isms forum

GESTIÓN DE PLANES DE **CONTINUIDAD DE NEGOCIO** PARA PYMES

GUÍA Y BUENAS PRÁCTICAS

GESTIÓN DE PLANES DE CONTINUIDAD DE NEGOCIO PARA PYMES

Con la participación de los siguientes profesionales y organizaciones:

Dirección y coordinación

Toni García
Olga Forné

Participantes

Álvaro Lanza
Elisabet Viladomiu
Ignacio Hornes
Macarena Rodríguez
Manel Herrer
Mara Fernández
María Cumbreras ARIA
Marta Bellere
Pedro Bennasar
Raquel Garrote
Santiago Raúl de la Fuente

Diseño y maquetación

Raquel García, Responsable de Comunicación Externa de ISMS Forum

ÍNDICE

1 RESUMEN EJECUTIVO

Desastres naturales, fallos tecnológicos, brechas de datos o ciberataques son sólo algunos de los riesgos a los que prácticamente todas las organizaciones están expuestas de forma permanente y sobre los que es complicado predecir cómo, cuándo y dónde se van a materializar o, lo que es lo mismo, su impacto sobre el negocio. Es cierto que las amenazas abren un escenario de incertidumbre que en ocasiones no podemos controlar, por ello debemos planificar nuestra forma de actuar y responder frente a ellas construyendo una resiliencia adecuada para el negocio.

Para llevar a cabo esta planificación y capacidad de respuesta se desarrollan los denominados Planes de Continuidad de Negocio (en adelante, también, 'PCN')[1] que ayudan a las organizaciones en la identificación de aquellas debilidades o vulnerabilidades sobre las que la acción de un agente interno (fallo eléctrico, error en la ejecución de una tarea manual…) o externo (inundaciones, hackeo…) pueda ocasionar un daño, una interrupción o una paralización de la actividad del negocio; y, además, sirven de guía para el diseño de estrategias que minimicen posibles impactos negativos.

Existen diversas guías de buenas prácticas, normas y estándares internacionales que nos pueden orientar en la construcción de un PCN, como es la "Norma ISO 22301: Gestión de la Continuidad de Negocio"[2], que son excelentes modelos, pero requieren para su implantación de unos esfuerzos, plazos, recursos, personas y costes difícilmente asumibles por las pequeñas y medianas empresas (PYMEs) que representan en 2021 el 83% del tejido empresarial de España.[3]

ISMS Forum, con la motivación de incentivar, facilitar y ofrecer una solución a la implementación de los Planes de Continuidad de Negocio en las PYMEs, elabora la presente guía en la que se incluyen escenarios, herramientas y consejos para el diseño, puesta en marcha y mantenimiento de los PCN.

[1] Plan de Continuidad de Negocio (PCN), en inglés: "Business Continuity Plan" (BCP).
[2] La Norma ISO 22301 "Gestión de Continuidad de Negocio" de BSI se puede encontrar en https://www.bsigroup.com/es-ES/ISO-22301-continuidad-de-negocio/.
[3] Datos: Instituto Nacional de Estadística (https://www.ine.es/).

La elaboración de un PCN no es tarea fácil, por ello, hemos trabajado para reducir su complejidad, limitando los escenarios a aquellos que pueden ser más relevantes para las organizaciones. En esta línea, la guía se estructura en cuatro casos prácticos que sirven como introducción al mundo de los Planes de Continuidad de Negocio a través de un enfoque sencillo y flexible para permitir a las organizaciones anticiparse a situaciones de riesgo, superarlas y abordar nuevos escenarios con la garantía de saber qué hacer en cada momento.

2 NOTA DE LOS REDACTORES

ISMS Forum presenta la primera edición de la "Gestión de planes de continuidad de negocio para PYMEs". El objetivo de esta guía es ofrecer a las Pequeñas y Medianas Empresas un punto de partida con la información, ejemplos y referencias básicas para iniciarse en la elaboración de los planes de continuidad de negocio.

La "Gestión de planes de continuidad de negocio para PYMEs" se actualiza periódicamente para estar al día de los cambios y riesgos que pueden afectar al ecosistema empresarial considerando tendencias, tecnologías, amenazas y lecciones aprendidas.

Del mismo modo que el resto de las guías, la "Gestión de planes de continuidad de negocio para PYMEs" es el resultado de la contribución de un grupo de profesionales cualificados y con amplia experiencia en las áreas de continuidad de negocio, riesgos tecnológicos, protección de datos y seguridad de la información que voluntariosamente han ofrecido su tiempo y conocimientos para dar soporte al tejido empresarial de las PYMEs.

Todas las personas que han colaborado en la creación y publicación de esta guía deseamos que su contenido sea interesante y de utilidad. Asimismo, nos gustaría hacer partícipe al lector e instar a que contribuya con cualquier sugerencia o apreciación sobre la presente guía y que ayude a mejorar su contenido.

3 INTRODUCCIÓN

3.1 Introducción a la guía

El concepto de continuidad de negocio ha evolucionado en las últimas décadas debido a factores como la dependencia creciente de la tecnología, la interdependencia de los proveedores, la competencia y velocidad de los mercados, así como el incremento regulatorio; y ha dado paso al desarrollo de múltiples metodologías y procedimientos. No obstante, la idea básica se ha mantenido: la continuidad de negocio proporciona a las organizaciones la resiliencia necesaria ante aquellos factores que puedan interrumpir la actividad de negocio. Esta definición es genérica ya que deben considerarse distintos elementos en función de la naturaleza del negocio, su objetivo y apetito al riesgo. Por estos motivos iniciamos la guía con una breve descripción de los conceptos esenciales que deben tenerse en cuenta en todo proyecto de continuidad de negocio.

3.2 ¿Qué es la "continuidad del negocio"?

De forma sencilla, se podría definir **continuidad de negocio** como la **capacidad o el nivel de preparación de una organización para mantener sus funciones esenciales tras producirse un evento que interrumpe total o parcialmente su actividad**, es decir, tras producirse un incidente que puede llegar a parar la actividad de negocio.

Existen distintos tipos de circunstancias que pueden suceder y afectan a la continuidad del negocio con independencia del tamaño de la organización o la tipología de negocio. Estos eventos pueden incluir, por ejemplo: desastres naturales, cortes de energía, avería de los equipos, la indisponibilidad de un proveedor o la salida repentina de una persona clave en la organización.

Así, para garantizar la continuidad del negocio es necesario que la organización elabore un plan, el Plan de Continuidad de Negocio, en el que se describan las actividades que debe llevar a cabo para mantener la disponibilidad de su actividad de negocio esencial ante incidentes que puedan ocasionar su interrupción.

3.3 ¿Qué es un plan de recuperación ante desastres?

En líneas generales se puede definir un **Plan de Recuperación ante Desastres** (en adelante, también, "PRD")[4] como el **conjunto de acciones que es preciso realizar para restablecer el funcionamiento de los sistemas (tecnologías de la información o herramientas digitales) que soportan las funciones críticas del negocio de una organización en el caso de producirse un incidente o desastre.**

3.4 ¿Cuál es la diferencia entre un Plan de Continuidad de Negocio y un Plan de Recuperación ante Desastres?

A simple vista puede parecer que estos dos términos son similares, sin embargo, existe una diferenciación clara en cuanto al alcance y finalidad de cada uno de ellos.

Así pues, un PCN es un plan amplio cuya finalidad es describir el funcionamiento de una organización ante cualquier circunstancia que pueda interrumpir su actividad de negocio, incluido un desastre que afecte la tecnología y sistemas de la organización; y un PRD se centra únicamente en la recuperación de las tecnologías y sistemas de información, por lo tanto, un PCN completo siempre incluirá un PRD y un PRD nunca garantizará la continuidad de toda la actividad de negocio, únicamente la de su tecnología y sistemas críticos.

