AUDITORÍA INTERNA

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Auditoría Interna de la gestión de crisis y resiliencia del negocio

The Institute of Internal Auditors

Instituto de Auditores Internos de España

El INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA es una asociación profesional fundada en 1983, cuya misión es contribuir al éxito de las organizaciones impulsando la Auditoría Interna como función clave del buen gobierno. En España cuenta con más de 3.500 socios, auditores internos en las principales empresas e instituciones de todos los sectores económicos del país.

LA FÁBRICA DE PENSAMIENTO es el laboratorio de ideas del Instituto de Auditores Internos de España sobre gobierno corporativo, gestión de riesgos y Auditoría Interna, donde participan más de 150 socios y profesionales técnicos expertos.

AUDITORÍA INTERNA

BUENAS PRÁCTICAS EN GESTIÓN DE RIESGOS

OBSERVATORIO SECTORIAL

PRÁCTICAS DE BUEN GOBIERNO

El laboratorio trabaja con un enfoque práctico en la producción de documentos de buenas prácticas que contribuyan a la mejora del buen gobierno y de los sistemas de gestión de riesgos en organizaciones de habla hispana. Además de desarrollar contenido, fomenta el intercambio de conocimientos entre los socios.

ENCUENTRA TODOS LOS DOCUMENTOS DE LA FÁBRICA EN www.auditoresinternos.es

AUDITORÍA INTERNA

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Auditoría Interna de la gestión de crisis y resiliencia del negocio

Diciembre 2021

MIEMBROS DE LA COMISIÓN TÉCNICA

COORDINACIÓN:

Jorge Pérez García. SEAT.

Alfonso Aldaz Moreno. FERROVIAL.

Belén Álvarez Álvarez. DELOITTE.

María del Pilar Amarillas Herraiz. REPSOL.

David Bello Castro, CIA. BANCO CRÈDIT ANDORRÁ.

José Antonio Castrillo Nuevo, CISA, CISM, CGEIT, CESCOM, IFCA, CDPS. MAZARS.

Jon Fernández Ellacuría, CIA, CISA. IBERDROLA.

Enrique García Maestre. AGBAR.

José Manuel Jiménez Rodríguez, COSO-CI. MAHOU-SAN MIGUEL.

Águeda de Lara Valero, CIA. GLOBALVIA.

Carlos Viola Fernández de Arcaya. BDO.

The Institute of Internal Auditors

Instituto de Auditores Internos de España

Instituto de Auditores Internos de España

Santa Cruz de Marcenado, 33 · 28015 Madrid · Tel.: 91 593 23 45 · Fax: 91 593 29 32 · www.auditoresinternos.es

Depósito Legal: M-34755-2021

ISBN: 978-122588-8-2

Diseño y maquetación: desdecero, estudio gráfico

Las situaciones de crisis, cuyo ejemplo cercano más palpable es la derivada del SARS-COV-2 a principios de 2020, nos muestran que en algunos casos las empresas no están preparadas para preverlas o reaccionar ante las mismas.

Bajo esta premisa, la Comisión Técnica que ha elaborado estas páginas analiza el papel que Auditoría Interna asume antes, durante y después de una crisis, así como la importancia de considerar la continuidad de negocio como un riesgo que debe revisarse y contemplarse en el Plan Anual de Auditoría Interna.

Pero este documento va más allá, al enfocarse muy acertadamente en cómo Auditoría Interna puede contribuir desde su posición a incrementar la resiliencia frente a una crisis a través de las mejores prácticas en diversos ámbitos -desde la gestión de riesgos a la información de gestión y *reporting*-.

Culmina con un amplio apartado en el que se tratan los diferentes roles del auditor interno frente a la resiliencia, que pueden variar en función del impacto de la crisis y de la fase en la que se encuentre; y de la Comisión de Auditoría frente a la resiliencia.

Desde el Instituto agradecemos el trabajo de la Comisión que ha elaborado este documento, una completa publicación que será de gran utilidad para que los auditores internos aportemos nuestro grano de arena en la prevención y gestión de las situaciones de crisis de nuestras organizaciones.

Instituto de Auditores Internos de España

Índice

Introducción

Las empresas que prevén y afrontan las crisis no solo sobreviven, sino que pueden salir reforzadas.

La crisis sanitaria y económica derivada del SARS-COV-2 a principios de 2020 puso una vez más de manifiesto la necesidad de que las compañías tengan mecanismos de preparación y respuesta ante situaciones que puedan poner en peligro la continuidad de su negocio. Todas pasan, a lo largo de su existencia, por periodos de crisis más o menos intensos.

Sus orígenes son diversos: los relacionados con ámbitos de la salud (COVID 19, SARS, MERS), con factores climatológicos (la borrasca Filomena o el huracán Katrina), con factores políticos (ataques terroristas del World Trade Center, cierres de fronteras), con accidentes locales (incendio edificio Windsor), con aspectos relacionados con la seguridad de la información (WannaCry), con factores económicos (Lehman Brothers), etc.

Estas situaciones de crisis han evidenciado, en algunos casos, que las compañías no estaban preparadas para prever dichas situaciones y cómo reaccionar ante las mismas. Aquellas que no se preparan con antelación para afrontar una crisis pueden llegar a sufrir las consecuencias e, incluso, llevarlas a su desaparición. Las que prevén y afrontan estas situaciones no sólo sobreviven, sino que pueden salir reforzadas.

En el cuadro se muestran ejemplos de eventos que propiciaron diferentes tipos de crisis con distinto alcance (empresa, sector, multisector) y localización geográfica (local, nacional, multinacional):

	LOCAL	NACIONAL	MULTINACIONAL
EMPRESA	UBER Barcelona/ UK (declara trabajadores a los conductores)	Expropiaciones de gobiernos a multinacionales	Lehman Brothers
SECTOR	Revueltas por cierre de industrias	Plaga naranjas. Argentina	Adaptación a legislaciones de emisiones para los automóviles
MULTISECTOR	Filomena, Huracán Katrina	Revueltas Chile 2020	Crisis sanitaria (COVID 19, SARS, MERS) WannaCry

Tabla 1: Fuente: Elaboración propia

El factor clave para que una compañía sea resiliente a las crisis es la capacidad de preparación, así como la capacidad de reacción para afrontar eventos imprevistos cuyo impacto afecta significativamente a la continuidad de las operaciones y/o negocio.

Una respuesta madura a la crisis es la realización de pruebas de Continuidad de Negocio: efectuar simulacros periódicos ante diferentes eventos de crisis permite tener a los equipos entrenados para enfrentarse a escenarios y situaciones complejas, favoreciendo la mejora continua del proceso correspondiente.

Aunque existen estándares internacionales y referencias de mejores prácticas globales de preparación para una crisis, que se tratan en los siguientes capítulos de este documento, no existe un único modelo válido para todas las compañías. Cada una debe identificar y evaluar los requisitos y necesidades que les afectan, para el desarrollo e implementación de su Sistema de Gestión de Continuidad de Negocio (BCM).

El rol de Auditoría Interna, como socio de confianza, aporta valor añadido por las habilidades y experiencia de los auditores en todos los ámbitos de la compañía (identificando y evaluando riesgos, controles, procesos y operaciones) y permite darles soporte con el objetivo de prepararse para la inevitable crisis y, de este modo, colaborar a mejorar la resiliencia de la compañía ante este tipo de eventos de riesgo.

Este documento abarca el rol que debe tener Auditoría Interna para supervisar los mecanismos de gestión de crisis y la resiliencia del negocio, así como el papel que asume en la fase previa, durante y después de que se produzca una crisis. Además, se identifican las mejores prácticas relacionadas con la actuación de Auditoría Interna en este tipo de trabajos.

En el Anexo se incluyen conceptos y definiciones clave para ayudar a una mayor comprensión sobre la Continuidad de Negocio y la Gestión de Crisis.

La realización periódica de pruebas de Continuidad de Negocio permite tener a los equipos entrenados favoreciendo la mejora continua del proceso correspondiente.

Normativas legales y estándares internacionales aplicables

Como ya se ha indicado, cada compañía debe identificar y evaluar sus requisitos y/o necesidades en función de su sector/modelo de negocio, su ubicación geográfica/alcance de sus operaciones y el tipo de crisis/evento de riesgo identificado.

Instituciones como la *International Organization for Standardization* (ISO), *British Standards Institution* (BSI), *National Institute of Standards and Technology* (NIST), *Business Continuity Institute* (BCI) y *Disaster Recovery Institute International* (DRII) han desarrollado estándares y guías de referencia con las herramientas necesarias para que compañías, privadas y públicas, incorporen en sus modelos de gestión el concepto de resiliencia.

Cada empresa debe diseñar y desplegar planes de Continuidad de Negocio en función de su apetito de riesgo y grado de madurez.

En función del nivel de apetito de riesgo de cada empresa y su grado de madurez en la actividad que desarrolla, se deben diseñar y desplegar planes de Continuidad de Negocio para prevenir y gestionar una crisis que pudiera afectar seriamente a su continuidad e, incluso, a su supervivencia.

Los sectores estratégicos (agua, banca, energía, salud…) **cuentan con regulación específica** porque deben demostrar a sus reguladores de forma recurrente, organizada e inmediata su capacidad de reacción ante simulacros de los posibles eventos negativos que afecten a su operativa. Por esta razón, se encuentran en un proceso de evaluación continua de sus planes de Continuidad de Negocio, repercutiendo en una actualización y perfeccionamiento de sus respuestas en tiempo y forma. En el caso particular de la Unión Europea (UE), existen directivas relacionadas con la protección de infraestructuras críticas y provisión de servicios esenciales: Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016 –relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión– y Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas.

En este documento no se plantean diferencias entre empresas reguladas y no reguladas, pues la finalidad que persiguen ambas es fortalecer la resiliencia y, por ende, su supervivencia.

En el Anexo se incluye el detalle de estándares internacionales y referencias de mejores prácticas clave para la gestión y respuesta a crisis. Pero debido a continuas revisiones y a la creación de nuevos estándares sectoriales, estas referencias podrían quedar desactualizadas rápidamente.

Mejores prácticas para incrementar la resiliencia frente a la crisis

GESTIÓN DE RIESGOS

Es clave para reaccionar de forma eficaz y planificada ante escenarios imprevistos de crisis con riesgo de interrupción en el negocio y poder mantener la productividad de la empresa en niveles aceptables.

Es imprescindible que los riesgos vinculados a acontecimientos sorpresivos con gran impacto –inclusive las crisis– estén previstos, documentados y gestionados (aportando controles o medidas para reducir su impacto) en las

compañías. Para que estén prevenidas ante una situación de crisis es necesario disponer de una óptima y sistematizada gestión de estas potenciales amenazas. El Plan de Continuidad de Negocio debe contemplar los riesgos asociados a las principales situaciones de crisis y definir las funciones esenciales y/o críticas de la compañía, necesarias para mantener su operatividad y productividad.

El marco *Enterprise Risk Management: Integrating with Strategy and Performance* (COSO, 2017) incluye, entre otros beneficios de dicha integración, la mejora de la resiliencia de las empresas, indicando que *"[…] la viabilidad a medio y largo plazo de una entidad depende de su capacidad para anticiparse y responder al cambio, no sólo para sobrevivir sino también para evolucionar y prosperar. Esto es posible, en parte, gracias a una gestión eficaz del riesgo empresarial".*

En la misma línea afirma que, entre las tendencias más destacadas sobre la gestión del riesgo empresarial se encuentra la *"oportunidad de construir organizaciones más fuertes"*, al poder conocer cuáles son los riesgos que mayor impacto podrían tener en la entidad, cuya consecuencia será *"poder poner en marcha capacidades que les permitan actuar con prontitud".*

Como primer aspecto para abordar una gestión de riesgos efectiva conviene que la compañía identifique sus procesos críticos de negocio y soporte para luego llevar a cabo un **Análisis de Impacto del Negocio** *(Business Impact Analysis*, BIA), que permita determinar fundamentalmente:

- Los procesos, las infraestructuras y los recursos/funciones clave de la compañía (incluyéndose la identificación de las terceras partes / proveedores de servicio, por la relevancia que pueden tener para ella).
- Los activos críticos para la compañía.
- Los tiempos en que puede soportar una pérdida de operatividad/información por proceso.
- Las personas más sensibles para la continuidad.

