LA CONTINUIDAD DE NEGOCIO PASO A PASO

Análisis de riesgos y gestión de crisis

Juan Vicente Teodoro Vidal

Copyright y registro

JUAN VICENTE TEODORO VIDAL es licenciado en Ciencias (Químicas) y toda su larga carrera profesional ha estado ligada a la industria, en varias empresas tanto en el sector privado como público, en puestos de investigación, producción y dirección. En su página web, **unoydostres.com** ha publicado centenares de entradas para la difusión del conocimiento, relativas a temas científicos, técnicos, organizativos y del mundo de la empresa.

LA CONTINUIDAD DE NEGOCIO PASO A PASO es una obra apta para principiantes, sin ningún conocimiento previo al respecto, que facilita la comprensión y el dominio de la continuidad. Mediante un esquema **DAFO** que resultará familiar a cualquier técnico o directivo, porque se trata de un método popular de organización, se van creando en pequeñas dosis, las bases para abordar distintos tipos comunes de crisis y para profundizar en técnicas específicas.

Primera edición

Corrección: Gemma Teodoro Baldó. Doctoranda en Comunicación. Licenciada en Filología Inglesa y Comunicación Audiovisual.

La figura principal de la cubierta representa la estatua de la Victoria Alada en la cúpula del edificio Metrópolis de la Calle de Alcalá de Madrid.

> *Nota sobre los enlaces a sitios web que aparecen a lo largo del texto:* Los enlaces se ofrecen de buena fe, *tal como estaban publicados* en el momento de la redacción de este libro, con fines divulgativos y como ampliación de conceptos del texto, sin ninguna dependencia entre este libro y dichos sitios de internet. Su inclusión no supone ni garantía de veracidad ni necesariamente conformidad con los contenidos publicados por sus autores. La gestión y control de los sitios, incluida la protección y el tratamiento de datos de quienes acceden a ellos es responsabilidad de sus propietarios y administradores. En consecuencia, no se admite responsabilidad por los posibles perjuicios, en materia de infracción de propiedad intelectual o de cualquier otra clase, que se pudieran producir como resultado del acceso a la información que contienen.

ISBN: 978-84-09-69698-7

LA CONTINUIDAD DE NEGOCIO PASO A PASO

Análisis de riesgos y gestión de crisis

Juan Vicente Teodoro Vidal

Los **negocios** son como los seres vivos:

Los grupos humanos, las sociedades y los negocios hacen lo que saben y pueden con el objeto de lograr su supervivencia y bienestar, a pesar de los riesgos que acechan en cualquier escenario. El comportamiento de los seres vivos y de los grupos humanos es una continua sucesión de acciones de **autodefensa** y **continuidad**. Todo ello **economizando**. Es decir: procurando que su esfuerzo valga menos que el bien que consiguen con sus actos.

Índice

PCN 0.: PROPUESTA DE ESTUDIO

Vamos a hacer este recorrido por los Planes de Continuidad de Negocio (en adelante PCN) mediante un proceso en que los contenidos se irán agregando sin que se hagan indigestos porque los vamos a trocear en pequeñas partes.

Contenido

Esta es una tabla abreviada de contenidos.

Sirva este capítulo a modo de prólogo

No encontramos en las librerías muchos **libros** sobre la continuidad de negocio en español. ¿Por qué? Puede que, porque nuestra manera de pensar mediterránea hace más uso de la **intuición** que de la **planificación**, y todo esto de la continuidad parece propio del mundo anglosajón y nórdico, más dado a hacer las cosas muy racionalmente. Vamos en muchas cosas a remolque de lo que inventan o proponen otros. Pero la **improvisación** no está reñida con el **conocimiento**, tal como sucede en **el jazz**, que es una música aparentemente improvisada, pero interpretada por virtuosos. Uniendo esa capacidad de seguir la **intuición con una sólida preparación planificada** se puede llegar muy lejos. Llegamos tarde a muchas tendencias, pero nos ponemos al día rápidamente. Yo quisiera contribuir a ello.