Si una organización se plantea implementar un PCN lo que está buscando es establecer un proceso que le permita seguir funcionando cuando un incidente anule o impida la operativa de uno o varios de los elementos de negocio (personas, sistemas de información, infraestructuras, ubicaciones y/o proveedores) esenciales para el desarrollo de su actividad crítica (por ejemplo: la desaparición de una persona con todo el conocimiento asociado a un servicio crítico podría parar dicho proceso si dicho conocimiento no se encuentra en otro lugar o está compartido con otras personas).

Por otro lado, si una organización pretende llevar a cabo un PRD su objetivo está centrado en garantizar que los sistemas de información y los datos pueden recuperarse y volver al estado en el que se encontraban antes de la materialización del incidente o desastre.

En resumen, si la mayor preocupación de la organización está asociada con el fallo o caída de las tecnologías y sistemas de información debido a un incidente, ésta deberá

[4] Plan de Recuperación ante Desastres (PRD), en inglés: "Disaster Recovery Plan" (DRP).

empezar por la elaboración de un PRD; si, además, le preocupa la continuidad del negocio en caso de que otros elementos (personas, infraestructura, ubicación o proveedores) fallen, la organización deberá abordar un PCN.

3.5 ¿Cuál es la necesidad y el valor de un Plan de Continuidad de Negocio?

Incidencias, interrupciones, ataques cibernéticos... son situaciones inesperadas que toda organización puede experimentar en cualquier momento, por lo que disponer de un PCN que le permita estar preparada y responder ante este tipo de eventos es una herramienta vital para prevenir o minimizar las pérdidas económicas, materiales e, incluso, humanas que puedan derivarse.

Cada año son más las organizaciones que sufren incidentes que afectan de forma directa o indirecta su actividad de negocio esencial y esta tendencia está en incremento. Esto nos muestra que aquellas organizaciones que han realizado un trabajo previo en materia de continuidad de negocio tienen mayores probabilidades de lograr recuperarse de un incidente e, incluso, de evitar daños, pérdidas y sanciones que pueden llegar a suponer la quiebra y cese de negocio.

La adopción de una estrategia de continuidad de negocio por parte de una organización constituye un ejercicio de responsabilidad corporativa que le permite la anticipación frente a eventos adversos como incidencias, interrupciones o ataques cibernéticos y la protección de su actividad de negocio. Algunas de las ventajas de disponer de un PCN, incluyen:

- Apoyo a la estrategia de la organización al incrementar el control y la protección de la actividad esencial del negocio.
- Gestión preventiva de los riesgos que permite un control más eficiente y efectivo para abordar las situaciones adversas.
- Prevención o minimización de las pérdidas ocasionadas por un incidente. En el caso de materializarse un desastre, la organización estaría preparada para una vuelta a la normalidad de forma controlada, ordenada y en un tiempo menor, por tanto, se reducirían las pérdidas asociadas con el incidente.
- Reducción de las sanciones por parte de los órganos reguladores en caso de incidente debido a una mejora en la debida diligencia (por ejemplo: sanciones

derivadas del incumplimiento con las regulaciones asociadas con los datos personales).

- Mayor resiliencia frente a situaciones adversas que puedan interrumpir la actividad de negocio.

- Mejora de la confianza, credibilidad e imagen reputacional delante de clientes o inversores ya que la organización ofrece mayores garantías en la continuidad de su actividad, productos y/o servicios proporcionados.

- Ventaja competitiva frente a otras organizaciones del mismo sector.

3.6 ¿Cuál es el valor que aporta un Plan de Continuidad de Negocio?

Invertir tiempo y recursos en un PCN permite a la organización incorporar un proceso continuo para la identificación de las personas, activos y recursos (sean éstos, infraestructuras y ubicaciones, sistemas de información y/o proveedores) que resultan imprescindibles para producir los productos y/o servicios de su organización, así como implementar medidas y procesos que permitan mitigar los riesgos de esos activos.

3.7 Caso práctico utilizado

Con el fin de dotar de un enfoque práctico, tomaremos como ejemplo una empresa familiar ficticia que llamaremos "ACME, S.A.".

ACME, S.A. es una empresa familiar de segunda generación fabricante de distintos tipos de calzado. Se encuentra ubicada en dos centros de trabajo: un edificio de oficinas en la ciudad de Madrid y una nave industrial con la fábrica y el almacén de productos situada en Coslada. La empresa cuenta con 40 empleados: 7 en la oficina de Madrid y 33 en la nave de Coslada. Para la fabricación de los productos, ACME, S.A. cuenta con dos proveedores para la materia prima: "Suelas, S.A." y "Tejidos y Hormas, S.A.".

4 MARCO DE ACCIÓN

Un Plan de Continuidad de Negocio se compone de varios procedimientos y documentos dirigidos a establecer, ejecutar, contrastar y mejorar la continuidad de negocio dentro de una organización. Esta guía muestra la actividad básica necesaria para que la organización sea capaz de identificar las principales amenazas a su actividad, el impacto que tendría su ocurrencia sobre el negocio y desarrollar una capacidad de respuesta para mantener un nivel aceptable de actividad tras la materialización de un desastre.

4.1 Apoyo de la Dirección

En el contexto actual de constante cambio y evolución en el que las organizaciones deben ser ágiles, flexibles, adaptarse e innovar para garantizar su pervivencia, el apoyo de la Dirección es un factor clave en todo proceso de cambio, incluido el de un Plan de Continuidad de Negocio, ya que es esencial para lograr involucrar y sensibilizar a las personas de la organización, así como para garantizar la asignación de los recursos necesarios para la implementación y mantenimiento del PCN. Para conseguir este objetivo es necesaria una comunicación efectiva y la concienciación de las posiciones ejecutivas y órganos de decisión internos ya que, solamente cuando entiendan la finalidad del PCN y el valor que aporta a la organización, serán las figuras clave para impulsar, promover y apoyar las actividades necesarias para el éxito del plan. Por tanto, es imprescindible obtener el respaldo, la implicación, y el liderazgo de la Dirección de la organización antes de comenzar el proceso de implantación de un PCN.

Ejemplo

> El responsable de producción de ACME, S.A. ha vivido durante el último año dos situaciones que han estado a punto de detener la producción: problemas de su principal proveedor de material causaron grandes retrasos en la recepción de lotes y una caída de los sistemas de información les impidió disponer de la planificación de la producción durante algunos días.

Siendo consciente de estos riesgos y de que ACME, S.A. estuvo muy cerca de interrumpir la actividad de la empresa, el responsable de producción plantea a la Dirección buscar alternativas para definir cómo actuar si otra circunstancia vuelve a amenazar la producción.

La Dirección de ACME, S.A. decide crear un Plan de Continuidad de Negocio para el proceso de producción de su calzado. Las estrategias de recuperación que se contemplan van a afectar tanto al principal proveedor de material de la empresa como a sus sistemas de información y recuperación de datos.

Cuestionario

¿Se ha conseguido el compromiso de la Dirección para el diseño e implementación del PCN?

SÍ **NO**

4.2 Cultura organizacional

Otro elemento que cualquier organización debe tener en cuenta es que la implementación de un PCN implica incorporar en la cultura organizacional los conceptos y el contenido del PCN. Esto se traduce en que, además de la aprobación formal del PCN, es necesaria la formación y concienciación de las personas que participan en el desarrollo de la actividad de negocio, así como la implementación de una serie de medidas organizativas que permitan que los procesos y controles del PCN se apliquen de forma efectiva sobre los procesos y activos de la organización.