Asimismo, otra tarea de gran importancia es determinar los riesgos/amenazas que, en términos generales, se podrían considerar a efectos de su análisis y gestión (identificación de controles establecidos y vulnerabilidades).

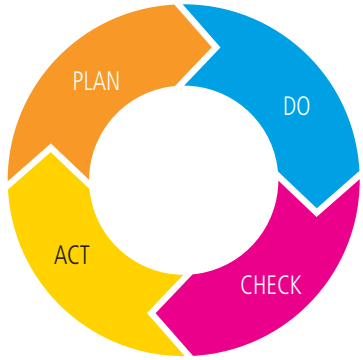
Las siguientes situaciones se pueden considerar como los principales riesgos a tener en cuenta en el ámbito de la continuidad del cegocio:

- Desastres naturales.
- Desastres de origen industrial.
- Sabotajes.
- Fallos o eventos que afecten a la disponibilidad de terceros.
- Indisponibilidad del personal (huelgas, pandemias).
- Vulnerabilidades del *software* y otros programas.
- Fallos de servicio de comunicaciones.
- Errores humanos.
- Ataques intencionados (internos / ciberataques).
- Incumplimientos legales.
- Fugas de información.

Para abordar una gestión de riesgos efectiva la compañía debe identificar sus procesos críticos de negocio y soporte para llevar a cabo un Análisis de Impacto del negocio.

ESTABLECIMIENTO DE UN PROGRAMA DE CONTINUIDAD DE NEGOCIO (BCP)

Las buenas prácticas sobre Continuidad de Negocio recogidas en la norma ISO 22301: 2019, utilizando el Ciclo de Deming, permiten establecer un PDCA *(Plan-Do-Check-Act)* donde se incorpora la estrategia de Continuidad (incluida la identificación y gestión de riesgos) y todos los elementos relacionados: BIA, riesgos, estrategias de recuperación, documentación, pruebas, formación, etc.



Fuente: Ciclo de Deming

Preparar un detallado plan de gestión frente a la crisis facilita la respuesta de la compañía de una forma óptima, considerando diferentes alternativas de antemano. El PDCA contempla:

- *Plan:* Definir una política, unos objetivos, metas, unos controles, unos procesos, procedimientos, etc. relacionados con la continuidad.
- *Do:* Implementar y operar la política de Continuidad de Negocio, controles, procesos y procedimientos.
- *Check:* Seguimiento y revisión del rendimiento de la política, controles, objetivos, etc., de continuidad.
- *Act:* Mantener y mejorar el Sistema de Gestión de Continuidad de Negocio mediante la aplicación de medidas preventivas y correctivas.

PLAN DE RESPUESTA (BCP)

Planificación

Un plan de respuesta o BCP *(Business Continuity Plan)* es una planificación de cómo una compañía debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas, dentro de un tiempo predeterminado, tras una interrupción no deseada o desastre.

Para su planificación, la compañía debe designar personal de respuesta a incidentes con la responsabilidad, autoridad y competencia necesarias para su gestión.

- Confirmar el carácter y alcance de un incidente.
- Provocar una respuesta de continuidad de negocio apropiada.
- Contar con planes, procesos y procedimientos para la activación, operación, coordinación y comunicación de la respuesta al incidente.
- Contar con recursos para dar soporte a los planes, procesos y procedimientos para gestionar un incidente.

Establecimiento

La compañía debe contar con planes documentados que detallen cómo se gestionará un incidente y cómo recuperará o mantendrá sus actividades en un nivel predeterminado en el caso de producirse una interrupción. En general, cada plan debe:

- Tener un propósito y alcance definidos.
- Ser accesible y ser entendido por las personas que lo usen.
- Tener propietario/s identificado/s, nombrados/s para que sea/n responsable/s de su revisión, actualización y aprobación.
- Estar alineado con los planes y acciones de contingencia externos a la compañía.

Asimismo, y de manera particular, cada plan contendrá:

- Líneas de comunicación identificadas.
- Tareas fundamentales e información de referencia.
- Funciones y responsabilidades definidas para personas y equipos humanos que tengan autoridad para invocar cada plan.
- Un método que determine cómo el plan es invocado.
- Lugares de reunión con alternativas, y datos de contacto actualizados, así como detalles de movilización.
- Un proceso de vuelta a la normalidad una vez el incidente haya sido solucionado.
- Una referencia a los datos de contacto esenciales para todos los grupos de interés.
- Procesos y tareas para permitir la continuidad y recuperación de las actividades críticas.

Evaluación

Evaluar de forma periódica el plan de respuesta permite a las compañías comprobar si las actividades planificadas como respuesta a la crisis funcionan o deben ser mejoradas. Adicionalmente, uno de los principales objetivos que se pretende es que las compañías estén preparadas para prever dichas situaciones y saber reaccionar ante ellas de la manera más ágil. Además de "entrenar" a las personas que responden más activamente en estas situaciones, la compañía debe:

- Probar sus planes para asegurarse de que cumplen con sus metas y objetivos.
- Desarrollar ejercicios que sean coherentes con el alcance del Plan de Continuidad.
- Disponer de una estrategia aprobada por la alta dirección y comunicada, con el objeto de asegurar que los ejercicios se realicen a intervalos programados y cuando se produzcan cambios significativos, tanto desde el punto de vista operativo como de la concienciación del personal.
- Llevar a cabo ejercicios diversos que, en conjunto, validen la totalidad de sus previsiones de Continuidad de Negocio.
- Planificar ejercicios de forma que se minimice el riesgo de que se produzca un incidente como consecuencia directa del ejercicio.
- Definir objetivos y metas de cada ejercicio.
- Llevar a cabo una revisión, después de cada ejercicio, para evaluar la consecución de sus objetivos y metas.
- Redactar un informe por escrito del ejercicio, los resultados y la retroalimentación, incluyendo las medidas que deban tomarse.

Mantenimiento

La compañía debe, de forma periódica o cuando se produzcan cambios significativos, mantener y revisar los planes de respuesta para asegurar que continúan siendo idóneos, adecuados y eficaces.

La compañía debe tener planes documentados que detallen cómo se gestionará un incidente y cómo recuperará sus actividades. Estos planes deben evaluarse y revisarse periódicamente.

TECNOLOGÍAS DE LA INFORMACIÓN

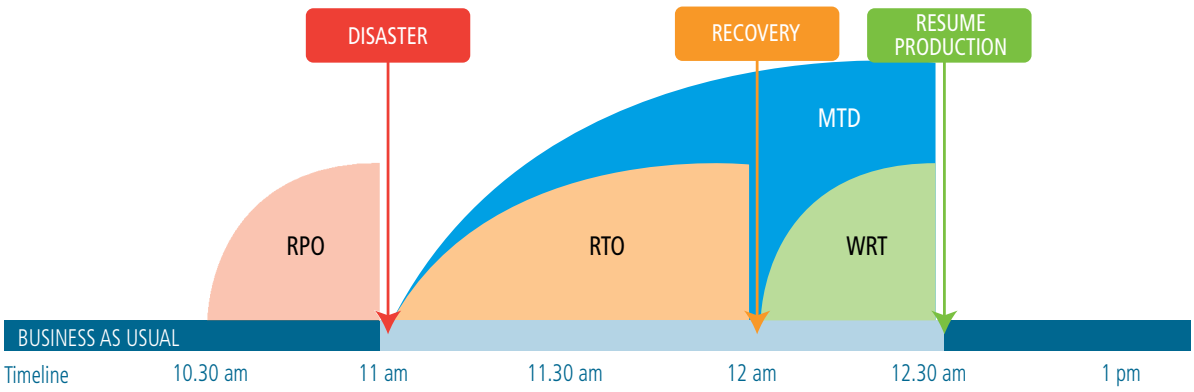
La infraestructura tecnológica es uno de los pilares a la hora de garantizar la resiliencia.

Definición de la estrategia de recuperación

El área de Informática, como gestora de los sistemas informáticos, debe solicitar a los propietarios de los procesos el nivel de criticidad de los sistemas informáticos que soportan dichos procesos. En función de esta criticidad, el propietario del proceso definirá unos objetivos de recuperación, en colaboración estrecha con el área de Continuidad de Negocio, que se encuentra constituida por expertos en este campo y que disponen de una visión perimetral de toda la compañía.

Estos objetivos, en el mejor de los casos, se deben basar en el proceso de BIA. En ese momento, el área informática debe tenerlos en cuenta para poder asegurar que el sistema informático cumpla con los requisitos definidos por el propietario del proceso o de los datos.

CONCEPTOS DE RECUPERACIÓN



Ver la definición de conceptos clave en el Anexo.

El área de Informática puede documentar estos requisitos en los **Acuerdos de Nivel de Servicio** *(Service Level Agreement, SLA)* para poder dar seguimiento del servicio requerido por el propietario del proceso o dato cuyas necesidades pueden ser dispares. Por ello, las áreas de informática y de Continuidad de Negocio deben definir estrategias de recuperación para cada uno de los sistemas considerando el coste/beneficio para la compañía.

Aspectos a seguir por el área de Informática:

- Conocer y documentar las necesidades de recuperación de sistemas de la compañía y/o áreas de negocio, incluyendo la arquitectura de los Centros de Procesamiento de Datos (CPD s), comunicaciones, etc.
- Establecer acuerdos de Nivel de Servicio en función de las necesidades a cubrir por las

áreas de negocio. En estos acuerdos pueden definirse niveles de soporte predeterminados (oro, plata, bronce; sólo *backup).*

- Analizar los planes de continuidad o recuperación de TI y respuesta a incidentes asegurando que las principales plataformas a recuperar están incluidas en el alcance, así como la trazabilidad de estos con los BIAs de negocio, incluyendo los planes de *backup* cuyo objetivo es preservar la información.
- Garantizar, mediante pruebas, que los sistemas proporcionados a las áreas de negocio cumplen sus expectativas de disponibilidad y de recuperación de datos *(backup),* para dar una respuesta eficiente a la continuidad de las operaciones. La organización y ejecución periódica de simulacros constituye un aspecto critico en un sistema de respuesta a las crisis maduro. Es muy recomendable contemplar diferentes simulacros de eventos de crisis para disponer de equipos entrenados y preparados que afronten escenarios y situaciones complejas.
- Asegurar que la provisión de servicios por parte de terceros está correctamente gestionada, tanto para garantizar que en una situación de contingencia de la compañía el tercero se puede adaptar a la nueva situación, como para el caso en que el tercero atraviese una situación de contingencia. Este factor es clave, teniendo en cuenta que, cada vez, hay más servicios y procesos externalizados y en diferentes situaciones (servicios *cloud,* servicios *in-house* pero gestionado por externos, etc…)

Asegurar la provisión de servicios por parte de terceros es clave ya que cada vez hay más servicios y procesos externalizados.

PERSONAL Y FORMACIÓN

Para preparar una contingencia, la compañía debe identificar sus requisitos y organizar los procesos y recursos (humanos y técnicos) para garantizar la Continuidad del Negocio.

La identificación de personal clave para la compañía cuya participación sea difícilmente reemplazable en el corto plazo, debe ser un punto indispensable y contemplado en el Análisis de Impacto de Negocio (BIA). En este proceso, se deberían valorar tanto las necesidades relativas a la toma de decisiones, como otros aspectos únicamente operativos en los que prime el conocimiento de negocio o *know-how.*

Se deben identificar y documentar claramente los planes de sucesión y los sustitutos para que, en caso de que la persona no pueda incorporarse, exista una opción de reemplazo temporal y alternativa. Es necesario recoger estas alternativas en el Plan de Continuidad de Negocio, y es una prioridad que queden registrados los responsables iniciales y personal alternativo de cobertura.