El propósito de este libro es aportar un texto lo suficientemente **comprensible** y a la vez práctico que permita difundir los conceptos de continuidad de negocio **en nuestro idioma**. No sigue el esquema expositivo de las normas sobre continuidad, que podemos considerar como su gramática, ni el de los demás textos que conozco, pero todo su contenido es compatible con las mismas. Es como si aprendiéramos una nueva lengua hablando, sin necesidad de conocer sus reglas antes de intentar a

expresarnos. Así es como aprendemos de pequeños a hablar, y nos permite emplear la comunicación desde el primer momento. El texto está completamente **estructurado** y a la vez trata temas que se pueden leer de forma **independiente** de los demás, sin perder perspectiva. Algunos de los aspectos más técnicos, como son la **organización** que se precisa en nuestra entidad, el **análisis de impacto** en función del tiempo de interrupción o la **gestión de crisis**, se han trasladado al final, donde hablamos de tipos concretos de crisis, de forma que se pueden percibir como necesarios, cuando de verdad hacen falta. Aunque se tratan allí para que sirvan de estrategias en determinados tipos de incidentes, tienen aplicación en todos los casos.

SERÁN SINÓNIMOS EN TODO EL TEXTO LAS SIGUIENTES EXPRESIONES:

PCN, CONTINUIDAD, PLANES DE CONTINUIDAD, PLANES DE CONTINUIDAD DE NEGOCIO, SISTEMA DE PLANES DE CONTINUIDAD.

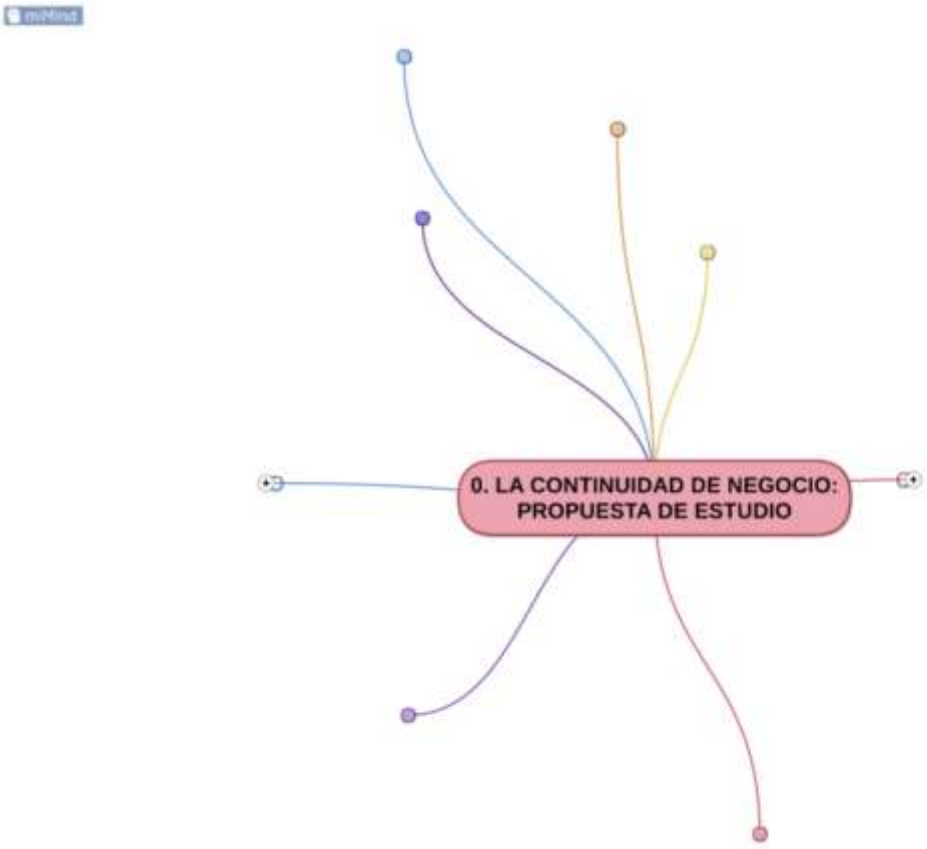
Nos referiremos a ellas indistintamente. Al final del libro espero que el lector, si llega hasta allí, no eche en falta nada realmente importante sobre la continuidad.

El contenido que sigue es el resultado de 7 años de **experiencia** en el asunto, gestionando un **sistema de PCN certificado,** en una empresa puntera en su sector a escala mundial, y de más de 22 años responsable de I+D y producción, en **industrias** papeleras, en las que la continuidad es una característica distintiva del negocio, porque los equipos y las máquinas trabajan en ***non-stop***. Añadamos a esto una breve pero intensa experiencia como **CISO**, que es uno de los empleos más apasionantes que se pueden desempeñar hoy en día, que incluye también una importante faceta de continuidad y seguridad.