Ejemplo

ACME, S.A., dentro de su PCN, creó un documento para gestionar incidentes. Si bien este documento de gestión de incidentes se aprobó en su momento,

- no se ha actualizado su contenido (en particular, las personas que integran el Comité de Crisis),
- no se han ejecutado los planes de concienciación y de pruebas previstos en el PCN,

- se han aprobado nuevas políticas internas que incluyen gestión de brechas de seguridad de protección de datos e incidentes de seguridad de la información y no han sido consideradas.

Con estos antecedentes, surge un incidente y la empresa detecta que:

- figura la identidad y los datos de contacto del anterior Director de Comunicación y no aparecen los de la actual,
- la actual Director de Comunicación desconoce sus funciones como miembro del Comité de Crisis.
- la gestión del incidente en el PCN, además, no concuerda con la gestión de brechas de seguridad de protección de datos e incidentes de seguridad de la información.

Cuestionario

¿Existen políticas internas en la Organización?

SÍ **NO**

¿Existe un plan de concienciación en materia de seguridad o que incluya aspectos asociados con la continuidad de negocio?

SÍ **NO**

¿Existe un Plan de Recuperación ante Desastres?

SÍ **NO**

¿Existe un plan de pruebas y se cumple?

SÍ **NO**

¿Existe una definición formalizada de roles y responsabilidades dentro de la Organización?

SÍ **NO**

4.3 Alcance del Plan de Continuidad de Negocio

Al desarrollar por primera vez un PCN para la organización es aconsejable seleccionar qué actividades, productos y/o servicios son más críticos, como una forma de acotar

el trabajo y priorizar los esfuerzos. Posteriormente, cuando la organización ya tenga experiencia en la elaboración del PCN, el alcance se podrá ir ampliando progresivamente añadiendo actividades, productos y/o servicios.

Para definir el alcance la organización deberá listar los procesos de negocio a alto nivel (por ejemplo: producción, distribución, compras…) y seleccionar aquellos cuya interrupción pueda acarrear un mayor impacto en el negocio.

En aquellas organizaciones que no dispongan de una definición y listado de los procesos de negocio, para determinar el alcance puede ser útil pensar en aquellas actividades, productos y/o servicios que, en caso de dejar de proveerse, implicarían pérdidas o daños para la organización por ser los que proporcionan mayor beneficio al negocio, los que son más valorados por los clientes, los que representan más a la marca, forman parte de un requerimiento contractual o legal, entre otros.

4.4 Cómo elaborar un análisis de impacto

El siguiente paso para desarrollar un PCN es la elaboración de un análisis de impacto en el negocio (BIA) . Para elaborar este análisis, la organización debe conocer y documentar cuáles son las actividades que se realizan en su negocio que, o bien no admiten interrupciones, o bien tienen una tolerancia muy baja a estas. Así, en la elaboración del BIA se documentará para estas actividades consideradas esenciales, cuál es el impacto que tendría para la organización la interrupción de dicha actividad durante distintos intervalos de tiempo considerando las personas, sistemas y tecnologías de información, infraestructuras, ubicaciones y proveedores imprescindibles para su ejecución, esto es, identificando los recursos críticos de la actividad de negocio.

La realización de este ejercicio permitirá a la organización priorizar las actividades para la aplicación de la continuidad de negocio.

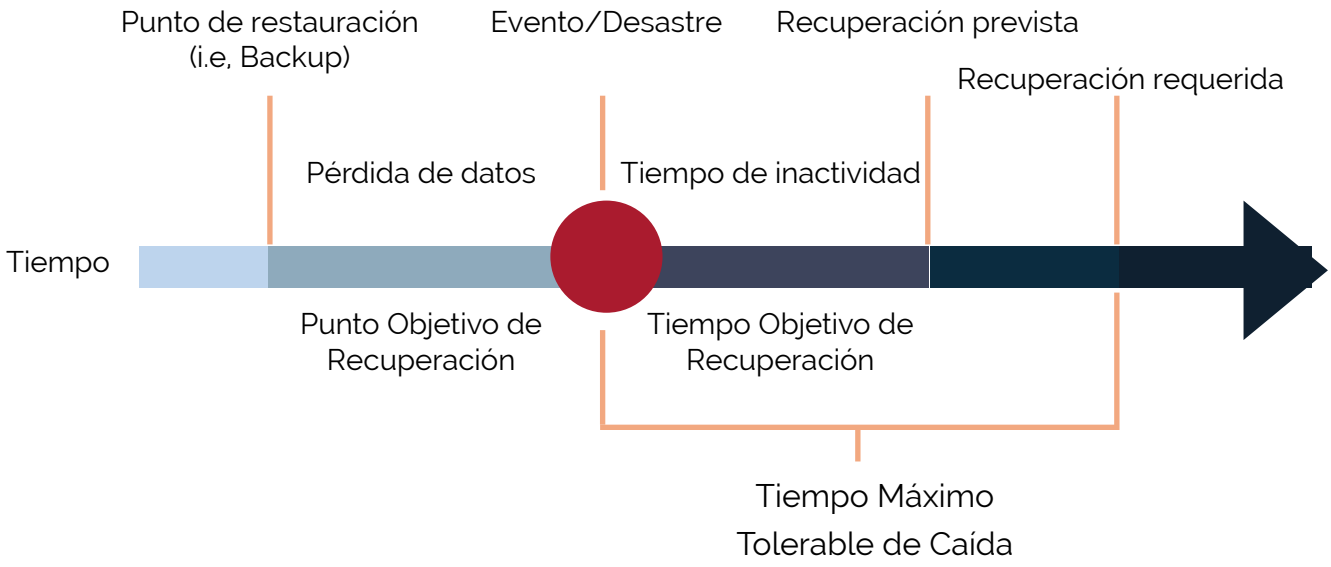
Para poder realizar esta medición es necesario tener claros tres conceptos básicos:

- Tiempo Objetivo de Recuperación (RTO)[6] : Tiempo de recuperación de las actividades bajo unas condiciones mínimas.

- Punto Objetivo de Recuperación (RPO)[7]: Cuanta información podemos perder o de cuanto tiempo atrás necesitamos recuperar.

[5] Análisis de Impacto al Negocio, en inglés: "Business Impact Assessment" (BIA).
[6]. Tiempo Objetivo de Recuperación, en inglés: "Recovery Time Objective" (o "RTO").
[7] Punto Objetivo de Recuperación, en inglés: "Recovery Point Objective" (o "RPO").

- Tiempo Máximo Tolerable de Caída (MTD)[8]: Cuanto tiempo puede estar caído un proceso antes de que produzca efectos desastrosos para la organización.



Ejemplo

BIA de ACME, S.A. para el proceso de recepción y descarga de material:

Tiempo de interrupción	Impacto[9]
Hasta 8h	No hay impacto porque el stock disponible en almacén garantiza la producción de todos los modelos por 4 días.
8 a 48h	No hay impacto porque el stock disponible en almacén garantiza la producción de todos los modelos por 4 días.
48h a 1 semana	Impacto medio: debería detenerse la producción de algunos modelos, manteniendo la actividad de la fábrica solo con aquellos modelos para los que quede stock. El problema no sería percibido por clientes porque la distribución se hace de forma semanal.
1 semana a 1 mes	Impacto alto: debería detenerse la actividad de la fábrica por falta de materia prima. Habría retrasos en la entrega de material a clientes, posible incumplimiento de contratos.

[8] Tiempo Máximo Tolerable de Caída, en inglés: "Maximum Tolerable Downtime" (o "MTD").
[9] Los intervalos de tiempo de interrupción y los niveles de impacto deben ser definidos por cada organización, de acuerdo con las particularidades de su actividad.