Una correcta definición de habilidades unidas a los puestos de trabajo facilita la identificación del personal clave y agiliza el proceso de contratación *ad-hoc* si fuera necesario aumentar la fuerza de trabajo durante la situación de emergencia. Para ello, la compañía tiene que contemplar este tipo de situaciones a la hora de establecer contratos con agencias de colocación de empleo.

Aunque depende de la tipología de incidente que haya ocurrido, es razonable pensar que,

durante la contingencia, puedan surgir cambios en el régimen y condiciones de trabajo que se han de acordar con los sindicatos y otros agentes sociales bajo el amparo de los servicios jurídicos. Puede hacerse frente a aspectos como la reubicación de empleados en otros centros de trabajo, la obligatoriedad de puestos necesariamente presenciales por requerimientos operativos, la ampliación de turnos de trabajo para el restablecimiento de los procesos de negocio, etc.

Es preciso revisar objetivos y componentes del programa corporativo de formación en Continuidad de Negocio apoyado por la alta dirección.

Formación

Es preciso revisar que se han establecido los objetivos y los componentes del programa corporativo de sensibilización y formación en materia de Continuidad de Negocio y que lo apoya la alta dirección, así como que se ha definido un nivel de concienciación deseado, en función de las responsabilidades existentes. Además, este plan de formación se actualizará periódicamente. También hay que confirmar que se han identificado y priorizado, por un lado, los grupos objetivo-internos (miembros del equipo, figuras clave, etc.) y, por otro, los grupos objetivo-externos (clientes, proveedores, etc.).

Estos empleados deben recibir una notificación inicial y formación específica de Continuidad de Negocio y de Seguridad IT con los objetivos de:

- Saber responder a amenazas o eventos específicos.
- Saber qué hacer cuando se evacúa el lugar de trabajo.
- Disponer de conocimiento de los planes de recuperación.

Esta concienciación sobre el Plan de Continuidad de Negocio puede realizarse mediante reuniones informativas para todo el personal en una fase temprana de su desarrollo, debiendo revisarse si se han tratado específicamente las razones del BCP y sus beneficios para la compañía, cómo se desarrollará éste y cómo participará el personal en el mismo.

COMUNICACIÓN

Una crisis puede tener su origen en circunstancias internas y/o externas a la compañía, pudiendo tener consecuencias para su reputación, impactando rápidamente en la opinión pública a través de los medios de comunicación o las redes sociales, así como en su ámbito interno. La comunicación de crisis debe acompañar siempre a la gestión operativa en tiempo y forma y debe estar centralizada en un órgano de comunicación.

Este órgano debe estar coordinado con cualquier departamento que pudiera verse implicado en la resolución de la incidencia, tales como gestión de riesgos, servicios jurídicos, seguridad física o relaciones laborales, y siempre formar parte de los comités de gestión de crisis que se pudieran establecer.

Además de los comités establecidos con su titular y su sustituto, deberían existir unos grupos de apoyo que se formalizarán ad-hoc para cada crisis, en función de la casuística de ésta, y estarán compuestos por empleados "críticos", pertenecientes a las áreas transversales de la compañía implicadas directa o in-

directamente con el factor que haya generado la crisis.

La gestión de la comunicación de la crisis debe estar contemplada dentro del plan de respuesta. Pueden establecerse diferentes niveles de gestión de la comunicación de la crisis (A, B y C), en base a la gravedad de la situación y de la repercusión pública de la misma y, según progrese, ésta puede escalar a través de estos diferentes niveles, así como también lo hará la respuesta necesaria que dará la compañía.

Cada uno de estos niveles de gestión deben contar con diferentes respuestas en función de la estrategia de comunicación acordada en el comité de gestión de crisis. Y siempre es recomendable preparar un argumentario, mensajes clave, comunicado de prensa, definir portavoz, etc., para el caso de tener que ser utilizados.

GESTIÓN DE TERCEROS Y FORMALIZACIÓN CONTRACTUAL

La externalización de determinados procesos por parte de las empresas (gestión de la facturación, gestión de nóminas, gestión de cobros, procesos tecnológicos, servicios logísticos, etc.) implica exponerse a diferentes tipologías de riesgos, según el caso, que deberían ser considerados para prevenir y mitigar.

La relación de una compañía con los terceros que formen parte de la cadena de suministro debe estar fortalecida para asegurar que, durante las situaciones de contingencia que afecten tanto a dicho tercero como a la entidad, esta relación se pueda desarrollar bajo condiciones previamente establecidas y el impacto de las contingencias se minimice a un nivel aceptable.

Al igual que la propia compañía, estos terceros están expuestos a situaciones de crisis en incidentes que les puedan provocar una situación de contingencia, por lo que se debe velar por que cuenten con medidas de continuidad razonables y puedan responder ante las demandas de la entidad contratante, de tal modo que ésta también pueda alcanzar sus objetivos de recuperación y de vuelta a la normalidad.

No vamos a definir la gestión del riesgo de terceros. Pero sí considerar establecer una estrategia de resiliencia frente a los proveedores existentes y futuros, dependiendo de la criticidad que tenga cada uno y adaptando diferentes estrategias para cada tipo de proveedor. Podría ser:

- No hacer nada, pasando por reducir dependencia aumentando proveedores.
- Valorar el *insourcing* en caso de contingencia.
- Establecer un marco de colaboración con el proveedor incluyéndolo en nuestro plan de continuidad (opción deseable para los más críticos), o, incluso, finalizar la relación si no cumple con las expectativas de la compañía.

Una vez que la estrategia está clara para cada tipología de proveedor, la compañía debe establecer cuáles son los requisitos a cumplir por ambas partes durante la relación. Para ello, los procesos del área de Compras que se encargan de la selección de los proveedores pueden establecer criterios que prioricen a aquellos que sean capaces de evidenciar madurez en aspectos de Continuidad de Negocio (certifica-

La externalización de determinados procesos implica exponerse a diferentes tipologías de riesgos, según el caso, que deberían considerarse para prevenir y mitigar.

ciones, realización de auditorías de continuidad, adaptación de terceros a los requisitos de Continuidad de Negocio propios, informes realizados por terceras partes de confianza, etc.).

Todos estos requisitos deberían quedar formalizados en los contratos o documentos que formalicen la relación, con una serie de indicadores que permitan a la compañía evaluar su cumplimiento. Gran parte de ellos podrán ser revisados con la información que se comparta de manera transparente en el modelo de cliente-proveedor, y posiblemente puedan estar más detallados en los SLA.

La evaluación del control del entorno de Continuidad de Negocio de terceros es una práctica cada vez más implantada en las compañías, para llevar a cabo acciones de aseguramiento de terceros *(Third Party Assurance).* En este sentido, existe una serie de estándares internacionales que garantizan el correcto funcionamiento de los mecanismos de control implementados en las compañías prestadoras de los servicios externalizados, y que aportan una serie de certificaciones tras llevar a cabo exámenes independientes de los procesos, mecanismos de control y entornos informáticos de proveedores. Entre estos estándares –cuyos resultados se concretan en unos Informes de Aseguramiento denominados SOC *(Service Organization Control)*– destacan SOC 1 para el Aseguramiento sobre la información financiera, y SOC 2 y SOC 3 para el Aseguramiento sobre los controles operativos[1].

Gestión de las operaciones

De acuerdo con el artículo *Striving for operational resilience* (Brandenburg, Ivell, Sekeris, Gruber, & Lewis, 2019), el concepto de resiliencia operacional está enfocado en la **"anticipación, prevención y adaptación,** en lugar de las actividades de recuperación una vez que la situación se ha desbocado. La resiliencia operacional tiene un alcance mayor y debe estar integrada en la cultura de mitigación de riesgos de la compañía".

Estos tres componentes se unen para determinar la flexibilidad de la cadena de valor, o la capacidad de seguir generando valor bajo diferentes condiciones de oferta y demanda.

La compañía debe evaluar estas potenciales condiciones y anticipar las necesidades de reajustar su producción u oferta de servicios a la nueva posición de demanda.

Las situaciones pueden variar: desde que la capacidad de producción haya disminuido debido al impacto del incidente en nuestro negocio y la demanda se mantiene o incluso aumenta, hasta que –sin vernos afectados por dicho incidente– la demanda se congela debiendo disminuir dicha capacidad productiva o reorientándola para producir bienes o servicios que no son el objetivo primordial de la compañía, pero que pueden reaprovechar la infraestructura y *know-how* existente.

Por otro lado, existen compañías de provisión de servicios esenciales donde la resiliencia no es un objetivo buscado, sino un requisito legal imperativo que puede traer consecuencias severas si no son capaces de garantizarla ante el regulador.

Un BIA que considere aspectos de capacidad ayudará a las compañías a anticiparse a los incidentes.

1. Ver Anexo.

Entre las cuestiones más importantes que cabe plantearse se encuentran las siguientes:

- ¿De qué capacidad sobrante disponemos para hacer frente a aumentos de demanda imprevistos?
- ¿Cuáles son las líneas de producción que mayor margen nos aportan para priorizarlas sobre otro tipo de productos, cuando todos compitan por los mismos recursos para la recuperación?
- ¿Tenemos la posibilidad de que socios o aliados estratégicos complementen nuestra falta de producción?
- Si los escenarios previstos incluyen la necesidad de aumentar la actividad laboral, pero no disponemos de personal formado ¿en qué medida el personal actual puede cumplir con estas necesidades?, ¿se podrían realizar jornadas de trabajo intensivas?
- ¿Tenemos una gestión de riesgos de cadena de suministro suficientemente madura para cubrir las expectativas?
- Si el incidente ante el cual nos enfrentamos afecta de un modo significativo a la plantilla, ¿qué nivel de absentismo podemos asumir?, ¿podemos dotar de medios a dicha plantilla para reducir el absentismo?, ¿en qué medida es factible el trabajo en remoto?
- ¿De qué manera debemos incluir al área de Prevención de Riesgos Laborales/Seguridad e Higiene para adecuar las condiciones de trabajo?
- ¿Se encuentra la compañia en una posición de cambiar de mercados u objetivos, aprovechando un posible cambio de paradigma debido al incidente/crisis?

Las **medidas para mitigar el riesgo en el área de operaciones** pueden ser:

- Un análisis de capacidad que permita planificar el desvío de producción a diferentes plantas o instalaciones donde el incidente haya afectado de menor manera.
- La cobertura de demanda con sobreproducción disponible en las condiciones actuales.
- Incrementar el *stock* de seguridad que permita aumentar la entrega de bienes mientras se escala la producción.
- La externalización de operaciones propias en otros socios ya sea por pérdida de capacidad productiva o aumento de demanda, etc.

El Análisis de Riesgos y los Planes de Continuidad de Negocio deben considerar no únicamente los riesgos propios de la compañía, sino también las posibles vulnerabilidades de las operaciones fuera de su entorno interno; es decir, aquellos **riesgos en el entorno de los proveedores** que pudieran tener un impacto significativo en las operaciones de la compañía. Entre estos riesgos, a modo de referencia y sin que sea limitante, deben considerarse:

- Riesgos políticos en los que se puedan ver afectados: regímenes inestables, posibles cierres de fronteras, aduanas y aranceles que puedan gravar sus productos.
- Riesgos medioambientales que puedan afectar a los proveedores, su logística o al personal que ejecuta los procesos.
- Riesgos sociales: huelgas, disturbios sociales, sabotajes, delitos que puedan afectar al proveedor o alguna de sus instalaciones.
- Riesgos técnicos y operativos: fallos en sus instalaciones que puedan derivar en falta de productos o mala calidad de estos.

El Análisis de Riesgos y los planes de Continuidad de Negocio deben considerar los riesgos propios de la compañía y aquellos en el entorno de los proveedores que puedan impactar en las operaciones de la compañía.