Casi todo el texto estará formado por **grupos** con cuatro partes: los que llamamos **elementos** del sistema los clasificamos en cuatro apartados, que son los que forman un **análisis DAFO**, cada uno de los cuales tiene a su vez cuatro partes para detallar distintos aspectos. Lo mismo ocurre con los cuatro **casos de crisis** que vamos a considerar, que nos aprovecharán para introducir cuatro **actuaciones** importantes de la continuidad de negocio cada uno. Eso hace un primer subtotal de **32** pequeños capítulos con aspectos **técnicos**.

Además, habrá otros capítulos como éste, que serán **cabeceras** de cada grupo, para introducir nueva materia. Este segundo subtotal es de **12** capítulos más.

A estos habrá que añadir varios **complementos**: cuatro capítulos de aspectos **administrativos** que describirán la infraestructura que será común al sistema de PCN pero que podría ser común a cualquier norma ISO, y otros dos para aplicarlos cuando todo lo anterior esté **ya implantado y funcionando**, que nos dirán cómo se ha de **planificar** el sistema de PCN y cómo optar a la **certificación** del mismo. Este tercer subtotal será de **seis** capítulos más. **El total general es de 32+6+12 = 50 capítulos**.



Empezamos de cero. La Continuidad depende de muchas cosas, pero aún no hemos dicho cuáles.

Podemos pensar en la **continuidad de negocio** como si fuera un pulpo, con ocho brazos (un ***octopus***), en que cada brazo tiene un cierto nivel de vida propia independiente de los demás. Iremos viendo poco a poco cómo en la práctica intervienen los distintos factores y la relación que tienen entre sí.

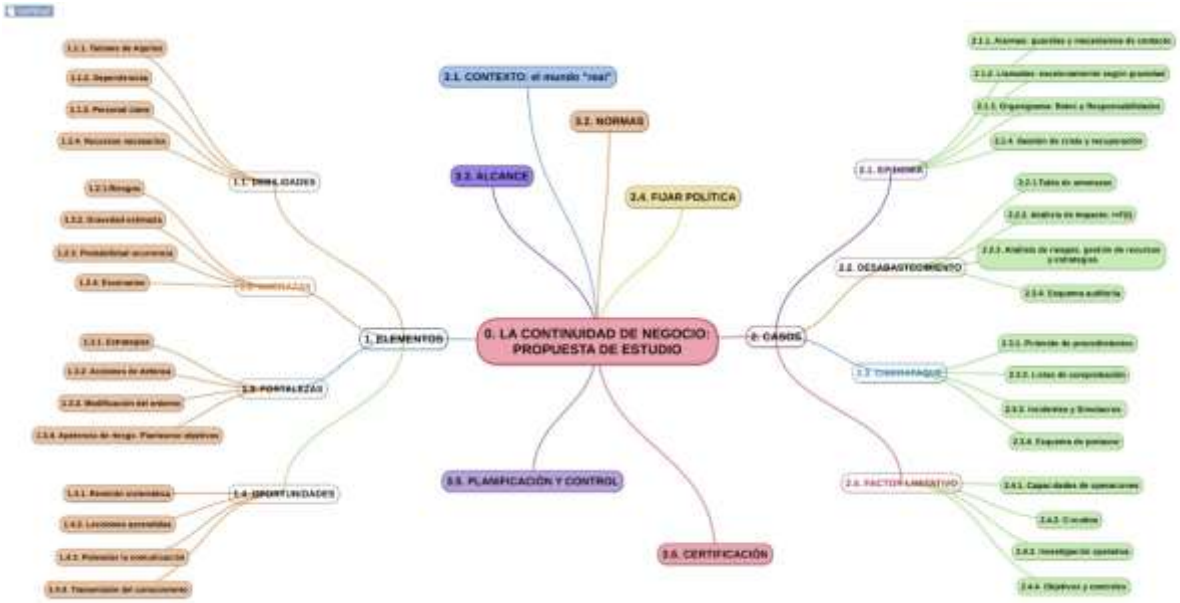
El enfoque empleado en el texto es que **no necesitamos tener conocimiento previo** de la materia para ir introduciéndonos en ella. A base de hablar con bastante frecuencia del asunto acabaremos teniendo conocimientos y opinión sobre el mismo. Si no tenemos prisa, podemos dedicar a cada capítulo un día y verlo así a fondo, dejando que los conceptos vayan decantándose e intentando ir completando las acciones que se van exponiendo.

El lector estará guiado todo el tiempo por este mapa mental, que irá ampliándose momentáneamente y detallando el lugar exacto de **PCN** en que nos encontramos.

Espero que sirva, ¿porqué no? de disfrute. Si resulta suficientemente interesante, animo a **comentarlo** con algún colega para ampliar el círculo de interesados en los planes de continuidad. También se puede **opinar, enviando mensaje al mail** **cero@unoydostres.com**.

