurar nuestra recuperación buscando más rapidez, o bien (dado que “son pocos” los procesos que desatiendo), buscar una solución alternativa. En definitiva, ABARATAR mi costo de recuperación.

¿Cuáles de mis procesos pueden ser realizados en forma remota? ¿Hay historia al respecto? ¿Cuáles inicialmente no podrían hacerse de esa forma y debería rediseñarlos para ello?

Frente al escenario de pérdida del sitio de trabajo (sea porque no existe o porque no podemos concurrir todos al lugar, por ejemplo, para cumplir con requerimientos de distanciamiento social), deberemos iden-

tificar cuáles son los procesos que inicialmente NO ACEPTAN ser ejecutados en forma remota para rediseñarlos en forma puntual. También habrá que detectar qué sistemas no están preparados para trabajar en forma remota, pero sostienen procesos que sí lo están. Este desalineado puede ser fatal a la hora de hacer sobrevivir ese proceso.

¿Qué recursos debo considerar tener disponibles para sostener mis procesos críticos?

Cuáles son los “**proveedores**” que colaboran o sostienen directamente mis procesos críticos, así como también las “**aplicaciones**” que se necesitan, la cantidad de “**puestos de trabajo**”, los “**sectores**” que deben sobrevivir, “**personal**”, “**otros recursos**” (como lo son los registros vitales, gabinetes ignífugos), etc.

Esta identificación permitirá investigar si existen debilidades en estos recursos y así poder gestionar su fortalecimiento.

Por ejemplo:

Proveedores: ¿Quiénes no tienen cláusula de continuidad acordada? ¿Quiénes me “adeudan” información sobre sus tests? ¿Quiénes participan en procesos que requieren una disponibilidad más inmediata que otros? (eso nos permitirá advertir si nuestro proveedor está alineado con nuestros tiempos necesarios de recuperación)

Aplicaciones: ¿Qué sistemas críticos aún no tienen un lugar alternativo de procesamiento? ¿Cuáles se recuperan en forma más tardía de lo que el negocio puede soportar? ¿Cuáles no dependen de nuestra organización y deberíamos confirmar si se recuperan y en cuánto tiempo/momento?

Puestos de trabajo: ¿Qué tipos de puestos de trabajo se requieren para mis procesos críticos? ¿En cuánto tiempo y en qué cantidad?

Sectores: ¿Cuáles son los que deben sobrevivir ya que están a cargo de procesos críticos?

Personal: ¿Quiénes son más críticos que otros y en qué momento deberían quedar disponibles? Además, deberemos conocer cuáles tienen herramientas para trabajar en forma remota y quiénes no las tienen.

Otros recursos: ¿Cuáles deberían estar en mi sitio alternativo de trabajo y no lo están? ¿En qué momento los necesito? También debo saber si están o no alineados con el MPIT del proceso en el que son utilizados (por ejemplo: registros vitales no digitalizados, formularios, etc.)