- Riesgos legales: incumplimientos de normativa vigente que pueden provocar sanciones y cierres de proveedores o alguna de sus instalaciones.
- Riesgos económicos: limitaciones económicas o falta de liquidez en los proveedores pueden detener su actividad.
- Riesgo de concentración: es aconsejable no depender de un solo proveedor para el suministro de productos o servicios si bien, en ocasiones, es algo inevitable.

ASPECTOS FINANCIEROS

Un *Business Impact Analysis* (BIA) que considere aspectos financieros ayudará a anticiparse a los incidentes.

Las repercusiones económicas de una crisis, en función de su tipo y sector al que afecte, pueden ser negativas o incluso positivas y tendrán impacto en los estados financieros de la compañía. Un BIA que considere aspectos financieros ayudará a anticiparse a los incidentes. Las principales cuestiones a plantear pueden ser:

- ¿Existen contratos de seguros que permitan a la compañía transmitir a terceros los riesgos sobre el inmovilizado, las operaciones propias y el circulante necesarios para su actividad que puedan quedar inoperativos o gravemente dañados? De esta forma, podrá mitigar el impacto hasta lograr recuperar sus funciones productivas.
- ¿Existe una política y/o procedimiento para que la compañía controle las condiciones y límites disponibles tanto de sus líneas de crédito a corto plazo como de sus préstamos a largo plazo, así como las ratios de endeudamiento a partir de los cuales se consideraría necesario reestructurar su deuda? Para determinados sectores, como el financiero, se debe evaluar el sistema de control interno para garantizar la aplicación de políticas y procedimientos para el cálculo y monitorización de ratios tales como el de solvencia, el de liquidez, etc.
- ¿Existen políticas y/o procedimientos relacionados para solicitar a las autoridades pertinentes la suspensión temporal de empleo a los trabajadores que no sean identificados como esenciales, o para la solicitud de subvenciones o procedimientos de prospección y análisis de si a la compañía le corresponde ser sujeto elegible para recibir ayudas públicas?
- ¿Se ha considerado el riesgo de no poder generar efectivo debido a la crisis? ¿Se establecieron medidas compensatorias? Por ejemplo, un evento climático como un huracán tropical puede afectar a las operaciones de un hotel; o un confinamiento de la población puede provocar ausencia o reducción de ingresos en el sector restauración.

INFORMACIÓN DE GESTIÓN Y REPORTING

Es fundamental que en la compañía se proporcione de forma clara y transparente –en especial a la alta dirección y a la Comisión de Auditoría– una visión periódica de la situación en materia de Continuidad de Negocio/ Gestión de Crisis, en cuanto a la madurez y

efectividad de estos procesos. Disponer de un sistema de indicadores para el seguimiento y efectuar el *reporting* a nivel de alta dirección, debe poner de manifiesto la situación real sobre los principales elementos de gestión de crisis/continuidad, en aspectos como:

- Procesos Críticos sin Planes de Continuidad de Negocio.
- Grado de actualización de los Procesos Críticos / BIAs / Planes de Continuidad.
- Grado de cobertura de los Planes Contingencia TI / *IT Disaster Recovery vs* Procesos Críticos.
- Pruebas efectivas (OK/KO) de los Planes de Continuidad de Negocio.
- Pruebas efectivas (OK/KO) de los Planes Contingencia TI / *IT Disaster Recovery.*
- Etc.

Gestionando la crisis

COMITÉS DE GESTIÓN Y PROCESO DE ESCALADO

La adaptación, la flexibilidad y la diversidad son los pilares para soportar una crisis e incrementar la resiliencia de la compañía, según el artículo *Design of a Business Resilience Model for Industry 4.0 Manufacturers* (Morise & Prigge, 2017). Estos tres pilares se concretan en un *portfolio de productos y/o servicios y empleados altamente cualificados con diferente experiencia y formación, dado que son capaces de reaccionar rápidamente a eventos, reorganizar procesos y construir nuevas soluciones en base a dicha experiencia y conocimientos".*

En definitiva, un concepto que se enmarca en lo que podemos conocer como una compañía *agile,* capaz de reaccionar rápido a su entorno cambiante y proveer de nuevos servicios adaptados a las nuevas exigencias.

Esta flexibilidad se ha de soportar en estructuras organizativas acordes a las necesidades de la compañía. Si bien la estructura jerárquica clásica asociada a la estructura de silos puede ser más eficiente para conseguir resultados particulares de un área en concreto, no es la más apropiada para responder rápidamente a un evento de crisis, donde confluyen factores ajenos a la compañía y se deben tomar decisiones transversales de manera coordinada. Debe asegurar la comunicación con el gobierno corporativo, funcionando como asesor de éste.

Las compañías deben tener una estructura idónea, con líneas de dependencia y responsables con funciones y responsabilidades específicas claramente definidas para la gestión del riesgo inherente y residual a la Continui-

Adaptación, flexibilidad y diversidad son los pilares para soportar una crisis e incrementar la resiliencia de la compañía.

dad de Negocio. Esta estructura, aprobada por el gobierno corporativo, es una evidencia del compromiso con la Gestión de la Continuidad de Negocio y establece la ubicación tanto de los comités de gerencia (COMEX, Tecnología y Sistemas, Inversiones, Créditos, etc.) como de las comisiones del consejo (Auditoría, Riesgos, Cumplimiento, etc.) y líneas de reporte a los mismos. En el reglamento de estos comités, debe constar su composición y periodicidad de reunión, y las funciones de establecer acciones de supervisión, control y seguimiento de la Continuidad de Negocio.

En el reglamento de los comités de gerencia debe constar su composición y periodicidad de reunión, y las funciones d establecer acciones de supervisión, control y seguimiento de la Continuidad de Negocio.

Se tendrán en cuenta, tanto para escalar como desescalar, la toma de decisiones, incluyendo la posibilidad de instaurar un comité *ad hoc* (por ej. de Seguridad e Higiene), en caso de que la situación lo requiera. Este comité *ad hoc* centralizaría las acciones relacionadas con la Continuidad de Negocio para una coyuntura específica (por ejemplo, en el caso de COVID-19). Las actas de dichos comités aportarán trazabilidad de las decisiones tomadas y serán útiles para gestionar la mejora continua del proceso de Continuidad de Negocio.

El estándar ISO 22301-2020, en su capítulo 8.4.2 *Estructuras de respuesta,* establece la necesidad de *"implementar y mantener una estructura identificando uno o más equipos responsables de responder a incidentes".* Dicha estructura debe tener sus roles, responsabilidades y canales de comunicación claramente definidos, acordados y aceptados por todos los participantes.

En la misma serie, el estándar ISO 22320-2018, en su apartado 5.3 *Estructuras de Gestión de Incidencias* detalla qué funciones, tareas, roles y responsabilidades se deberían considerar al definir el proceso de gestión de incidentes en un sistema de Gestión de Continuidad de Negocio.

En compañías de gran tamaño pueden existir diferentes estructuras organizativas adecuadas al nivel de interlocución. Pero el gobierno corporativo debe formar parte de dicha estructura y su liderazgo y compromiso se ha de reflejar con la participación de un miembro de la dirección *(C-Level executive,* en inglés), con autoridad suficiente como para involucrar a las áreas afectadas y tomar medidas que dirijan la respuesta (Kelson, *IT Continuity Planning Audit/Assurance Program,* 2010).

Para dar soporte a la Gestión de Continuidad de Negocio, como mínimo, serían necesarias las siguientes funciones:

Comité de crisis

Su principal función es **definir la estrategia necesaria** con el objetivo de afrontar con garantías el desastre o incidente.

Recoge y **evalúa el impacto de una crisis** en la compañía y, si es el caso, convoca los comités de Continuidad de Negocio.

Es el encargado de aprobar la matriz de impacto de incidentes, y **establecer los umbrales de riesgo.**

Comité de continuidad

Su principal misión es **evaluar la situación de crisis y de continuidad.** Está compuesto por los responsables de las áreas de negocio involucradas en el Modelo de Continuidad de Negocio (p.ej. RRHH, Operaciones, Finanzas, Asesoría Jurídica, Comercial, Comunicación Corporativa, etc).

Tiene máxima capacidad de decisión y se reúne periódicamente o bien a demanda, en función de la situación de crisis. Pueden ser invitados a participar otros miembros de la compañía, si es necesario, para temas puntuales. Debe reportar al comité de crisis los resultados de su evaluación.

Comités o equipos técnicos

Tienen la responsabilidad, técnica y operativa, de las decisiones tomadas por los anteriores comités y ejerce de **nexo entre todos los equipos** que participan en las distintas fases de los planes de recuperación, transmitiendo las tareas a los responsables de los equipos de recuperación de las áreas de negocio.

ROL DEL GOBIERNO CORPORATIVO

Es el garante de la implantación de un sistema de control interno eficaz y apuntala las bases para la Continuidad de Negocio frente a situaciones adversas. Para este caso concreto, este sistema de control interno pasa a formar el sistema de Gestión de Continuidad de Negocio basado en los principios de autocontrol, autorregulación y autogestión, estableciendo los métodos, las políticas, los procedimientos, las acciones, los mecanismos de prevención, control, evaluación y de mejora continua de la compañía.

Su finalidad es tener seguridad sobre la consecución de sus objetivos y del manejo de los riesgos que afronta la entidad. Estos requisitos están definidos en las *buenas prácticas de Continuidad de Negocio* recogidas en el artículo 5 de la ISO 22301.

A este respecto, los responsables de la gestión de los procesos de Continuidad de Negocio, situados a niveles apropiados dentro de la estructura de la compañía y con visibilidad en la alta dirección, deben:

- Garantizar el establecimiento de una política y unos objetivos de Continuidad de Negocio, y velar por que éstos estén alineados con la dirección estratégica de la compañía.
- Comunicar la importancia de una continuidad de negocio eficaz en la entidad.
- Dirigir y apoyar a las personas para contribuir a la eficacia del sistema.
- Asegurar que los requisitos del sistema de Gestión de Continuidad de Negocio están integrados en los procesos de negocio de la compañía, con los recursos necesarios, y velar por el logro de los resultados previstos promoviendo la mejora continua.

Como ejemplo, en las compañías a las que pertenecen los profesionales que han participado en la elaboración de este documento, la involucración del gobierno corporativo durante la crisis COVID-19 tuvo un rol decisorio. Los comités de gestión de crisis adoptaron un rol de asesoramiento al gobierno corporativo, tomando como punto de partida el trabajo conjunto de las áreas de la compañía.

El Gobierno Corporativo es el garante de la implantación de un sistema de control interno eficaz y apuntala las bases para la Continuidad de Negocio frente a situaciones adversas.