CONTINUARÁ…

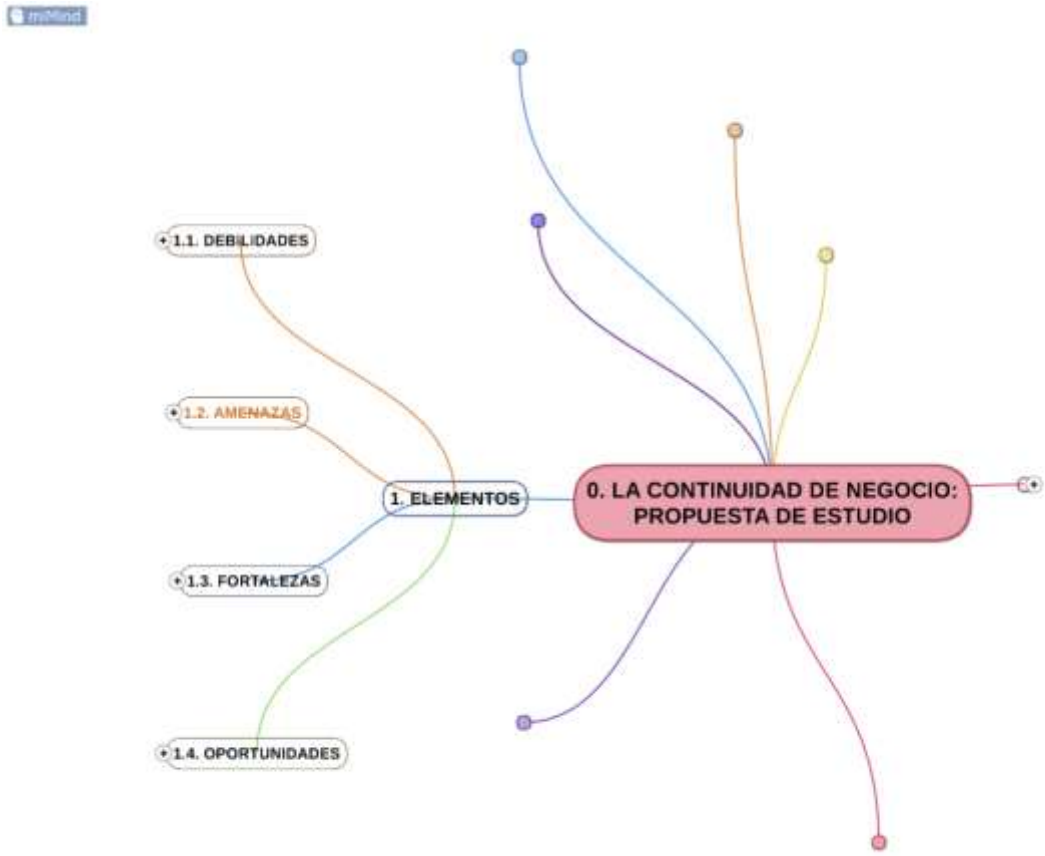
Este es el mapa general del libro:



PCN 1. ELEMENTOS

En el estudio que nos ocupa sobre los planes de continuidad, empezaremos por algo fácil: por unos pocos elementos como los que se describen en un análisis DAFO. Así, sin dejar el ambiente conocido de la gestión de la empresa, entraremos poco a poco en otro punto de vista: el de la continuidad.

La **continuidad de negocio** **no es algo distinto de lo que hacemos a diario** en el día a día de nuestra empresa o nuestra organización. Simplemente se trata de **enfocarlo todo** para lograr la mayor disponibilidad al mínimo esfuerzo. Con este enfoque es creativo **utilizar lo que ya sabemos**, para asegurarnos de que en caso de incidente vamos a salir lo más airosos posible sin demasiados costes ni pérdida de tiempo para nadie.



Los elementos que consideraremos son los que se derivan de un análisis DAFO.

Análisis DAFO

Dado que una empresa se comporta **como un ser vivo**, que no puede dejar de *respirar*, todo lo que pueda afectar hasta el punto de provocar su parada *vital* o su falta de **disponibilidad**, que es lo que tratamos de proteger, será un problema que debemos de considerar desde los cuatro puntos de vista posibles combinando: origen **interno o externo** y capacidad de **dañar o mejorar** los intereses de la organización.