ANEXO 4 – Opciones básicas sugeridas como estrategias de contención

RIESGO	POSIBLE ESTRATEGIA DE CONTENCIÓN
Fuego, explosiones (pérdida del sitio de trabajo)	Establecer sitios alternativos de trabajo de concretarse el riesgo, incluyendo la posibilidad de trabajo remoto.
Tormentas, huracanes y vientos fuertes (pérdida del sitio de trabajo).	Establecer sitios alternativos de trabajo de concretarse el riesgo, incluyendo la posibilidad de trabajo remoto.
Inundaciones, diluvios (pérdida del sitio de trabajo).	Establecer sitios alternativos de trabajo de concretarse el riesgo, incluyendo la posibilidad de trabajo remoto.
Terremotos (pérdida del sitio de trabajo).	Establecer sitios alternativos de trabajo de concretarse el riesgo, incluyendo la posibilidad de trabajo remoto.
Pandemias (pérdida del sitio de trabajo).	Utilización de trabajos individuales en forma remota en sitios alternativos (por ejemplo: domicilios).
Ausentismo/interrupción del transporte público, piquetes.	Habilitar el uso de transportes privados. Tener armadas rutas y formas de transportes de la organización. Contar con personal reemplazante alterativo.
Paro general del personal de la organización.	Capacitación y asignación a personal fuera de convenio.
Terrorismo, amenazas químicas o biológicas.	Utilización de trabajos individuales en forma remota en sitios alternativos (por ejemplo: domicilios).
Ciberataques.	Uso de <i>scripts</i> de comunicaciones institucionales mientras se soluciona la problemática. Armado de posibles vulnerabilidades y planes de acción para las más dañinas y probables.
Falta de energía eléctrica.	Generadores de emergencia que además cuenten con testeos habituales de su condición de usabilidad.
Caída del <i>Data Center</i> primario	<i>Data Center</i> Alternativo.
Pérdida de las telecomunicaciones.	Redes redundantes. Establecimiento de intercambio de información por otros medios magnéticos.
Falla en el sistema principal de la organización.	Rutinas administrativas alternativas en los sectores que emplean este sistema. Resguardos de versiones anteriores del sistema y sus conexos. Guardias activas y pasivas.
Corte del suministro de Internet.	Proveedor alternativo de Internet. Utilización de Internet desde otros lugares alternativos de trabajo.
Salida del servicio de la impresora del sector.	Uso testeado de otra impresora de la organización.
Robo y daños intencionales.	Otros recursos para su uso en contingencia.

ANEXO 5 – Contenidos básicos sugeridos para un Plan de Continuidad

Entendemos como Plan de Continuidad el documento que explica en cada sector o, si se quiere, a nivel de toda la organización, qué debe hacer frente a la aparición de un escenario de interrupción.

Los contenidos son variables y pueden extenderse inmensamente. Existen normas y regulaciones que establecen contenidos básicos, por lo que deberán tenerse en cuenta cuáles son estos de acuerdo con la institución en que se esté trabajando.

Inicialmente, los contenidos básicos propuestos para este documento son:

1. Descripción del área o sector al que pertenece el Plan de Continuidad.
2. Objetivo del Plan.
3. Alcance (qué cubre y qué NO cubre).
4. Instrucciones para cada escenario que se desea contener:
 - a. Nombre del escenario.
 - b. Descripción.
 - c. Impacto en el caso de concretarse.
 - d. Evaluación del incidente y procedimiento de activación.
 - e. Estrategia de contención establecida para dicho escenario.
 - f. Procedimiento de contención hasta poder retomar actividades.
 - g. Registros vitales que utiliza y su ubicación.
 - h. Nómina de proveedores y contactos.
 - i. Logística a usar durante la crisis (para transportes, cajas chicas, etc.).
 - j. Evaluación de la vuelta a la normalidad y procedimiento de desactivación.
 - k. Estrategia para la vuelta a la normalidad.
 - l. Procedimiento para la vuelta a la normalidad.
 - m. Registros clave para poder realizar “Lecciones Aprendidas” del escenario.
 - n. Comunicaciones Institucionales.
 - o. Matriz RACI de asignación de responsabilidades (*Responsible, Accountable, Consulted, Informed*-Responsable, Autoridad, Consultado, Informado).
 - p. Árbol de llamadas (quién debe llamar a quién y adónde). Comunicaciones alternativas.

ANEXO 6 – Contenidos básicos sugeridos para un manual de comunicaciones

1. INTRODUCCIÓN

Indicar brevemente cuáles son las características existentes en la organización que dan inicio a la formación del presente manual.

Por ejemplo: “La organización tiene relación no sólo con sus clientes, proveedores y personal sino además con las familias de los mismos, entidades externas regulatorias, grupo regional y medios de prensa y difusión pública. Los impactos que una comunicación errónea, deficiente o mal interpretada puede generar a la organización dependerán no solo de dicho error, deficiencia o mala interpretación, sino además del interlocutor con quien se traba el diálogo y la situación que se está viviendo. En tal sentido, y con el objetivo de minimizar los riesgos en estas comunicaciones, se realiza el presente manual para establecer claramente quién/es es/son el/los autorizado/s a realizar dichas comunicaciones, cuál ha de ser el entorno en el que se deben realizar, y todo lo que hace al formato de las mismas”.