Gestión de las operaciones

Las compañías pueden subcontratar parte de sus procesos de negocio y servicios, lo que implica una mayor dependencia de terceros en la gestión de materias primas, envases y embalajes, repuestos para fabricación, servicios de mantenimiento de las infraestructuras,

servicio de distribución, etc. Por ello, el análisis de riesgos y los planes de Continuidad de Negocio deben **contemplar las vulnerabilidades de toda la cadena de suministro, incluyendo las de los proveedores.** Cuando una crisis se presenta, hay que reevaluar la situación. Esta visión integral del negocio debe contener, entre otras:

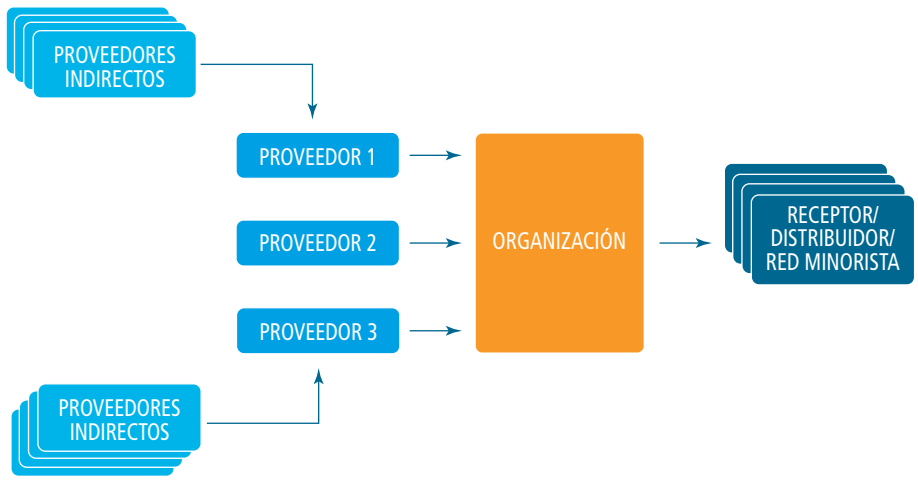
- **Evaluación de riesgos,** comprender cómo afectan a la consecución de los objetivos de la compañía, especialmente para la entrega de productos y servicios.
- **Priorizar activos y procesos críticos** para su recuperación en función de los objetivos de la compañía. Por ejemplo: centros de producción y almacenamiento alternativos, *hardware* redundante de alta disponibilidad, proveedores alternativos, etc.
- **Identificar posibles escenarios consecutivos de desastre** preparando acciones para abordarlos (escasez de materias primas alternativas, crisis en determinadas zonas geográficas, ...).
- **Implementar controles específicos** que permitan una gestión del riesgo dentro de los límites marcados por el apetito al riesgo de nuestra empresa para la situación dada.

La cadena de suministro aborda desde el aprovisionamiento de las materias primas hasta la entrega del producto final al cliente, pasando por el ciclo productivo de la compañía. Debemos controlar el flujo de bienes y servicios a lo largo de toda la cadena de suministro, incluyendo proveedores directos e indirectos, ya que una interrupción en cualquier punto de la cadena puede poner en peligro la continuidad de la compañía.

Durante la gestión de la crisis debemos reanalizar los proveedores relevantes para toda la cadena de suministro y comprobar cómo están funcionando sus planes de continuidad. Anticiparse a posibles fallos de suministros proporcionará tiempo suficiente a la compañía para gestionar este evento de una forma planificada, y ayudará a reducir los impactos y efectos de un riesgo en las operaciones.

Anticiparse a posibles fallos de suministro proporcionará tiempo para gestionar este evento de forma planificada, y ayudará a reducir los impactos y efectos de un riesgo en las operaciones.

CADENA DE PROVEEDORES



Supply chain resilence and continuity (ISACA)

Los aspectos a tratar en la planificación de la Continuidad de Negocio en las operaciones pueden incluir:

- Evaluar y planificar para realizar los ajustes necesarios ante desequilibrios de la oferta y la demanda ("gestión de la escasez") como, por ejemplo, analizar el impacto y posibles restricciones de personal, bienes y servicios propios y externos.
- Evaluar los plazos de recuperación y los criterios de escalado.

IDENTIFICACIÓN DE NUEVAS OPORTUNIDADES

En algunos momentos surgen oportunidades para que la compañía muestre nuevas capacidades ante mercados, clientes, proveedores o inversores. Su adaptación, flexibilidad y diversidad son factores clave para incrementar la resiliencia en las compañías.

En crisis globales en las que todo el ecosistema de la compañía sufre cambios significativos, es imprescindible actuar de manera adecuada frente a la velocidad de los cambios. Las acciones diseñadas para captar las nuevas oportunidades de mejora son diferentes, en función de esta velocidad, mientras que el alcance de la crisis es quien define los ámbitos que se puedan mejorar.

En crisis globales se abre un proceso de acompañamiento de los clientes actuales de la empresa para ofrecerles herramientas y servicios que favorezcan su resiliencia, tales como:

- Cancelación de servicios que no sean esenciales; uso de datos que ya están disponibles y que sean de utilidad para los clientes, etc.
- Reformulación de procesos comerciales; nuevos espacios para conseguir una mayor agilidad; obtener procesos comerciales más eficientes, con menos retrasos, etc.

Como respuesta a la crisis, la compañía debe identificar las nuevas oportunidades de negocio que pudieran asegurar su continuidad. Para identificarlas debe contemplar:

- Acelerar el proceso de desarrollo de negocio al máximo sin obstruir la gestión de la crisis. Es necesario anticipar cómo la crisis genera o crea nuevas necesidades en el mercado. Dar forma de manera proactiva a las necesidades que se identifiquen: M&A, *partnerships*, etc.
- Diagnosticar problemáticas a nivel de sector/ industria.
- Desarrollar nuevos canales de venta.
- Agilizar los procesos de innovación.
- Colaborar con el resto de los agentes sociales para mitigar los efectos de la crisis proporcionando medios, instalaciones o dotando de bienes a las administraciones públicas.

Los procesos de crisis aceleran métodos de transformación que de otra manera se hubieran alargado en el tiempo. Las dificultades sufridas han generado respuestas por parte de las compañías en diferentes campos como, por ejemplo:

- Aceleración o implantación de procesos de digitalización.

Como respuesta a la crisis, la compañía debe identificar las nuevas oportunidades de negocio que pudieran asegurar su continuidad.

En eventos de crisis el sistema de control interno puede no operar efectivamente, por lo que debe adecuarse a las nuevas realidades y posibilidades futuras.

- Evaluación del incremento y actualización del plan de respuesta de los ciber riesgos.
- Evaluación y actualización de los procesos llevados a cabo para el cumplimiento de las responsabilidades regulatorias.
- Identificación y revisión de las cláusulas contractuales clave con proveedores y terceros que afecten a la operativa de la compañía.
- Evaluación de nuevos proveedores no considerados hasta la fecha.
- Revisión de procesos y estrategias de aprovisionamiento.
- Revisión de planes de contingencia en función de disrupciones de suministro para proveedores.
- Redefinición de nuevas especializaciones dentro de la compañía que no fueron identificadas como críticas con anterioridad.
- Actualización de medidas de salud, seguridad y prevención de riesgos laborales.
- Actualización de las necesidades de capital y las previsiones de flujo de efectivo, considerando escenarios con aumento de la presión sobre las líneas de capital, tanto de explotación como de liquidez derivado de la disminución de los ingresos.
- Evaluación de los impactos económicos y posibilidades de ruptura de los *covenants* acordados en los contratos de financiación con las entidades financieras.
- Gestión del riesgo de fraude y de elusión de controles internos a todos los niveles de la compañía. En eventos de crisis, el sistema de control interno puede verse alterado y, en consecuencia, no operar efectivamente durante la duración del evento. Adicionalmente, podría encontrarse obsoleto, por lo que deberá adecuarse a las nuevas realidades y posibilidades futuras, como la automatización de determinados controles manuales que no se llevaran a cabo durante un evento de crisis.

Proceso de mejora continua

Una crisis combina detectar y reconocer las debilidades y/o aspectos de mejora de las compañías en un escenario adverso con la necesidad de continuar con su actividad. La realización de un ejercicio de análisis retrospectivo proporcionará una serie de lecciones aprendidas que, documentadas en protocolos de actuación, pueden ser aplicadas en futuros incidentes para mejorar la resiliencia de la compañía.

Esta mejora continua **nos permitirá minimizar los errores o pérdidas de forma permanente.** Seguir una serie de técnicas concretas (metodología) que permita a la compañía tener en cuenta e incorporar en sus procesos las lecciones aprendidas durante la crisis, es una herramienta imprescindible para fomentar esta mejora continua.

INTEGRACIÓN DE LAS LECCIONES APRENDIDAS EN LA COMPAÑÍA

Como ejercicio para identificar e incorporar las lecciones aprendidas tras una situación de crisis, John Rapa, presidente y CEO de la consultora Tellefsen and Company, LLC, propone –en el documento *Global Perspectives and Insights: Crisis Resilience* publicado por el IIA Global– *"una serie de cuestiones a plantear cuando la situación se tranquiliza"*. Entre ellas, destaca:

- ¿Cómo y quien descubrió el incidente?
- ¿Quiénes fueron los primeros en responder porque identificaron el efecto del incidente?
- ¿Cómo gestionó la gerencia de la unidad de negocio la respuesta al incidente?
- ¿Con qué frecuencia y con qué nivel de detalle se comunica la empresa con el personal, los clientes, los clientes clave, los proveedores de servicios clave, los reguladores y los medios de comunicación?
- ¿Se realizó una revisión *post mortem* en cuanto a la causa raíz de los incidentes, los efectos y los impactos en el negocio, así como las lecciones aprendidas?
- ¿Se implementó un plan de acción para abordar las deficiencias, los riesgos o las amenazas adicionales?

Será necesaria la aplicación de una metodología, identificando previamente los riesgos cubiertos, las preguntas clave a formular, las personas a entrevistar y los objetivos a cubrir. Todo ello permitirá analizar de manera objetiva y rigurosa la gestión de la crisis realizada.

El programa de trabajo habitual para el auditor interno es útil en esta fase de preparación, ya que se trata de una labor de canalización e identificación de buenas prácticas. Este ejercicio no es una auditoría de aseguramiento normativo, sino de identificación e integración de las lecciones clave en la compañía, concretando acciones que permitan aumentar la resiliencia ante futuras crisis.

Entrevistas

El orden de las entrevistas para conocer la respuesta de la compañía es relevante en el proceso de preparación del retorno de experiencia adquirido. Existen dos vías de aproximación:

- Tener un **primer contacto con las direcciones de las unidades de negocio;** entrevistar a continuación a los responsables de negocio y, finalmente, al comité de dirección para cumplir con dos objetivos:
  - obtener una visión más estratégica al final del proceso, y
  - compartir ya en ese momento las preocupaciones y dificultades más relevantes y repetidas entre los equipos de trabajo.
- Tener un **primer contacto con el comité de dirección** para conocer su estrategia y comprobar cómo se ha implementado en las unidades de negocio para cumplir con dos objetivos: a
  - conocer qué espera el comité de dirección, y
  - focalizar las entrevistas con las áreas de negocio para ver su grado de alineamiento frente a la estrategia.

Un buen punto de partida será la elaboración de un cuestionario para ordenar las entrevistas, siguiendo las fases naturales de la crisis: la preparación, la gestión y la recuperación. Asimismo, identificar métricas de análisis estandarizadas, alineadas con los objetivos del

Aplicar una metodología que identifique los riesgos cubiertos, preguntas clave, personas a entrevistar y objetivos a cubrir permitirá analizar objetivamente la gestión de la crisis.

comité de dirección, facilita la comparación entre las áreas de negocio, con objeto de identificar fácilmente aquellas unidades organizativas que han podido cumplir con mayor solvencia los objetivos y, por tanto, pueden aportar sus prácticas al resto de la compañía.

Métricas comparativas

Las métricas comparativas permiten medir el nivel de madurez de los procesos de gestión de crisis y deben alinearse con los objetivos previamente definidos por la dirección.

Permiten medir los niveles de madurez de los procesos de gestión de crisis y deben estar alineadas con los objetivos previamente definidos por la dirección de la compañía: ¿Cuáles son las prioridades de la compañía durante la crisis? ¿Cuándo y cómo podremos considerar que la empresa sale airosa de una situación de crisis?