- Interno y dañar = (**D)ebilidad**
- Externo y dañar = (**A)menaza**
- Interno y mejorar = (**F)ortaleza**
- Externo y mejorar = (**O)portunidad**

Este es un análisis simple, conocido como **DAFO**, pero extremadamente eficaz, porque resulta intuitivo incluso a quien no lo haya realizado antes, y porque a la vista de los resultados **invita inmediatamente a la acción**. Además, se trata de una reflexión que conviene hacer independientemente de que queramos tratar el aspecto de la continuidad. En gestión empresarial es una de las tareas elementales que conviene realizar **periódicamente** para evitar problemas de funcionamiento de toda índole.

Hay otras variantes de esta técnica en las que no entramos ahora, para exponer el tema con la mayor sencillez posible, y que invitamos a buscar e investigar.

Para nosotros será un **ejercicio de preparación** en los periodos en que no esté a la vista ninguna crisis. O sea, un trabajo para estar cada vez más preparados y listos por si surgen problemas que afecten a nuestra **disponibilidad**.

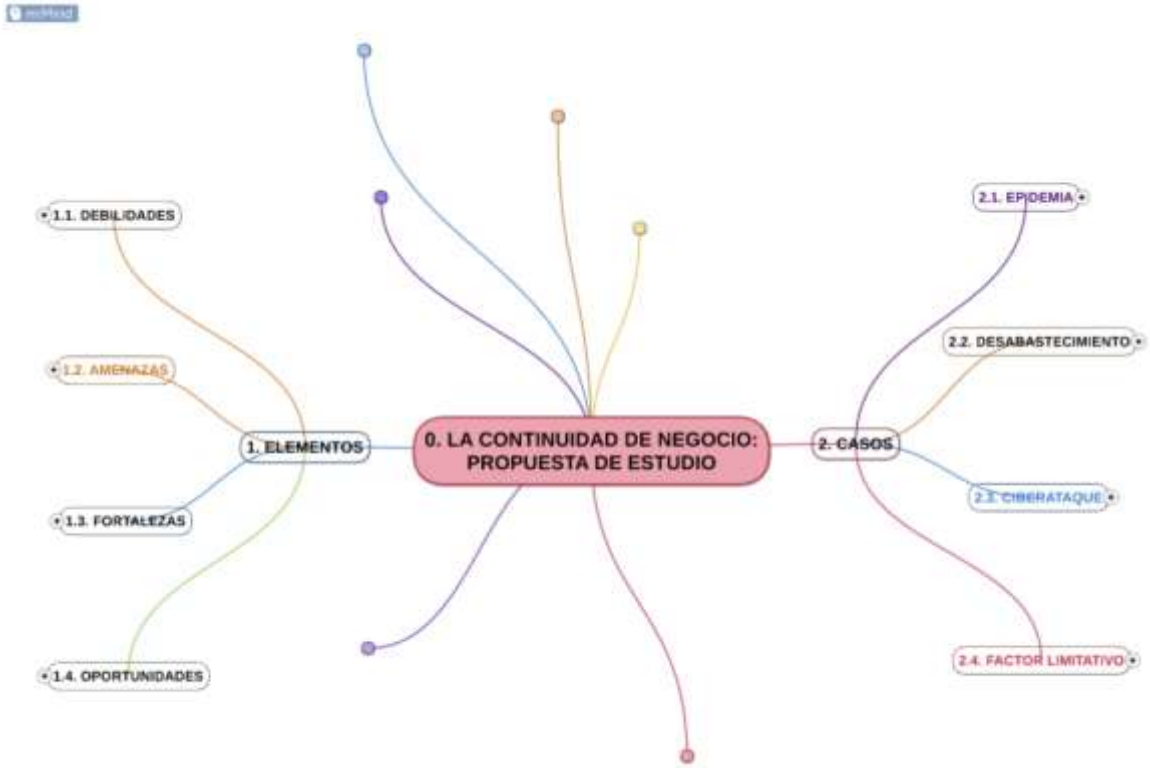
El término **disponibilidad** es el que emplearíamos de forma intuitiva, para significar la capacidad de seguir desempeñando **normalmente** la misión que tenemos asignada, es decir: una manera de decir que *el estado de disponibilidad* es aquel en que no sucede nada anormal que nos impide trabajar o hacerlo sin cargas o retrasos, originados o provocados de forma involuntaria (otra cosa es cuando nos hemos empeñado en hacer más cosas de lo normal y llevamos nuestro proceso a un estado de no disponibilidad de cumplir con un ritmo excesivo). La falta de disponibilidad, tal como la consideramos aquí, surge como consecuencia de una causa **involuntaria** y **no planificada ni presupuestada**.