Recursos necesarios:

Recursos	Detalle	Comentarios
Personas	1 Persona de almacén 1 Responsable de logística	Lu a Vie, de 8 a 15h. Almacén (Coslada) Lu a Vie, de 8 a 15h. Oficinas (Madrid)
Proveedor	Pieles S.A. Tejidos y Hormas, S.A.	Entregas c/2 días Entregas c/15 días
Ubicación	Almacén	Coslada
Sistemas	Correo electrónico	Para comunicación con proveedores

Tras analizar el impacto que tendría para la organización la interrupción de las actividades definidas en el alcance, podrá identificarse para cada una cuál es el tiempo de interrupción que causaría un impacto alto (o no asumible) para la organización. En este sentido es recomendable tener en cuenta el tiempo y cómo la organización, con las personas y recursos disponibles, sería capaz de recuperar las operaciones para:

- Ordenar las actividades de más a menos críticas (aquellas que, con interrupciones cortas tienen impactos altos, son más críticas y deberán ser abordadas en primer lugar).

- Disponer de una referencia de tiempo para planificar cuán rápida debe ser la respuesta que se documente en el PCN.

4.5 Definición de escenarios y ejemplos prácticos

Una vez identificados los recursos críticos de la actividad del negocio, se deberá identificar y definir cómo se recuperará la disponibilidad de la actividad o servicio en función del recurso crítico que falte, esto es, se deberán definir los escenarios asociados a la ausencia o indisponibilidad de cada recurso crítico y/o de un conjunto de estos.

Para la definición de los escenarios se pueden utilizar una o más estrategias de las defi-

nidas en el siguiente apartado (ver apartado 4.6 Estrategias de continuidad de negocio). Es posible que sea necesario cubrir escenarios adicionales, para lo que será necesario estudiar e identificar las estrategias en las que estos se soportan.

En el 6.1 Cuestionario de autoevaluación se recoge un cuestionario de estrategia cuya finalidad es ayudar a las organizaciones a identificar los escenarios que pueden ser más convenientes de abordar en el PCN.

Escenario 1: Indisponibilidad de personas.

La plantilla de ACME, S.A. está compuesta por 26 personas repartidas en 7 departamentos. Todos esos departamentos serían bloqueantes para la producción en distintas franjas temporales. Un contagio de algún agente infeccioso, un accidente de un vehículo que compartan varias personas o una intoxicación alimentaria en una cena de equipo son ejemplos de casos en los que alguno o todos los departamentos podrían quedarse durante un tiempo sin profesionales que ejecuten las tareas y que, por tanto, podría hacer que se parase la producción.

Escenario 2: Indisponibilidad de sistemas de información.

Además de los propios sistemas operativos de los ordenadores que ACME, S.A utiliza para la producción de calzado, existen 8 aplicaciones específicas para los distintos procesos que la empresa ejecuta. Entre los ejemplos que podrían poner en riesgo estos sistemas se encontrarían: ataques informáticos, errores de configuración u obsolescencia de los equipos.

Escenario 3: Indisponibilidad de ubicación de negocio.

El almacén de Coslada es una nave anexa a la fábrica y se encuentra en un polígono industrial. Las principales amenazas que podrían inhabilitar la ubicación serían una inundación (por fenómeno meteorológico o rotura de canalizaciones, propias o de vecinos), un incendio (en la propia instalación o vecinas) o la interrupción de la única vía de acceso por carretera (por fenómenos meteorológicos o accidente de tráfico). Todas estas amenazas producen el mismo efecto: la indisponibilidad de la ubicación, por este motivo se agrega en un escenario.

Escenario 4: Indisponibilidad de proveedores.

ACME, S.A. cuenta con una serie de proveedores de distintos productos materiales y servicios (telas, suelas, cordones o diversos químicos…). El cese de la prestación de servicios por parte de uno o varios proveedores podría originar que la organización tuviese que parar su producción al existir una alta dependencia de terceros para su objeto de negocio.

4.6 Estrategias de continuidad de negocio

La estrategia de continuidad de negocio de las organizaciones se basa en el aseguramiento de la continuidad de los activos o recursos que dan soporte al negocio. Si bien se pueden desarrollar estrategias basadas en escenarios de riesgo, un buen punto de partida para las organizaciones sería dotarse de estrategias que cubran las indisponibilidades de las personas, la información y los sistemas que utilizan, las instalaciones donde se encuentran, así como los proveedores cuyo cese de actividad pondría en riesgo la organización.

A continuación, se plantean cuatro de las estrategias a alto nivel más comunes para una organización.

- Estrategia 1 Personas

Objetivo: asegurar que aquellas actividades internas que, en caso de no poder realizarse, podrían parar una organización se puedan realizar en ausencia de las personas que las realizan habitualmente.

Posibles estrategias o alternativas: definir personal de reemplazo dentro del mismo departamento; buscar personal en otro departamento con el conocimiento necesario para cubrir la posición requerida; buscar un proveedor que pueda asumir la realización de la actividad hasta que la persona vuelva a estar disponible (por ejemplo: el pago de nóminas, impuestos, etc.) o contratar personal externo para cubrir la posición.

- Estrategia 2 Sistemas de información

Objetivo: Cubrir la indisponibilidad de la información y los sistemas que le dan soporte como hardware y software a nivel de puesto de usuario, servidores de ficheros, teléfonos, ordenadores o impresoras. En primera instancia, lo más inmediato es asegurar la disponibilidad de la información en formato físico y los sistemas de usuario.

Posibles estrategias o alternativas: ante la indisponibilidad de sistemas de información pueden ser priorizar el uso de los terminales y/o equipos que funcionen para las personas que desarrollan actividades críticas o tener un stock de equipos de reserva disponibles.

- Estrategia 3 Infraestructura física / Ubicación

Objetivo: dar solución a aquellos escenarios en los que no se pueden utilizar las ubicaciones y/o instalaciones habituales debido a incendios, inundaciones, protestas/manifestaciones, fallos eléctricos, etc.

Posibles estrategias o alternativas: trabajar en remoto para aquellas actividades que lo permitan, trasladar la actividad a otras instalaciones de la organización (local, oficina o almacén en otra dirección o ubicación geográfica) o alquilar un espacio temporal (espacios compartidos, oficina o almacén) para mantener la actividad más esencial.

- Estrategia 4 Proveedores

Objetivo: definir el modo de actuar ante una eventual indisponibilidad de algún proveedor que proporcione productos y/o servicios cuya ausencia bloquee la actividad de la organización.

Posibles estrategias o alternativas: si se cuenta con proveedores diversificados, derivar las tareas a otro proveedor, provisión del servicio y/o producto del primero, activar a un proveedor alternativo ya identificado y contactado previamente (quizás con precios ya acordados) o buscar alternativas en el mercado.

4.7 Plan de pruebas

Para garantizar que el Plan de Continuidad de Negocio esté actualizado y evitar errores o problemas cuando sea necesaria su activación, es necesario que se pruebe periódicamente. Con esta finalidad se seleccionarán los distintos escenarios para los que se ejecutarán las estrategias definidas y se simulará de forma teórica o práctica la interrupción de la actividad de negocio del escenario en particular.

El resultado de las pruebas del PCN debe ser un informe que recoja los resultados de estas, las debilidades encontradas, con las lecciones aprendidas y las acciones que habría que realizar sobre las estrategias definidas para poder así conseguir corregir errores

y una mejora continua. Una vez corregidas las debilidades, se incorporarán los cambios a las estrategias para poder ser utilizadas en una contingencia real o ser probadas de nuevo en el siguiente ciclo de pruebas.