Ejemplos de métricas y variables que pueden ser analizadas:

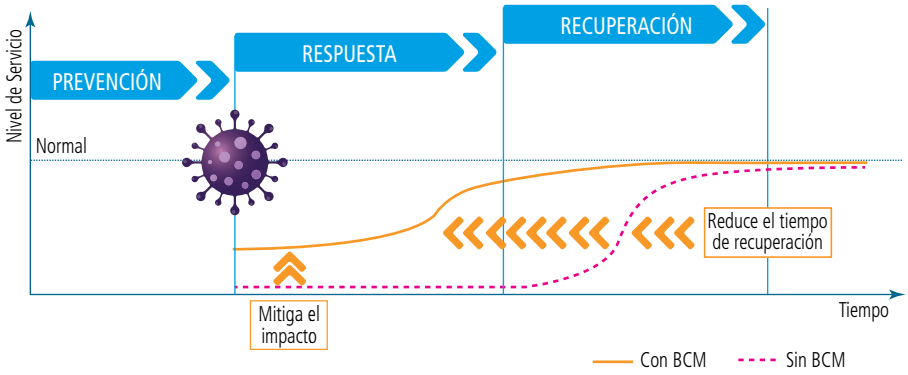
- **Continuidad de Negocio.** Número de instalaciones operativas; número de instalaciones cerradas; producción no realizada; producción no distribuida; etc.
- **Reactividad.** Tiempo que se ha destinado para la activación de la célula de crisis. Tiempo dedicado para la emisión de los primeros comunicados.
- **Protección de empleados.** Ratios frecuencia/impacto de H&S. En caso de crisis globales, indicadores que permitan comparar las ratios país con las ratios empresa.
- **Impacto financiero.** Impacto en cuenta de resultados antes y después de la puesta en marcha de medidas mitigadoras.
- **Cooperación de las áreas de negocio.** Resultados de encuestas efectuadas a las áreas de negocio solicitando *feedback* sobre interacciones realizadas.
- **Organización.** Inclusión de los ámbitos adecuados en los planes de gestión de crisis, existencia de un modelo operativo y de gobierno para la gestión de la crisis, nombramiento y asignación de funciones según la tipología de crisis, identificación de posiciones clave, existencia de plan de sucesión, designación de un equipo de alerta, etc.
- **Comunicación.** Existencia de un protocolo de activación de alertas. Suficiencia de las comunicaciones realizadas con todos los *stakeholders:* empleados, sindicatos, clientes, administraciones, opinión pública, proveedores, etc. Participación previa del departamento de comunicación en los simulacros. Inclusión del ámbito de comunicación en los planes de gestión de crisis, etc
- **Rapidez en la toma de decisiones en los comités.** Su frecuencia. Tiempo transcurrido en la implementación de acciones.
- **Anticipación.** Formación (calidad y frecuencia), realización de simulacros (creación de diferentes escenarios, participación de alta dirección, retorno de experiencia de los ejercicios, etc.). Disponibilidad previa y suficiencia de los marcos de actuación para la gestión de crisis y de los BCPs.

ASEGURAMIENTO DE MEJORAR EL BCP CON LOS PUNTOS DÉBILES

La disponibilidad de un BCP lo más completo posible es un factor clave para gestionar con éxito la crisis.

Durante el proceso de Retorno de Experiencia, es importante obtener *feedback* sobre la aplicación real de los BCPs durante la crisis.

Algunos aspectos a considerar en este ejercicio retrospectivo son la formulación de preguntas sobre la disponibilidad y exhaustividad del BCP, entender cómo ha contribuido en anticipar y reaccionar ante la crisis, verificar si había sido testado con anterioridad e identificar qué puntos son mejorables para próximas crisis.



Fuente: *Risk Management and Internal Audit in times of COVID-19.* KPMG

ISACA publicó un patrón de programa de trabajo (Kelson, *IT Continuity Planning Audit/Assurance Program,* 2010) que incluye capítulos específicos y puede servir de referencia para evaluar la formación y testear los planes de gestión de crisis.

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
2.5.1 **Training** Control: Key crisis responders and contributors are scheduled for and receive testing in the implementation of the crisis plan at least annually, and the executive crisis committee monitors the frequency and quality of the training.	DS7			x					
2.5.1.1 Determine if the training program scope is aligned with the crisis plan's training requirements.									
2.5.1.2 Determine if the training program participation is monitored.									
2.5.1.3 Determine if the training program attendance, scope and evaluations are summarized and reported to the executive crisis committee.									
2.6 **Crisis Management Plan Tests and Maintenance** Audit/Assurance Objective: The crisis management plan is tested and modified to reflect the results of the tests and changes in the business and operating environments.									
2.6.1 **Testing** Control: Testing procedures have been established, tested at least annually, the results of the testing have been analyzed, and identified weaknesses have been remediated.	DS4 ME4			x	x	x			
2.6.1.1 Determine if the crisis plan is tested at least annually.									
2.6.1.2 Determine if the various scenarios are tested.									
2.6.1.3 Determine if the test results are analyzed and the plan modified.									
2.6.2 **Plan Maintenance** Control: The crisis plan is routinely reviewed to ensure alignment with the business risks and requirements, and the plan is updated.	DS4 ME4			x	x	x			
2.6.2.1 Determine if the plan's risk assessment is updated at least annually, or more frequently if key business processes or requirements warrant.									
2.6.2.2 Determine if the plan documentation is updated to reflect risk assessment or test-driven modifications.									
2.6.2.3 Determine if a copy of the plan is maintained in a secure, off-site location.									
2.6.2.4 Determine if plan modifications are distributed to all first responders and the offsite archive when changes are made.									

El rol de Auditoría Interna y la Comisión de Auditoría frente a la resiliencia

El rol de Auditoría Interna puede variar en función del impacto de la crisis y de la fase de ésta –preparación, gestión o finalización–.

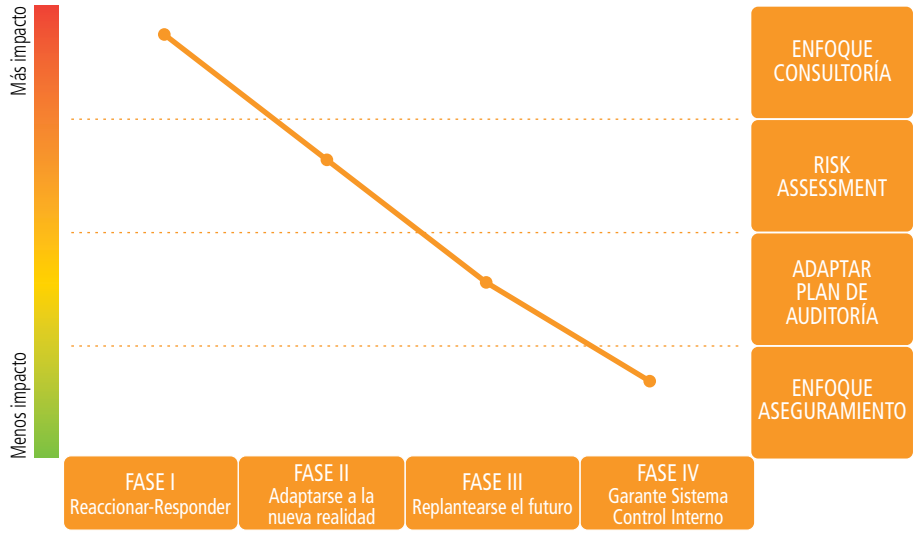
Los auditores internos pueden colaborar en las diferentes fases de una crisis, preparar a la compañía para afrontarla, gestionarla y asegurar el retorno de las lecciones aprendidas. Esto es así porque los auditores internos poseen:

- **Conocimiento transversal de la compañía.** Las crisis son multidisciplinares tal y como refleja la composición del comité de crisis. Auditoría Interna dispone de una visión única y estratégica de la compañía, con una perspectiva completa de todos los aspectos de negocio y de los procesos de gestión clave antes y durante la crisis.
- **Experiencia en crear y aplicar una metodología** (utilización de programas de trabajo enfocados a riesgos).
- **Disciplina para ejecutar los programas de trabajo con celeridad,** y ayudar a la compañía a prepararse ante situaciones de crisis similares, o para nuevas olas en la misma crisis.
- **Interlocución con los órganos de gobierno al más alto nivel.**

Estas competencias determinan la participación de Auditoria Interna para incrementar la resiliencia de las compañías.

Su rol puede variar en función del impacto de la crisis y de la fase de ésta (preparación, gestión, finalización).

FASES DE LA CRISIS Y PARTICIPACIÓN DE AUDITORIA INTERNA



Fuente: elaboración propia.

PREPARACIÓN Y ANTICIPACIÓN ANTE LAS CRISIS

El rol de Auditoría Interna está definido en las guías para la implementación de las *Normas Internacionales para la Práctica Profesional de Auditoría Interna*[2] en la que se establece que:

"La actividad de Auditoría Interna debe evaluar y hacer recomendaciones apropiadas para mejorar los procesos de gobierno de la compañía para:

- *Tomar decisiones estratégicas y operativas.*
- *Supervisar el control y la gestión de los riesgos.*
- *Promover la ética y los valores apropiados dentro de la compañía.*
- *Asegurar la gestión y responsabilidades eficaces en el desempeño de la compañía.*
- *Comunicar la información de riesgos y control a las áreas adecuadas de la compañía.*
- *Coordinar las actividades y la información de comunicación entre el consejo de administración, los auditores internos y externos, otros proveedores de aseguramiento y dirección."*

Auditoría Interna tiene un rol activo para preparar a la compañía frente a una crisis, con el objetivo de incrementar la resiliencia de ésta.

Actividades previas a una crisis[3]

- **Marco de Gobierno y Gestión de Crisis** (políticas, estructuras definidas y comités de gestión de crisis, procesos/criterios de activación y escalado/decisión, valoración de la efectividad de los entrenamientos y simulacros de gestión de crisis, incorporación de las lecciones aprendidas en los simulacros en los procesos de gestión de crisis, etc.)

- **Considerar la continuidad de negocio como un riesgo que debe revisarse y contemplarlo dentro del Plan Anual de Auditoría.** En el caso de que, para elaborarlo, Auditoría Interna se apoye en un área de segunda línea encargada de identificar y medir los riesgos de la compañía, debe asegurar que el riesgo de Continuidad de Negocio esté contemplado en el universo de riesgos de la compañía. Adicionalmente, la labor de evaluación del riesgo por parte de dicha Segunda Línea debe integrarse dentro del Plan de Auditoría Interna como parte del universo auditable.

  Un plan de Continuidad de Negocio maduro incluye pruebas y simulacros que permiten a la compañía prepararse para situaciones de crisis y adiestrar a los empleados. La existencia de esas pruebas y simulacros, cómo se realizan, cuándo, en qué entornos, con qué nivel de profundidad, etc deberían contemplarse en el Plan Anual de Auditoría.

- **Compartir el conocimiento y la revisión de los planes con la alta dirección y la Comisión de Auditoría.**

- **Evaluar los acuerdos con proveedores clave,** asegurando que existen cláusulas de nivel de servicio, derecho a realizarles auditorías y que se realizan los informes necesarios para la administración, con respecto al

El Plan de Auditoría Interna debe contemplar pruebas y simulacros, y cómo, cuándo, en qué entornos y con qué profundidad se realizarán.

2. Guía de implementación de la Norma 2210 – Gobierno Corporativo.

3. *IPPF-Practice Guide Business Continuity Management*. IIA Global. Agosto 2014.

La Comisión de Auditoría actúa de salvaguarda de la independencia y objetividad de Auditoría Interna, y debe estar informada de los riesgos que pueden desencadenar la activación del Plan de Continuidad.

entorno de control del proveedor. En contratos clave para la compañía, Auditoría Interna puede realizar una labor de asesoramiento sobre el marco de control que mitigue los riesgos asociados a la discontinuidad del servicio prestado por proveedores clave. Puede ser especialmente relevante su participación en la redacción de cláusulas *rigth to audit* (junto con el resto de las funciones de aseguramiento presentes en la compañía, que puedan requerir efectuar una revisión del proveedor), en las que se debe garantizar la posibilidad de que sea la propia Auditoría Interna u otra función de la compañía, quien realice las revisiones y verifique la existencia de un plan de continuidad en los proveedores clave.

- **Asesorar en el desempeño de las evaluaciones o autoevaluaciones de riesgo de Continuidad de Negocio**. Auditoría Interna conoce de forma global y en profundidad los procesos desempeñados por la compañía, lo que debe ser puesto en valor como input para las evaluaciones de riesgos relacionados con la Continuidad de Negocio.