2. OBJETIVO

Indicar los tipos de comunicaciones incluidos en el presente manual.

Por ejemplo: “Este manual se refiere entonces a comunicaciones con:

- a) Nuestro personal y sus familias.
- b) Nuestros clientes.
- c) Nuestros proveedores y eventuales servicios tercerizados.
- d) Entidades regulatorias, como BCRA, Cámara de Transporte, etc.
- e) Televisión.
- f) Prensa”.

3. ALCANCE

Indicar con mayor detalle qué es lo que se está cubriendo y que NO se está cubriendo.

Por ejemplo: “Las comunicaciones a que hacemos referencia en este manual son aquellas que se deberán realizar con motivo de la ocurrencia de un evento que amenace la continuidad de la operatoria de nuestro negocio.

No se incluyen en este manual comunicaciones internas habituales ni comunicaciones externas del giro normal del negocio (*marketing*, campañas publicitarias, ofertas de servicios, pedidos de presupuestos, etc.)”.

4. GLOSARIO

Indicar los significados de conceptos vertidos en el presente manual, que deben ser comprendidos claramente a efectos de asegurar la eficiencia y eficacia del mismo.

Por ejemplo:

“Comunicación”: trato o conferencia entre dos o más personas o instituciones, donde enviamos y recibimos mensajes.

“Medios de difusión pública”: entiéndase televisión (pública o privada), radio, medios gráficos, prensa.

“Interlocutor válido”: única persona o personas autorizadas a tomar la representatividad de la organización para los efectos de comunicar información a entidades externas o internas.

“Escenario de la comunicación”: formato visible en el que se debe desarrollar la comunicación. Se refiere, por ejemplo, a: vestimenta, lugar, colores, luces, tonos de voz, comunicación gestual, aditamentos visuales en la zona de comunicación.

“Esquema de diálogo”: formato en que deberán expresarse (presentación inicial, introducción, cuerpo, conclusiones, preguntas y respuestas, etc.). Fundamentalmente, qué decir y qué no decir durante la comunicación.

“Feedback”: mecanismo de inteligencia que aporta calidad al mensaje. Siempre es destinatario el emisor del mensaje y, este, si no se produce, debería solicitarlo a su interlocutor. Sirve para evitar malas interpretaciones y minimizar los efectos del “ruido” en la comunicación.

“Ruido”: elementos que distorsionan o pueden distorsionar el mensaje.

“Canal”: medio por el que circula el mensaje (papel, entrevistas individuales, entrevistas grupales o conferencias, videoconferencias, comunicación *in itinere*, comunicaciones telefónicas, correos electrónicos, visitas personales, etc.).

“Comunicación unidireccional”: se dan noticias o se proporcionan datos sobre un evento. Es expositiva en una única dirección.

“Comunicación bidireccional”: se ponen en común ideas, mensajes, y hay una ida y retorno entre las partes.

5. PROCEDIMIENTOS A SEGUIR

Indicar paso a paso quién y cómo debe comunicarse ante cada uno de los escenarios que se están incluyendo en el manual.

Por ejemplo:

ID	EVENTO	RESPONSABLE	ACCIONES A TOMAR
1	Incendio	Responsable de Comunicaciones Públicas.	1. Planificar lo que se quiere decir. 2. Identificar plenamente al interlocutor al que se está atendiendo. 3. Identificar el nivel de riesgo de la comunicación. 4. Verificar que se cuenta con los recursos necesarios para efectuar la comunicación como se pretende hacerlo. 5. Proceder de acuerdo con el esquema de diálogo previsto en este manual. 6. Mantenerse actualizado por el líder del equipo de trabajo que está atendiendo la crisis. 7. Decidir cuándo, qué y a quiénes volver a comunicar novedades. 8. Controlar la comunicación distribuida luego de la alocución o distribución de información escrita.

6. ASIGNACIÓN DE RESPONSABILIDADES

Indicar los nombres y apellidos de quienes tomarán roles y responsabilidades de acción frente a distintos escenarios. Indicar, además, formas de contacto con ellos.