Ejemplo:

Para evitar volver a encontrase en una situación crítica con un PCN obsoleto, la Dirección de ACME, S.A., además de impulsar su revisión y actualización anual del PCN, decide implementar un Plan de Pruebas en el que se simularán aquellos escenarios que más le preocupan y hacer seguimiento de los resultados de las pruebas para corregir los errores detectados. Con ello, establece un calendario de pruebas mediante el cual establece fechas de compromiso aproximadas de las pruebas que quiere realizar priorizando, dado que ya se ha encontrado en alguna ocasión con problemas en su cadena de suministro, las tareas en dicha área.

En el Plan de pruebas participarán tanto ACME, S.A., como sus principales proveedores Suelas, S.A. y Hormas y Tejidos, S.A. y se discutirán todas las medidas que cada una realizaría en función de sus estrategias. Por un lado, los proveedores deberán exponer las medidas preventivas y reactivas que impedirían o minimizarían el cese temporal en la prestación de su servicio y por otro lado la propia ACME, S.A. deberá exponer las acciones que llevaría a cabo en el caso en que las anteriores no fuesen suficientemente efectivas.

Como conclusión de prueba de este ejemplo, ACME, S.A. concluye que su estrategia de proveedores no era la más adecuada y decide modificar su estrategia repartiendo la carga de trabajo entre dos proveedores de modo que uno de ellos pueda asumir la carga del otro si fuese necesario.

4.8 Plan de comunicación

En función del tipo de escenario que se presente, es posible que el colectivo susceptible de ser informado sea distinto, así como el tipo de mensaje a trasladar. Por este motivo, es necesario que se desarrolle un Plan de Comunicación que defina qué, quién, cómo y a quién comunicar en cada caso. Para este plan se deberá tener en cuenta las comunicaciones a: personal interno, comunicación externa a autoridades, partes interesadas, medios, etc.

Ejemplo:

La prueba o simulacro realizado en el ejemplo anterior, también dejó al descubierto que ACME, S.A. no había determinado quién tendría que estar contactando con el personal interno, en caso de un fallo del proveedor que parase la producción. Tampoco estaba nada claro a través de qué medio se debería contactar con el personal, cuál debería ser el tono de la comunicación ni qué tipo de mensajes deberían estar publicándose en redes sociales y medios de comunicación.

En el Plan de Comunicación de ACME, S.A. ahora figura una tabla con la siguiente información:

- Tipo de comunicación: Interna o externa
- Responsable de la comunicación.
- Mecanismo o medio para realizar la comunicación: email, portal interno, mensajería instantánea.
- Listado de receptores.

Además, ACME, S.A. ha establecido una serie de plantillas o mensajes tipo que cubren unos determinados escenarios, de modo que en caso de producirse cualquier incidente que ponga en riesgo la producción van a poder basarse en alguna de esas plantillas para desarrollar la comunicación adecuada de una forma ágil y rápida.

5 CONCLUSIONES

Actualmente, uno de los mayores riesgos en las organizaciones es la ausencia de preparación ante eventos que puedan ocasionar la disrupción de la actividad de negocio, así como la carencia de un Plan de Continuidad de Negocio.

La creación de un PCN puede parecer una tarea complicada, pero con unas líneas claras y un alcance acotado a las necesidades y medios disponibles de cada organización puede ser asumible y su consecución no sólo es una ventaja competitiva, sino que ayudará a evitar o minimizar las pérdidas y sanciones en caso de que se produzca un incidente que ponga en riesgo la continuidad del negocio.

En esta guía hemos visto la importancia de contar con un claro apoyo de la Dirección de la organización para poder realizar un cambio cultural real sobre la percepción de los riesgos asociados con la continuidad de negocio. Asimismo, se ha recomendado empezar un PCN con un alcance razonable y asumible que permita a la organización realizar con mayor facilidad una de las fases del PCN más complicadas, el Análisis de Impacto al Negocio.

Para simplificar y ayudar en el diseño del PCN, se han incluido unos cuestionarios de autoevaluación con los que la organización podrá focalizar sus esfuerzos iniciales y se han presentado unos escenarios agregados y sencillos que pueden ser aplicados tanto si la prioridad de la organización es la continuidad de las personas, la tecnología, la infraestructura y/o los proveedores y que permiten definir una estrategia de continuidad de negocio preparada ante eventos disruptivos que pudieran ocasionar pérdidas o provocar el cierre de la organización.

Con lo anterior, en la guía se ha remarcado la importancia del Plan de Pruebas y la actualización del PCN para evitar que acabe convirtiéndose en un documento obsoleto sin valor en el momento en que se produce un incidente.

Finalmente, se ha recordado tener en cuenta el Plan de Comunicación asociado con los incidentes ya que un excelente PCN sin una correcta comunicación puede ser inefectivo y también puede causar pérdidas o dañar la imagen de una organización.

6 ANEXOS

6.1 Cuestionario de autoevaluación

Esta prueba de autoevaluación está diseñada para ayudar a identificar la situación actual de la organización frente a la gestión del Plan de Continuidad de Negocio.

Una primera recomendación es que se realice esta prueba en diferentes momentos del proceso de implantación del PCN ya que puede servir para determinar cuál es el estado inicial y su evolución. Así, se recomienda realizar la prueba, al menos, en tres ocasiones:

- Previo al PCN: con este análisis se identifica el punto de partida y, comparándolo con el análisis final, se atestigua la mejora.
- Durante el desarrollo del PCN: la evaluación de seguimiento es muy importante para informar del progreso y servir como elemento motivador durante el desarrollo del PCN.
- Al final del PCN: esta última evaluación permite comprobar hasta qué punto se han alcanzado los objetivos fijados al inicio del PCN.

6.1.1 Cómo realizar el cuestionario

Se proporcionan algunas recomendaciones para la realización del cuestionario:

- En el momento de seleccionar una opción, se recomienda elegir la que describa la realidad, situación o estado de la organización de la forma más objetiva posible.
- Para obtener un resultado completo es necesario responder a todas las cuestiones que se plantean en los distintos apartados.
- Cada elección realizada está asociada a un valor. Deben sumarse todos los

valores.

- El resultado de esta suma servirá para identificar el nivel de madurez de la organización en el momento de la realización del cuestionario.

- Los valores más bajos muestran donde es necesario focalizar los esfuerzos durante la implantación del PCN.

6.1.2 Cuestionario de autoevaluación

- Las siguientes 10 preguntas le permitirán identificar cuál es su nivel de madurez en la gestión de la continuidad de negocio en la organización.

ORGANIZATIVAS						
NIVELES	**1**	**2**	**3**	**4**	**5**	**PUNTUACIÓN**
Riesgos asociados a la organización	Desconozco los riesgos de mi organización 1	Tengo identificados algunos de los riesgos 2	Tengo identificados todos los riesgos, pero no se gestionan 3	Tengo identificados todos los riesgos, se gestionan y se aplican medidas de control 4	Tengo identificados todos los riesgos, se gestionan, se aplican medidas de control y se realizan actividades de seguimiento 5	
Recursos para la gestión de riesgos	Desconozco si tengo asignados recursos 1	No existe una asignación de recursos 2	Tengo capacidad para asignar personas, recursos técnicos y económicos cuando se producen los incidentes 3	Tengo asignadas personas, recursos técnicos y económicos de forma planificada, pero únicamente en las áreas técnicas o de TI 4	Tengo asignadas personas, recursos técnicos y económicos de forma planificada y supervisados por la Dirección 5	
Auditorías y revisiones	Desconozco si realizo algún tipo de auditoría 1	No realizo ningún tipo de auditoría 2	Dispongo de un plan de auditoría 3	Dispongo de un proceso de auditoría y un plan de acciones correctivas 4	Dispongo de un proceso de auditoría y un plan de acciones correctivas supervisados por Dirección 5	
Plan de actuación en caso de desastres	Desconozco si dispongo de un plan 1	No dispongo de un plan 2	Dispongo de un plan de actuación, pero no revisado ni actualizado 3	Dispongo de un plan actuación y se mantiene y actualiza desde el área técnica o de TI 4	Dispongo de un plan actuación, se mantiene y actualiza desde el área técnica o de TI y supervisado por Dirección 5	
Tiempo que puedo permanecer sin actividad	Desconozco los tiempos que la organización puede permanecer sin actividad 1	Tengo identificados algunos tiempos 2	Tengo identificados todos tiempos, pero no se gestionan. 3	Tengo identificados todos los tiempos, se gestionan y se aplican medidas de compensación en caso de incidente 4	Tengo identificados todos los tiempos, se gestionan, se aplican medidas de compensación en caso de incidente y se prueban 5	