Es a la vista del **propósito** de nuestra organización y de nuestros compromisos como se deben analizar los elementos considerados. Cuando se funda una empresa o se activa una organización, se hace al amparo de unas determinadas **leyes**, de un **contrato** privado o social (que puede ser una declaración de intenciones, la política de la organización o la escritura de constitución de la entidad y sus **estatutos**), teniendo una **reputación** que nos avala (o al menos el beneficio de la duda cuando aún no somos conocidos) y **evitando provocar retrasos** y problemas a otras partes que necesitan de nuestra actividad para llevar a cabo o continuar con la suya.

Esta tarea primera que tenemos a la vista nos llevará varias sesiones que constituyen la **parte 1 del texto**. En ella vamos a estar apoyándonos en este tipo de **ejercicio de preparación extensiva** del conocimiento sobre nuestra organización que nos dará el **DAFO**. De forma que no entraremos en muchos otros aspectos de la continuidad hasta la parte 2 del texto.

En esta segunda parte abordaremos cuatro tipos de crisis, que llamaremos **casos** (pandemia, desabastecimiento, ciberataque y factor limitativo —vulgarmente atasco–), para que veamos espontáneamente y de forma natural qué cosas nos habrán quedado por hacer en la primera parte y cómo llevarlas a cabo según el tipo de incidente. Aunque la estructura de los planes de continuidad es la misma en toda la organización y circunstancias, según la clase de problema que tratemos hacen más falta algunas funciones de la organización que otras.

Para conseguir una mayor aproximación a la realidad de la **organización o de la empresa en acción**, los **tipos de crisis** mencionadas que hemos elegido para la parte 2 las representamos en la derecha del siguiente diagrama:

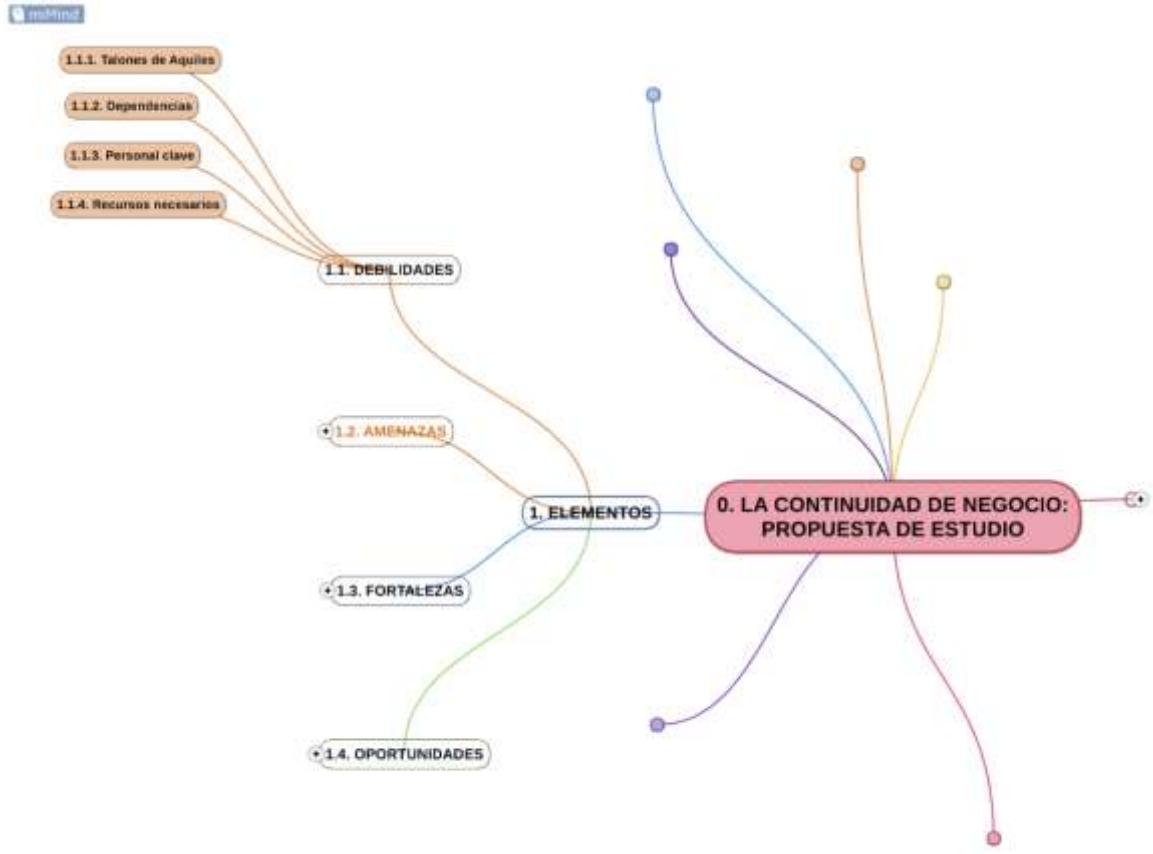


PCN 1.1. DEBILIDADES

Estamos poniendo la lupa en los primeros elementos que nos interesan de los planes de continuidad. Nos vamos a centrar hoy en las debilidades. Es una forma de conocer más a fondo nuestro negocio y hacer autocrítica.

Empezar por las debilidades, por un lado, aparentemente, **es lo más fácil**, porque estamos viéndolas a diario en nuestro trabajo. En lugar de protestar, veamos **qué cosas deben mejorar** y empecemos a pensar de qué forma podemos cambiar nuestro sistema.

Por otro lado, paradójicamente, hay una especie de **punto ciego** que nos impide hacer autocrítica de lo que tenemos. Es imprescindible que traspasemos ese *velo*, pues de ello depende que hagamos lo que toca.



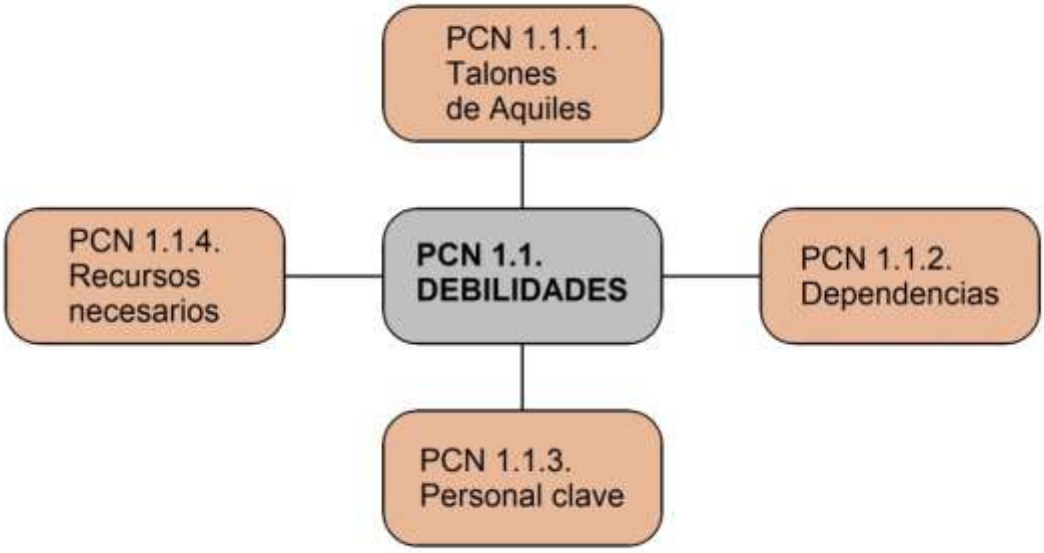
Estudiar las **debilidades** de nuestra organización: primera tarea en PCN.

Al novato se le plantea la primera duda al tener que ver primero qué cosas pueden fallar en la organización, en lugar de ir directamente a ver qué clase de riesgos son los que estamos corriendo. En PCN es más importante y urgente averiguar cuáles son nuestros **puntos débiles** por varios motivos:

- Es más inmediato actuar sobre lo que **está en nuestra mano** que pretender *arreglar el mundo* (que además no es nuestra misión, a menos que gobernemos una gran potencia o estemos al frente de una multinacional).
- Los **incidentes** que podemos tener en un *universo caótico* son de infinitos tipos. Además, no sabemos cuáles de ellos se volverán graves. Es mejor reforzar las cosas que vemos o descubrimos que penden de un hilo, de forma que tengamos una situación más segura.

El criterio que debe guiar esta parte de la actuación es **determinar las prioridades y requisitos**. Esto es lo que nos dirá más tarde la norma correspondiente a la organización de planes de continuidad, cuando la leamos con calma (punto 8.2.2. de la ISO 22301) y se referirá a este ejercicio como **análisis de Impacto sobre el negocio**. Puede ayudarnos lo que nos enseñan los **asesores de gestión** empresarial, aunque es importante que aprendamos a **emplear nuestros propios métodos**, tras interiorizar aquello que tiene relevancia para nuestro negocio, adaptando o **inventando los mejores métodos**.