- **Realizar trabajos de aseguramiento relacionados con el Plan de Continuidad de Negocio,** como parte del Plan Anual de Auditoría (componentes del plan, protocolos de comunicación, aspectos operativos, etc).

- **Establecer el rol del auditor interno y la Comisión de Auditoría en los Planes de Continuidad de Negocio,** si no están descritos en el Estatuto de Auditoría.

Cabe destacar que el *Marco Internacional para la Práctica Profesional de la Auditoría Interna,* en la Norma y Guía de implementación-1112, indica: *"Cuando el director de Auditoría Interna asuma o se espera que asuma un papel y/o responsabilidades adicionales a la de Auditoría Interna, debe aplicar salvaguardas para limitar impedimentos a la independencia y objetividad"*. Resulta clave la importancia de las salvaguardas, como la vigilancia de las actividades, a menudo realizada por la Comisión de Auditoría, para resolver impedimentos potenciales a la independencia y objetividad del DAI.

El rol de la Comisión de Auditoría consiste, entre otros, en actuar de salvaguarda de la independencia y objetividad del área de Auditoría Interna, así como estar informada de los riesgos que pueden desencadenar la activación del Plan de Continuidad de Negocio y su gestión. En este sentido, **la supervisión de los riesgos no financieros por la Comisión de Auditoría ha ido cobrando especial relevancia** en los últimos años, quedando plasmada finalmente en la última revisión en 2020 del **Código de Buen Gobierno de Sociedades Cotizadas.**

Así, la **Recomendación 12** identifica, dentro de las funciones del consejo de administración, la de promover la continuidad del negocio[4] delegándose, según el propio Código, en la Comisión de Auditoría la labor de supervisión de los riesgos que puedan poner en causa dicha continuidad. Así, la **Recomendación 42,** establece: *"que además de las previstas en*

4. Que el consejo de administración desempeñe sus funciones con unidad de propósito e independencia de criterio, dispense el mismo trato a todos los accionistas que se hallen en la misma posición y se guíe por el interés social, entendido como la consecución de un **negocio rentable y sostenible a largo plazo, que promueva su continuidad** y la maximización del valor económico de la empresa

la ley, corresponda a la comisión de auditoría las siguientes funciones: a) Supervisar y evaluar (…) los sistemas de control y gestión de riesgos financieros y no financieros relativos a la sociedad y, en su caso, al grupo –incluyendo los operativos, tecnológicos, sociales, medioambientales, políticos y reputacionales o relacionados con la corrupción– (…)". Es dentro de la categoría de riesgos de carácter no financiero donde se pueden englobar especialmente los relacionados con gestión de crisis y Continuidad de Negocio.

REACCIÓN, GESTIÓN Y SOPORTE DURANTE LA CRISIS

Las crisis transforman la realidad de las compañías de manera repentina, ya sea de forma temporal o permanente; además, la contundencia de este cambio variará dependiendo de su impacto y alcance.

Actividades específicas

Entre las actividades específicas a desarrollar por Auditoría Interna durante la gestión de la crisis, acordadas por la Comisión de Auditoría o el Gobierno Corporativo, podemos enumerar:

- **Supervisar y evaluar la respuesta** de la compañía ante un evento de crisis.
- **Formar parte del comité de gestión de crisis,** para garantizar que se tienen en cuenta los riesgos que pueden afectar durante el incidente y realizar recomendaciones de acciones que se pueden acometer, bajo una óptica de consultoría.
- **Participar en la gestión de crisis y recuperación de la compañía,** según lo acordado y autorizado por la Comisión de Auditoría o el Gobierno Corporativo.
- **Observar el incidente para tenerlo en cuenta en el plan de auditoría** para años posteriores.
- **Adaptar** a la compañía, por contingencias sobrevenidas, **el Plan de Auditoría** y la disposición de los recursos internos. **Establecer nuevos objetivos y riesgos.**

Como ejemplo, en las compañías a las que pertenecen los profesionales que han participado en la elaboración de este documento, los diferentes departamentos de Auditoría Interna adoptaron las siguientes vías de actuación durante la gestión de la crisis COVID-19:

- Tercera Línea sin participación en la gestión de la crisis, pero como ente consultado por las áreas de negocio de la entidad o por organismos reguladores de la Administración Pública.
- Asunción temporal de los roles de gestión de riesgos y control interno, con las debidas salvaguardas.

Por su parte, la Comisión de Auditoría debe garantizar su labor de supervisión de la gestión de riesgos durante el período de crisis a través de los mecanismos que considere más convenientes, mediante reuniones con la Segunda Línea o recibiendo un reporte directo de Auditoría Interna.

ROL DE AUDITORÍA INTERNA Y EVALUACIÓN DE LA EXPERIENCIA

Cuando la crisis ha finalizado, Auditoría Interna debe centrarse en el enfoque de aseguramiento, contribuyendo a la adecuada evaluación y funcionamiento del sistema de control interno de la compañía mediantes acciones esenciales como:

- **Realizar ejercicios de análisis de causa-raíz** (*Root Cause Analysis)* para identificar los orígenes de los eventos que han dado lugar a la crisis y facilitar la emisión de recomendaciones más efectivas para que los riesgos materializados no vuelvan a producirse.
- **Asegurar que existen medidas o controles nuevos** para los casos de riesgos materializados durante la crisis.
- **Asegurar que los procesos que se mostraron débiles son perfeccionados** mediante planes de acción por parte de la compañía, cuya revisión puede ser incorporada en el Plan de Auditoría Interna

La involucración de los profesionales de los diferentes departamentos de Auditoria Interna que han participado en este documento tras la gestión de la crisis COVID-19 se centró en:

- Incluir en el Plan de Auditoría Interna el aseguramiento de los sistemas de gestión de crisis.
- Asumir un rol más activo de Auditoría Interna en la preparación de la gestión de futuras crisis.

Conclusiones

Si bien existen estándares internacionales y referencias globales de mejores prácticas para la preparación ante una crisis, no existe un modelo único que sea válido para todas las compañías.

Cada entidad debe poner en marcha y coordinar las actividades necesarias que le permitan identificar y evaluar los requisitos y necesidades que les afectan para el desarrollo e implementación de su Sistema de Gestión de Continuidad de Negocio (BCM). Mantener a los equipos entrenados para enfrentarse a escenarios y situaciones complejas es un aspecto esencial. Para ello, una pieza fundamental en un sistema maduro de respuesta a la crisis es la realización periódica de pruebas y simulacros que permitan la mejora continua del proceso de Continuidad de Negocio.

Los auditores internos, al disponer de un vasto conocimiento transversal de la compañía, de la experiencia en crear y aplicar una metodología de trabajo enfocada a riesgo, y de la interlocución necesaria con los órganos de gobierno al más alto nivel, representan una oportunidad de oro para aportar estas habilidades en la preparación y gestión de la crisis y la posterior vuelta a la normalidad de sus compañías.

Durante las fases de **preparación y anticipación de la crisis,** Auditoría Interna evalúa y propone recomendaciones para introducir mejoras en los procesos de gobierno de la compañía, con los objetivos fundamentales de supervisar el control y la gestión de riesgos, comunicar los controles al resto de áreas y asegurar la gestión y responsabilidades apropiadas dentro de la compañía.

En cuanto a las fases de **reacción, gestión y soporte durante la crisis,** Auditoría Interna puede supervisar y evaluar la respuesta proporcionada por la compañía, formar parte del comité de crisis y tener en cuenta el incidente de crisis para mejorar y/o retroalimentar el Plan Anual de Auditoria. Esta participación vendrá condicionada por los acuerdos previos alcanzados con la Comisión de Auditoría y/o el Gobierno Corporativo de la entidad.

Tras la crisis, para la preparación del retorno de la experiencia y la obtención de lecciones aprendidas a incorporar en el proceso de mejora continua de la compañía, Auditoría Interna debe asegurarse de la existencia y eficacia de los controles diseñados para los riesgos que se hayan materializado en la entidad durante el evento de crisis e, igualmente, incluir en el Plan Anual de Auditoría aquellos procesos que durante este período han mostrado debilidades o aquellos en los que, por la razón que sea, se han identificados potenciales ámbitos de mejora.

Bibliografía

- AGNES M., LUKASZEWSKI, PARRA, H.R., RAPA, J. *Global perspectives and insights: crisis resilience – Issue 7.* The Global Institute of Internal Auditors, 2017. https://global.theiia.org/knowledge/Public%20Documents/GPI-Crisis-Resilience.pdf
- BAKSHI, S. *Supply Chain Resilience and Continuity: Closing Gaps Esposed in a Global Pandemic.* ISACA, 2020. https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpbsc?cid=pr_2004609
- BRANDENBURG, R., IVELL, T., SEKERIS, E., GRUBER, M., & LEWIS, P. *Striving for operational resilience.The questions Boards and Senior management should ask.* Oliver Wyman, 2019. https://www.oliverwyman.com/our-expertise/insights/2019/may/striving-for-operational-resilience.html
- COSO. *Enterprise Risk Management. Integrating with Strategy and Performance. Executive Summary.* 2017.
- EVEREST, D., ROY, G., KEATING, M., & PETERSON, B. *Global Technology Audit Guide Business Continuity.* The Institute of Internal Auditors, 2008.
- KELSON, N. *Crisis Management Audit/Assurance Program.* (ISBN 978-1-60420-161-1) ISACA, 2010.
- KELSON, N. *IT Continuity Planning Audit/Assurance Program.* (ISBN 978-1-60420-079-9) ISACA, 2010.
- MORISE, M., & PRIGGE, C. *Design of a Business Resilience Model for Industry 4.0 Manufacturers.* Association for Information Systems, 2017. https://aisel.aisnet.org/amcis2017/OrganizationalIS/Presentations/4/

Anexo

Definición de conceptos clave

A modo enunciativo, pero no limitativo, estos son los conceptos clave en Continuidad de Negocio:

- **Crisis:** Un evento crítico que, si no se gestiona de manera adecuada, puede afectar dramáticamente la rentabilidad, reputación o capacidad de una compañía para operar. *(Ref. The International Glossary for Resilience – DRI).*
- **Continuidad de Negocio:** Prácticas en una compañía para recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado, tras una interrupción no deseada o crisis.
- **Plan de Continuidad de Negocio:** Proceso de gestión global que identifica potenciales amenazas para una compañía y los impactos que pueden tener en las operaciones comerciales, si se materializan, proporcionando un marco para construir resiliencia organizacional, con la capacidad para dar respuesta eficaz que salvaguarde los intereses de sus partes interesadas, su reputación, marca y actividades de creación de valor. *(Ref. The International Glossary for Resilience – DRI).*
- **Resiliencia:** La capacidad de prepararse y adaptarse a las condiciones cambiantes y recuperarse rápidamente de las interrupciones operativas. La resiliencia incluye la capacidad de resistir y recuperarse de ataques deliberados, accidentes o amenazas o incidentes que ocurren de forma natural. *(Ref. The International Glossary for Resilience – DRI).*
- **BIA:** El análisis de impacto al negocio *(Business Impact Analysis)* es otro elemento utilizado para estimar la afectación que podría padecer una compañía como resultado de la ocurrencia de algún incidente o un desastre
- **MTD** *(Maximum Tolerable Downtime):* indica la cantidad máxima de tiempo que un proceso puede estar sin funcionar sin causar un perjuicio grave a la compañía.
- **RTO** *(Recovery Time Objetive):* establece cual es el tiempo objetivo para recuperar el proceso a un nivel aceptable, teniendo en cuenta que se encuentra en una situación de emergencia. Este tiempo es menor al MTD. En compañías de ámbito industrial para los sistemas de producción este valor tenderá a 0.
- **RPO** *(Recovery Point Objective):* establece cual es la pérdida máxima de información que puede asumir un área antes de que el proceso pueda volver a operar, medida desde el momento de la interrupción; es decir, las operaciones realizadas en las últimas 12 horas, los últimos 2 días, la última semana…. En compañías donde el punto crítico es asegurar las transacciones realizadas este valor es especialmente crítico.
- ***Covenants.*** Financiación que está sujeta a compromisos o cumplimiento de ciertos indicadores. Si se dejan de cumplir hay penalizaciones y se pone en riesgo la financiación.