PERSONAS						
NIVELES	**1**	**2**	**3**	**4**	**5**	**PUNTUACIÓN**
Formación del personal	Desconozco si el personal tiene formación 1	El personal no está formado 2	El personal dispone de formación no específica 3	El personal dispone de la formación específica para actuar en caso de desastre 4	El personal dispone de la formación continua específica para actuar en caso de desastre 5	
Personal prioritario o que realice tareas críticas del negocio	Desconozco si tengo personal prioritario o que realice tareas críticas del negocio 1	No tengo identificado al personal prioritario o que realiza tareas críticas del negocio 2	Tengo identificado al personal prioritario y no tengo personal alternativo ni documentada su actividad 3	Tengo identificado al personal prioritario y documentado sus actividades, pero no tengo personal alternativo 4	Tengo identificado al personal prioritario y personal alternativo con sus actividades documentadas 5	
PROVEDORES						
NIVELES	**1**	**2**	**3**	**4**	**5**	**PUNTUACIÓN**
Proveedores críticos	Desconozco sí tengo proveedores críticos 1	No tengo identificados a mis proveedores críticos 2	Tengo identificados a mis proveedores críticos, pero no tengo definido el plan de acción en caso de su indisponibilidad 3	Tengo identificados a mis proveedores críticos y definido el plan de acción en caso de su indisponibilidad 4	Tengo identificados a mis proveedores críticos, definido el plan de acción y supervisado por Dirección 5	
INFRAESTRUCTURA						
NIVELES	**1**	**2**	**3**	**4**	**5**	**PUNTUACIÓN**
Centro de trabajo	Desconozco si pudiera necesitar un centro alternativo en caso de incidente 1	No tengo un centro alternativo en caso de incidente 2	Tengo identificada la necesidad de un centro alternativo, pero no la he valorado 3	Tengo evaluadas alternativas para reemplazar el centro de trabajo en caso de que sea necesario 4	Tengo evaluadas alternativas para reemplazar el centro de trabajo y podría ponerlas en práctica 5	
TECNOLOGÍA						
NIVELES	**1**	**2**	**3**	**4**	**5**	**PUNTUACIÓN**
Medidas de recuperación tecnológicas	Desconozco si dispongo de medidas 1	No dispongo de medidas 2	Dispongo de medidas, pero no se revisan o actualizan 3	Dispongo de medidas de recuperación, se mantienen y actualizan 4	Dispongo de medidas, se mantienen, actualizan desde el área técnica y supervisan por Dirección 5	
PUNTUACIÓN FINAL						

6.1.3 Interpretación del resultado

Tal y como se ha indicado anteriormente, con la suma de las puntuaciones obtenidas, en la siguiente tabla, debe buscarse el nivel de madurez correspondiente al valor obtenido.

Nivel de madurez	Resultado	Descripción
Optimizado	**50**	Lo primero que tenemos que hacer es felicitarlo. Bajo nuestros parámetros, dispone de un sistema de gestión de continuidad de negocio que le permite responder ante cualquier incidente o desastre. Si es que no la tiene ya, le animamos a implantar la ISO 22301 "Sistema de Gestión de la Continuidad de Negocio" que, como norma certificable, le permitirá aumentar su prestigio ante clientes o terceros.
Gestionado y medible	**de 40 a 49**	Su Organización tiene establecido un conjunto de medidas que están alineadas con los requisitos que definen un Plan de Continuidad de Negocio. Utilice esta guía para revisar su sistema de gestión de la continuidad de negocio, le ayudará a optimizar la gestión del riesgo y estará preparado para responder adecuadamente ante un incidente o un desastre.
Procesos definidos	**de 30 a 39**	Su Organización tiene conciencia sobre la importancia de la gestión de riesgos y existen medidas implantadas, sin embargo, su capacidad de respuesta ante desastres se puede ver limitada por una planificación poco organizada. Está muy cerca de completar un Plan de Continuidad de Negocio, siguiendo los pasos establecidos en esta Guía podrá adaptar y completar las medidas necesarias para su implantación.
Procesos intuitivos	**de 20 a 29**	Su Organización tiene predisposición para la gestión de riesgos, incluso puede tener implantadas algunas medidas, pero el éxito o el fracaso ante un incidente o desastre dependerá del azar más que de una actuación organizada y estructurada. Depender de la suerte o de otros factores aleatorios no es la mejor manera para enfrentarse a los riesgos. Por ello, le animamos a implantar un Plan de Continuidad de Negocio como el que le proponemos en esta Guía.
Inicial	**de 10 a 19**	Su Organización está totalmente indefensa ante incidentes o desastres y es muy probable que sufra graves daños o interrupciones que paralicen su funcionamiento si estos se materializan. Es imprescindible que realice, al menos, un análisis de los riesgos que amenazan a su Organización y recomendamos enérgicamente la implantación de un Plan de Continuidad de Negocio como el que le proponemos en esta Guía.

6.2 Cuestionarios de estrategia

A lo largo de esta guía se han visto los aspectos fundamentales de un Plan de Continuidad de Negocio. A través de cuatro escenarios, habituales en una PYME, se han procedido a analizar y proporcionar un conjunto de buenas prácticas que faciliten la implementación de un PCN. Hasta este apartado, se ha proporcionado la información necesaria para enfrentarse a la elaboración de un PCN. Como es posible que para una parte de los lectores de esta guía sea la primera vez que se aborda la elaboración de un PCN se quiere, también, ayudar al diseño del mismo. Para lograrlo, se han desarrollado unos cuestionarios que permitirán identificar cuál de los cuatro escenarios planteados es el más adecuado para comenzar con la implantación del plan.

6.2.1 Cómo realizar el cuestionario

El presente cuestionario debe ser visto como una herramienta de soporte para la identificación del escenario más apropiado sobre el que realizar un PCN en una organización.

Está estructurado en cuatro apartados (uno por cada escenario) y una valoración final de resultados. Cada apartado consta de 5 preguntas que ayudarán a reflexionar sobre los puntos más relevantes de cada escenario.

Recomendaciones previas para la realización eficaz del cuestionario:

- A la hora de seleccionar una opción, se debe elegir la que mejor describa la realidad, la situación o el estado de la organización.
- Para obtener un resultado objetivo y completo es necesario responder a todas las cuestiones que se le plantean en todos los apartados.
- Cada elección que se realice tiene asociado un valor. En cada apartado se deberán sumar todos los valores del propio apartado (por ejemplo: "Apartado 1: Personal" se deberán sumar los valores de cada una de las casillas seleccionadas para cada una de las cinco cuestiones que contiene el apartado). El resultado de la suma total del apartado definirá la importancia o el valor del escenario en la organización.
- Una vez finalizados los cuatro apartados y obtenido el valor de cada uno de ellos, debe dirigirse al apartado de valoración de resultados y colocar estos

resultados en las columnas correspondientes.

- Para facilitar la interpretación de estos resultados, se ha incorporado una escala de colores donde se puede valorar cuál de los escenarios es el más adecuado para comenzar la elaboración del PCN.