Por ejemplo:

ID	NOMBRE DEL CARGO	ASIGNADO A	ROLES Y RESPONSABILIDADES
1	Responsable de comunicaciones con medios de prensa y difusión pública.	Sitio que estará bajo su custodia comunicacional.	1. En situación normal: 1.1. Vigilar el cumplimiento de los testeos del manual de comunicaciones. 1.2. Vigilar la vigencia del contenido de esquemas de comunicación a su cargo. 1.3. Mantener una lista de medios de prensa y difusión pública con personas autorizadas a contactarse. 2. En situación de emergencia: 2.1. Apersonarse en el escenario de contingencia. 2.2. Tomar información de la situación.

Se indica expresamente que, fuera de la lista indicada en el presente capítulo, nadie más está autorizado a difundir, comunicar o establecer contactos con clientes, personal, familiares, etc., en situación de contingencia o ante un evento disruptivo de la operatoria del negocio.

7. SALA DE PRENSA O DIFUSIÓN PÚBLICA

Indicar el sitio donde se considerará la instalación de la Sala de Prensa o Difusión Pública, y los contenidos y las condiciones que deberá tener. Esta sala deberá ser revisada por el encargado de comunicaciones en forma mensual, en cuanto a su libre disponibilidad y contenidos.

Por ejemplo:

“Se establece, como lugar para la Sala de Prensa o Difusión Pública, la sala de reunión ubicada en xxxxxxxx, a la izquierda de la recepción.

En dicho lugar se deberá contar con:

- Refrigerios.
- Información Institucional.
- Organigrama
- Fotos de seguridad habitual en la institución”.

8. PREGUNTAS HABITUALES

Indicar cómo se debe proceder frente a determinado set de preguntas de riesgo para la organización. Las instrucciones deben ser precisas, claras, y deben ser testeadas como mínimo cada 6 meses.

Por ejemplo:

1. ¿Se encuentra amenazada la operatoria que atiende la organización? ¿Sus clientes?
2. ¿Ha fallecido algún miembro de su personal?
3. ¿Qué medidas de contención se han establecido?
4. ¿Conocen los impactos que el evento ha tenido para con los vecinos? ¿Qué se piensa hacer al respecto?

9. EVALUACIÓN DE LA COMUNICACIÓN

Indicar aquí cuáles han de ser los criterios para evaluar qué se ha hecho con la información que hemos transmitido. Señalar si ha sufrido alguna tergiversación, demora, edición, etc., y formas de reclamos (formales, informales) al medio o interlocutor involucrado.

Además, indicar los criterios para asignar criticidad a la comunicación. Estos riesgos y criticidades en la comunicación tienen que ver con la situación o contexto en que se está viviendo y donde es realizada la comunicación (dependiendo de la situación o contexto, el mensaje puede indicar algo totalmente distinto a lo que se quiso transmitir), los factores no verbales incluidos en la comunicación y la interpretación que se puede hacer de la misma de acuerdo con el interlocutor. Además, hay que considerar la fuerza de nuestro interlocutor en el medio donde se desenvuelve, pero no minimizar menospreciando lo que un simple periódico barrial puede provocar en nuestros vecinos, por ejemplo.

La Evaluación debería propender a la mejora de nuestro proceso de comunicación.

Por ejemplo:

Información parcializada: no han incluido los principales puntos comunicados oficialmente por la organización.

Información mal intencionada: han incluido o editado el formato de la comunicación de manera tal de perjudicar los intereses de la organización.

Información correcta: han transmitido lo que hemos querido transmitir.

Y en cuanto a los riesgos:

INTERLOCUTOR	ALTO RIESGO	RIESGO MEDIO	RIESGO BAJO
BCRA	X		
Personal		X	
Familiares	X		
Medios de prensa		X	
Medios televisivos	X		
Medios radiales		X	
Proveedores			X
Clientes	X		

10. CAPACITACIONES Y ENTRENAMIENTOS

Indicar las formas previstas de capacitación y entrenamiento. De ser posible, incluir formas de testeos incluyendo a personal que NO debería involucrarse en las comunicaciones en situación de contingencias.