Normativas ISO de referencia

Gestión de Riesgos

- ISO 31000:2018 - Gestión del riesgo. Directrices.
- ISO/TR 31004:2015 - Gestión del riesgo. Orientación para la implementación de la Norma ISO 31000.
- ISO 31010:2019 - Gestión del riesgo. Técnicas de evaluación del riesgo.
- NS 5814:2008 - *Requirements for risk assessment.*

Continuidad de negocio - TI - Resiliencia organizacional

- ISO 27000:2019 - Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Visión de conjunto y vocabulario.
- ISO 27001:2017 - Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.
- ISO/IEC 27002:2017 - Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información.
- ISO/IEC 27005:2008 - *Information technology - Security techniques - Information security risk management.*
- ISO 27031:2011 - *Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity.*
- ISO/IEC 27701:2019- (Privacidad información): *Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines.*
- ISO 22300:2018 - Seguridad y Resiliencia. Vocabulario .

- ISO 22301:2020 - Seguridad y resiliencia. Sistema de Gestión de la Continuidad del Negocio. Requisitos.
- ISO 22313:2020 - Seguridad y resiliencia. Sistemas de gestión de la continuidad del negocio. Directrices para la utilización de la norma ISO 22301.
- ISO 22316:2020 - Seguridad y resiliencia. Resiliencia organizacional. Principios y atributos.
- ISO/TS 22317:2020 - Protección y seguridad de los ciudadanos. Sistemas de gestión de la continuidad del negocio. Directrices para el análisis del impacto sobre el negocio.
- ISO / TS 22318:2015 - *Societal security - Business continuity management systems - Guidelines for supply chain continuity.*
- ISO 22320:2013 - Protección y seguridad de los ciudadanos. Gestión de emergencias. Requisitos para la respuesta a incidentes.
- ISO 22320:2018 - *Security and resilience _ Emergency management - Guidelines for incident management.*
- ISO/TS 22330:2020 - Seguridad y resiliencia. Sistemas de gestión de la continuidad del negocio. Directrices para los aspectos humanos de la continuidad del negocio.
- ISO/TS 22331:2020 - Seguridad y resiliencia. Sistemas de gestión de la continuidad del negocio. Directrices para la estrategia de continuidad del negocio.
- ISO 22395:2018 - *Security and resilience - Community resilience - Guidelines for supporting vulnerable persons in an emergency.*
- ISO 22398:2013 - *Societal security - Guidelines for exercises.*
- ISO 22399:2007: Guía para la preparación ante incidentes y gestión de la continuidad operativa.

Otros aplicables

- ISO/IEC 20000-1:2018 - Tecnologías de la información. Gestión de Servicios. Parte 1: Requisitos del Sistema de Gestión de Servicios (SGS).
- ISO/IEC 38500:2015 - *Information technology - Governance of IT for the organization.*
- PAS 200 / BS 11200: Gestión de crisis. Orientación y buenas prácticas.
- Guías NIST – SP 800.
- ITIL *(Information Technology Infrastructure Library).*
- Cobit 5.
- ISO 22301: 2020: es la nueva norma internacional de Gestión de Continuidad de Negocio que, a través del ciclo de mejora continua (PDCA), establece los requisitos para la planificación, el establecimiento, la implantación, la operación, la supervisión, la revisión, la prueba, el mantenimiento y la mejora de un SGCN documentado teniendo en cuenta la gestión de los riesgos globales de cada compañía y su capacidad de resiliencia.
- Integración con otros sistemas (fuente AENOR): https://www.aenor.com/certificacion/tecnologias-de-la-informacion/continuidad-negocio.
- El modelo de Gestión de la Continuidad del Negocio está alineado con otros como el de Seguridad de la información (UNE-ISO/IEC 27001), Gestión del Servicio de TI (UNE-ISO/IEC 20000-1) o Gestión de la Calidad (UNE-EN ISO 9001) con el objeto de facilitar la consistencia necesaria y permitir la sinergia en la implantación y operación de cada aspecto de gestión. Concretamente, la Norma UNE-ISO/IEC 27001 contempla la continuidad del negocio como un elemento clave dentro de la gestión de la seguridad de la información.
- ISO 22300:2018: Define los términos utilizados en los estándares de seguridad y resiliencia. Esta norma es revisada cada 5 años.
- ISO 22313:2020: Seguridad y resiliencia. Sistemas de gestión de la continuidad del negocio. Directrices para la utilización de la norma ISO 22301. (ISO 22313:2020). (Ratificada por la Asociación Española de Normalización en abril de 2020).
- ISO / TS 22318 Gestión de la Continuidad de Negocio: El objetivo es asegurar que se toman las medidas adecuadas para proteger a las compañías de las interrupciones del negocio provocadas por la ruptura de la cadena de suministro.
- Este TS proporcionará buenas prácticas en la evaluación y gestión de cadenas de suministro externo de bienes y servicios, así como de servicios de sociedades intracomunitarias. El objetivo es asegurar que se toman las medidas adecuadas para proteger a las compañías de las interrupciones del negocio provocadas por la ruptura de la cadena de suministro.
- ISO/IEC 27001 (Seguridad Información): gestión eficaz de la seguridad de la información permite garantizar su confidencialidad, asegurando que sólo quienes estén autorizados puedan acceder a la información; su integridad, asegurando que la información y sus métodos de proceso son exactos y completos, y su disponibilidad, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.
- ISO/IEC 27701 (Privacidad información): considerando el principio de responsabilidad proactiva, es una herramienta que ayuda a cumplir con los principios y obligaciones que impone la legislación en

materia de Protección de Datos y Privacidad, como pueden ser el Reglamento Europeo de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD).

Integración con otros sistemas:

Además de ser una extensión para ISO 27001, ambos referenciales se pueden integrar con:

- ISO 20000-1 – Gestión de Servicios TIC.
- Esquema Nacional de Seguridad (ENS - RD 3/2010).
- ISO 22301 – Gestión de Continuidad de Negocio.
- ISO 27017/ISO 27018 – Seguridad y Privacidad en *Cloud.*
- RP-CSG-064 Reglamento particular de certificación de sistemas de gestión de continuidad de negocio.
- BS 65000: Guía para la Resiliencia Organizacional. pretende mejorar los sistemas para la gestión de una crisis, así como las prácticas de Gestión de Continuidad de Negocio mediante la integración de éstos en un programa más amplio denominado "Programa sobre la capacidad de recuperación".

Introducción a SOC Control de Organización de Servicios

SOC 1: Aseguramiento sobre la información financiera

ESTÁNDARES DE REFERENCIA:

· *International Standard on Assurance Engagements 3402* (ISAE 3402): Estándar internacional de aplicación en el ámbito europeo que recoge un conjunto de buenas prácticas para la evaluación de controles en una compañía de servicios.

  Proporciona la evidencia suficiente sobre el nivel de control interno implantado dentro de una compañía de prestación de servicios, de tal forma que pueda:

  - Obtener el conocimiento suficiente de la naturaleza y significado de los servicios prestados por la compañía de servicios y de su efecto en los controles internos de la entidad usuaria relevantes, y así identificar y valorar los riesgos de incorrección material.
  - Diseñar y aplicar procedimientos de auditoría para responder a dichos riesgos.

· *Statement on Standards for Attestation Engagements 18* (SSAE 18): Equivalente a ISAE 3402 de aplicación al entorno norteamericano.

  De forma adicional a lo indicado para el ISAE 3402, se introducen las siguientes novedades:

  - La necesidad de realizar una evaluación de los riesgos, al menos, anualmente, con el fin de alinear el entorno de control a los riesgos clave identificados y evaluados por la compañía.
  - La inclusión de un apartado en el informe de aseguramiento sobre proveedores o externos que realizan actividades críticas en la compañía con impacto en los servicios prestados por ésta a terceros.

EN EL MARCO DE ESTOS DOS ESTÁNDARES SE PUEDEN EMITIR DOS TIPOLOGÍAS DE INFORMES:

· Informe SOC 1 - Tipo I que incluye:
  - un análisis de la compañía del servicio y de su entorno de control.
  - una descripción de los controles relevantes en un momento específico
  - opinión sobre si los controles fueron adecuadamente implantados para lograr sus objetivos, mediante Walkthrough.

· Informe SOC 1 - Tipo II, que además de los dispuesto en el Informe Tipo I se considera:
  - una descripción de las pruebas ejecutadas sobre los controles y resultados obtenidos, mediante Testing.

SOC 2 y SOC 3: Aseguramiento sobre los controles operativos

ESTÁNDAR DE REFERENCIA:

· International Standard on Assurance Engagements 3000 (ISAE 3000)

  Una guía en la que se establecen los principios y requerimientos que garanticen la conducta ética y la gestión de la calidad y el rendimiento. Su ámbito de aplicación es, por lo general, para auditorías de control interno, sostenibilidad y cumplimiento normativo.

  El alcance de este tipo de revisiones de terceros no se limita a los sistemas involucrados con el procesamiento de las transacciones financieras, sino en los ámbitos de la seguridad, disponibilidad, confidencialidad e integridad de procesamiento.

Los informes de SOC 2 son más detallados en comparación con los informes de nivel de síntesis de SOC 3. Y en ambos casos pueden, asimismo, emitirse de Tipo I o Tipo II de forma análoga a lo expuesto anteriormente, en relación con su alcance.

En cuanto a los informes de verificación de controles en una compañía de servicios bajo estos estándares, cabe destacar que proporcionan un grado de seguridad ante terceros sobre los controles que están implementados por parte de una compañía prestadora de servicios. Estos Informes de Aseguramiento SOC son emitidos por una entidad revisora independiente para garantizar la objetividad de las conclusiones.

OTRAS PRODUCCIONES DE LA FÁBRICA DE PENSAMIENTO

AUDITORÍA INTERNA EN LA ESTRATEGIA DE NEGOCIO

Este documento recoge el trabajo de Auditoría Interna en la definición y seguimiento de la estrategia de la compañía, describe los posibles roles que puede desempeñar respecto a la estrategia de negocio, y aporta una visión práctica de cómo ejecutar dichos roles en las distintas fases del proceso estratégico.

AUDITORÍA INTERNA DEL GOBIERNO DEL DATO

Aborda los problemas existentes y las mejores prácticas para resolverlos en lo referente a la definición de un buen gobierno del dato. Se analizan a fondo varios aspectos, desde el ciclo de vida del dato –incluyendo su trazabilidad y calidad– hasta metodologías y normativas aplicables en el proceso de gobierno del dato. Todo desde la perspectiva de Auditoría Interna.

AUDITORÍA INTERNA DE LA GESTIÓN DE PROYECTOS

Gestionar un proyecto implica planificar, organizar y dirigir el conjunto de procesos y operaciones diseñados para manejar el proyecto de inicio a fin, y Auditoría Interna debe proporcionar aseguramiento independiente para controlar los riesgos relacionados con el cumplimiento de objetivos.

ENTORNO DE CONTROL: SIETE PREGUNTAS QUE CUALQUIER CONSEJERO DEBE PLANTEARSE

A través de siete preguntas, cualquier Consejero podrá comprobar si su organización dispone de un entorno de control fuerte, ya que el documento resume los puntos críticos para asegurar que el entorno de control en la empresa es adecuado para cumplir su misión de protección de valor.

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Este documento abarca el rol de Auditoría Interna en la supervisión de los mecanismos de gestión de crisis y la resiliencia del negocio, así como el papel que asume en la fase previa, durante y después de que se produzca una crisis; e identifica las mejores prácticas relacionadas con la actuación de Auditoría Interna en este tipo de trabajos.

Instituto de Auditores Internos de España

The Institute of Internal Auditors