6.2.2 Apartado 1: Personas

Cuando se plantea la relevancia que tienen las personas dentro de una organización en el ámbito de la continuidad de negocio debe considerarse cómo de críticas o especializadas son las tareas que desempeñan. Un ejemplo de cómo puede afectar esto es lo que le sucedió a un fabricante de vehículos eléctricos.

- Una empresa fundada en el año 2009 como auxiliar del sector automovilístico, en el año 2011 enfocó su negocio hacia los vehículos eléctricos autónomos con la idea de convertirse en el rival más competitivo del mercado. Para alcanzar este objetivo, además de fuertes inversiones y acuerdos estratégicos con grandes corporaciones contrató a más de 100 trabajadores de la empresa rival, incluyendo a personal clave de ingeniería obteniendo conocimiento estratégico.

	Totalmente en desacuerdo	En desacuerdo	Indiferente	De acuerdo	Totalmente de acuerdo
La experiencia es imprescindible para el desempeño de las tareas o actividades	1	2	3	4	5
La especialización es imprescindible para el desempeño de las tareas o actividades	1	2	3	4	5
Los trabajos realizados están asociados a procesos o tareas críticas.	1	2	3	4	5
Los trabajos especializados o críticos están realizados por muy pocas personas.	1	2	3	4	5
Los trabajos no se pueden realizar sin el personal asignado a ellos	1	2	3	4	5

6.2.3 Apartado 2: Tecnología

Se puede afirmar que la tecnología está presente en todos los sectores de actividad y ninguna organización, ya sea en mayor o menor medida, queda al margen de su uso. Aunque nadie niega la afirmación anterior, suele ser motivo de discrepancia la valoración del nivel de concienciación frente a los ataques tecnológicos. Diversos estudios indican que más de la mitad de las PYMEs consideran que su negocio es demasiado pequeño para ser objetivo de estos ataques. La realidad muestra que cualquier organización está expuesta independientemente de su tamaño, por ello se quiere recordar un incidente:

- En 2017, una vulnerabilidad en un sistema operativo fue aprovechada para el primer gran ataque de ransomware de la historia. Más de 300.000 ordenadores en 150 países se vieron afectados, su nombre: WannaCry.

	Totalmente en desacuerdo	En desacuerdo	Indiferente	De acuerdo	Totalmente de acuerdo
La Organización busca innovar y mejorar su capacidad tecnológica siempre que sea posible	1	2	3	4	5
La Organización se bloquearía si no pudiera acceder a la información o utilizar la tecnología	1	2	3	4	5
En caso de siniestro, si no se dispone de copias de seguridad o tengo repuestos de las tecnologías se paralizaría la operativa.	1	2	3	4	5
El personal no dispone de la formación adecuada para el manejo de las tecnologías o programas críticos	1	2	3	4	5
La tecnología o programas carece de planes de mantenimiento o actualización controlados y revisados	1	2	3	4	5

6.2.4 Apartado 3: Infraestructuras

Las infraestructuras son vistas como un elemento fundamental en el desarrollo de la operativa de las organizaciones. Esta importancia es fácilmente identificable en el sector primario, pero a medida que avanzamos hacia otros sectores, esta identificación se vuelve más difícil ya que existen actividades en las que incluso sin instalaciones las organizaciones pueden llevar a cabo su operativa diaria. El ejemplo expuesto a continuación ilustra dos aspectos: por un lado, la importancia de las infraestructuras en una organización del sector servicios y, por otro, la capacidad para reponerse gracias a un Plan de Continuidad de Negocio.

- En 2021, en una de las principales capitales europeas se declaró un incendio en uno de los data centers más grande de Europa, propiedad de uno de los mayores proveedores europeo de servicios en la nube. El fuego, en menos de 8 horas, había destruido completamente un centro de datos, parcialmente otro y dejado sin energía al resto. Como consecuencia de esto, se calcula que alrededor de 3,6 millones de sitios web correspondientes a unos 464.000 dominios quedaron inaccesibles. La organización tardó más de dos semanas en recuperar las operaciones y dejó sin servicio a gobiernos, administraciones públicas y servicios críticos.

	Totalmente en desacuerdo	En desacuerdo	Indiferente	De acuerdo	Totalmente de acuerdo
El centro de trabajo es básico para desarrollar el negocio	1	2	3	4	5
El centro de trabajo es difícilmente reemplazable en caso de siniestro	1	2	3	4	5
El centro de trabajo está expuesto a catástrofes naturales	1	2	3	4	5
Necesitaría mucho tiempo para reemplazar el actual centro de trabajo	1	2	3	4	5
Un accidente, siniestro o desastre natural en las proximidades del centro de trabajo impediría la operativa habitual	1	2	3	4	5

6.2.5 Apartado 4: Proveedores

Un aspecto que muchas veces puede pasar de largo a la hora de identificar dónde aplicar un PCN son los proveedores ya que es habitual considerarlos como factores externos a la organización, incluso colaterales al negocio. Si bien es cierto que, no todas las empresas pueden quedar expuestas a un fallo en la cadena de suministro de sus proveedores, es relevante analizar el grado de dependencia con estos. Mostramos un ejemplo que ayudará a valorar la importancia de los proveedores en la actividad de negocio:

- En el primer semestre del 2021 la economía mundial comenzó a repuntar, después de la crisis provocada por la COVID-19 ya nada hacía pensar al sector de los electrodomésticos que algo microscópico podría ralentizar la esperada recuperación y se encontraron con una crisis de desabastecimiento de microchips al ser un mercado controlado a nivel mundial por un grupo reducido de organizaciones tecnológicas. Con este escenario, el sector de los electrodomésticos se ha visto forzado a reducir o paralizar su producción. Un problema de escasez en la provisión de materia prima.

	Totalmente en desacuerdo	En desacuerdo	Indiferente	De acuerdo	Totalmente de acuerdo
La mayoría de los trabajos o tareas están externalizados	1	2	3	4	5
Los trabajos fundamentales o actividades críticas del negocio están externalizados	1	2	3	4	5
Los trabajos dependen del suministro de los proveedores	1	2	3	4	5
La Organización utiliza muy pocos proveedores.	1	2	3	4	5
Los proveedores alternativos son difíciles de encontrar o son inexistentes	1	2	3	4	5

6.2.6 Apartado 5: Interpretación de los resultados

Con los resultados anteriores, deben completarse las casillas correspondientes con los valores obtenidos para cada escenario.

	Resultados		
Escenarios	**de 5 a 15**	**de 16 a 20**	**de 21 a 25**
Personas			
Proveedores			
Infraestructuras			
Tecnologías			

- **Entre 5 y 15 – Nivel de exposición bajo**, un análisis sencillo e informal de cómo manejar las amenazas daría cobertura a los riesgos que se le pueden presentar. No obstante, desde aquí queremos animar a que se realice un Plan de Continuidad de Negocio.

- **Entre 16 y 20 – Nivel de exposición medio**, la organización está expuesta a unos riesgos que, sin ser probablemente críticos, podrían ocasionar problemas operativos. Recomendamos elaborar un Plan de Continuidad de Negocio.

- **Entre 21 y 25 – Nivel de exposición elevado**, un Plan de Continuidad de Negocio es imprescindible para minimizar el daño potencial al que se encuentra expuesta la organización.

Para interpretar los resultados obtenidos para los escenarios se aconseja seguir las siguientes recomendaciones:

- Elegir el escenario con el nivel de exposición más elevado antes de abordar los escenarios con nivel de exposición inferiores.

- Cuando el nivel de exposición más alto se repite en varios escenarios se sugiere seguir con los siguientes pasos para elegir el escenario más adecuado en la implantación del PCN:

    1. Identificar cuáles son las actividades más críticas del negocio.

    2. Asociar el escenario de mayor dependencia para cada actividad (personas, tecnología, infraestructura o proveedores).

    3. Ordenar este listado en base a la relevancia de cada actividad para la consecución de los objetivos del negocio o la organización.

    4. Elegir el escenario de la actividad que figure como primera en la lista anterior.

6.3 Póliza de Ciberseguridad

Hasta ahora hemos aprendido que para enfrentarnos a las amenazas que puedan producir una interrupción de la actividad del negocio la mejor decisión que podemos tomar es llevar a cabo la implantación de un Plan de Continuidad de Negocio.

> "La seguridad total no existe

Pero ¿qué pasaría si estas amenazas estuvieran fuera de nuestra planificación, de tal manera que ni el más riguroso PCN fuera capaz de hacerlas frente? No es necesario ser alarmistas, pero estas situaciones ocurren y hay que estar preparados para cuando sucedan.

Ninguna organización está exenta de riesgos, precisamente por este motivo son necesarios mecanismos que permitan dar cobertura a estas incertidumbres. Es aquí donde las "pólizas de ciberseguridad o ciberriesgo" entran en juego y pueden ayudar a mitigar algunos de los riesgos asociados con las pérdidas financieras resultado de un incidente o desastre.

Inicialmente se pueden ver estas pólizas como algo superfluo o pensar que la organización no es lo suficientemente grande, interesante o importante como para estar expuestos a ciertos riesgos que puedan causar una pérdida que requiera el respaldo de un seguro. Incluso se puede llegar a pensar que aplicando las medidas expuestas en esta

Guía estamos suficientemente a salvo, pero esto puede ser una percepción errónea.

La intención no es la de convencer a ninguna organización para la contratación de una póliza de ciberseguridad, únicamente se pretende exponer esta opción como una medida adicional que debería ser estudiada como un complemento para garantizar la continuidad del negocio.

Los seguros en ciberriesgos

Los seguros de ciberseguridad o ciberriesgos están diseñados para mitigar las consecuencias financieras de un ciberataque, es decir, apoyar al Plan de Continuidad de Negocio cuando este ya ha cumplido la función para la que fue diseñado, siendo una extensión al mismo y ofreciéndonos una cobertura suplementaria.

Existen en el mercado multitud de compañías que ofrecen seguros de ciberriesgos, seguros que abarcan una amplia variedad de coberturas: desde aquellas que nos permiten mitigar los daños propios, hasta aquellas que llegarán a cubrir los daños ocasionados a terceros.

Analizar todas las variantes que el mercado oferta supondría una labor desproporcionada, fuera del objetivo de esta guía y que, en un breve plazo de tiempo, quedaría totalmente obsoleta. Se entiende que, por todos estos motivos, es mucho más práctico ofrecer una serie de pautas que permitirán identificar los puntos que son más relevantes para elegir una u otra póliza.

Para llevar a cabo este asesoramiento, se han enfocado estas pautas desde dos puntos de vista: la primera, orientada a identificar activos, tangibles e intangibles, y los daños proteger; y la segunda, permitir identificar qué criterios de cobertura deben tener las pólizas.

1. ¿Qué se quiere proteger o cubrir?

- Los daños propios, independientemente de su origen, podrían venir provocados por un tercero (proveedor, desastre natural…).
- Los daños provocados por la organización a terceros.
- La exposición ante incumplimientos normativos o legales (derechos de autor, privacidad…).

- La Responsabilidad Civil o Penal, tanto de la organización como de la Dirección o las personas que la componen.

2. ¿Qué deben ofrecer?

- Protección de la información frente a un incidente o desastre como: pérdida, robo, disponibilidad, reclamación…
- Cobertura en los gastos para la recuperación o restablecimiento y la gestión de la crisis.
- Cobertura frente a las pérdidas de beneficios, ingresos o la paralización de la actividad.
- Apoyo legal para reclamación de daños a terceros (proveedores, clientes…)
- Defensa legal y jurídica frente a inspecciones, denuncias o sanciones de organismos reguladores.
- Reclamaciones de afectados.
- Gastos por errores tecnológicos u omisiones.

Estas pautas representan un marco de referencia que debe ser ampliado por cada organización; en función de su actividad, su entorno o de las singularidades de su actividad de negocio. Si bien se recomienda el asesoramiento u orientación de una persona experta en esta materia, se ofrecen unas últimas recomendaciones que se consideran cruciales a la hora seleccionar una u otra póliza:

- Leer con detenimiento la póliza, es mejor una póliza básica y clara que una compleja y global.
- Identificar perfectamente las coberturas, los condicionantes y las exclusiones.
- Valorar sí el coste de la póliza en relación con la prima asegurada hace rentable su contratación.

7 GLOSARIO

Activo (Activo de información)

Cualquier información o sistema relacionado con el tratamiento de esta que tenga valor para la Organización; pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones.

Amenaza

Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un incidente de seguridad.

Brecha de seguridad

Incidente de seguridad que afecta a datos de carácter personal independientemente de si es la consecuencia de un accidente o de una acción intencionada y tanto si afecta a datos digitales o en formato papel. Una brecha de seguridad puede provocar la «destrucción, pérdida, alteración, comunicación o acceso no autorizada de datos personales».

Desastre natural

Cualquier evento catastrófico o incidente causado por la naturaleza o los procesos naturales de la tierra.

Dirección de la Organización

Mecanismo que desarrolla las líneas establecidas en las etapas de planeación y en el

seno de la Organización. Mediante la Dirección se establecen las líneas estratégicas y las directrices de la Organización y que se trasladaran en la estructura organizacional.

Estándar

Conjunto de normas y directrices para el control de la calidad y la gestión de la seguridad; permite establecer uniformidad en características de equipos, sistemas de cómputo, y procedimientos de operación, así como garantizar la integridad, compatibilidad y racionalidad en los procesos tecnológicos.

Guía de buenas prácticas

Conjunto de recomendaciones básicas dirigidas a dar soporte en la implementación de las medidas de seguridad de una Organización. .

Norma

Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.

Organización

Asociación de personas que se relacionan entre sí y utilizan recursos de diversa índole con el fin de lograr determinados objetivos o metas.

Plan de Continuidad de Negocio

Conjunto de planes de actuación, planes de emergencia, planes financieros, planes de comunicación y planes de contingencias destinados a mitigar el impacto provocado por la concreción de determinados riesgos que pueden ocasionar la falta de disponibilidad de la información y los procesos de negocio de una Organización.

Plan de Recuperación ante Desastres de TI

Proceso de recuperación que cubre los datos, el hardware y el software crítico, para que un negocio pueda comenzar de nuevo sus operaciones en caso de un desastre.

Procesos y actividades críticas de negocio

Conjunto de las tareas más importantes e imprescindibles que lleva a cabo una Organización para el desarrollo de su negocio.

Riesgo

La probabilidad de que una amenaza se materialice y resulte en una pérdida para la Organización.

Ransomware

Tipología de ataque informático en que el ciberdelincuente, toma control del equipo infectado y «secuestra» la información del usuario cifrándola, de tal forma que permanece ilegible si no se cuenta con la contraseña de descifrado. De esta manera extorsiona al usuario pidiendo un rescate económico a cambio de esta contraseña para que, supuestamente, pueda recuperar sus datos. La seguridad del sistema está basada en la dificultad de factorización de grandes números. Su funcionamiento se basa en el envío de un mensaje cifrado mediante la clave pública del destinatario y, una vez que el mensaje cifrado llega, éste se encarga de descifrarlo con su clave privada.

915 63 50 62

info@ismsforum.es

Calle Segre 29, 1B
28002, Madrid, Spain

@ISMSForum

ISMS Forum