Una vez situada en el diagrama general la posición del conocimiento de las **debilidades** de nuestros procesos, solo queda, de momento, indicar que vamos a actuar en cuatro líneas, que se describen en el esquema que sigue:



PCN 1.1. DEBILIDADES.

Debilidades tipo

Algunos de los puntos que llamamos debilidades se asumen enseguida, como por ejemplo los **talones de Aquiles** o las **dependencias**. Otros se diría que son puntos fuertes, como el personal clave o los recursos que movilizamos en nuestros procesos, pero no nos engañemos, el **personal especializado** que ocupa **puestos clave** cuesta de educar y es más exigente para aceptar nuestras condiciones de contratación, estando con más frecuencia tentado por otras organizaciones. Por este motivo, cuantos más **recursos** se necesiten para poder hacer nuestra función, más probabilidades habrá de que falte alguno que nos ponga las cosas complicadas.

Como en el conocido refrán que dice que

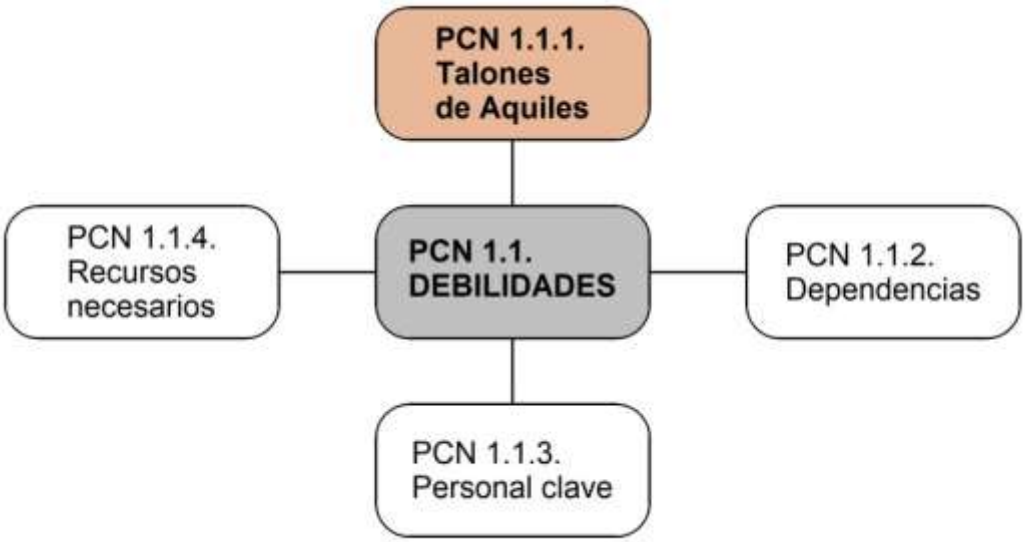
"NO ES MÁS RICO EL QUE MÁS TIENE, SINO EL QUE MENOS NECESITA"

Igual sucede en las organizaciones, que es más poderosa la que puede prescindir de medios que otras necesitan *sin falta*. Desarrollaremos estos conceptos en sucesivas entradas.

PCN 1.1.1. Talones de Aquiles

Dentro del grupo de debilidades, vamos a echar un vistazo a los talones de Aquiles, que son aquellos puntos del proceso que se vuelven vulnerables *por diseño*, es decir, por la forma en que está montado o funciona el dispositivo de nuestra actividad.

Recordaréis sin duda, de **la Iliada**, la fortaleza y valentía sin igual del héroe griego **Aquiles** en su lucha contra **Troya**, que sin embargo tenía un punto débil. **Paris** mató a **Aquiles** clavándole **una flecha envenenada en su talón**, la única parte de su cuerpo que era vulnerable, según una tradición posterior al poema de **Homero**.



Los talones de Aquiles en el contexto de las DEBILIDADES.

En nuestro caso, analizando cualquier proceso, siempre encontraremos algún **punto débil**: una parte que está **más expuesta** a cualquier manipulación, avería o accidente por la que quedaría inutilizada, una etapa que siempre sea **más lenta** que las demás y paralice todo el proceso, un **fallo de diseño** del proceso que obligue a parar en el momento más inoportuno.

En lugar de entrar en demasiados detalles, basta con considerar que en las películas bélicas se ve cómo se puede inutilizar un artefacto imponente como **un tanque** poniendo una (pequeña) carga en determinados puntos de su armadura, o cómo la mayoría de **accidentes** que paralizan la actividad ocurren por el detalle tonto menos pensado que podía ocurrir, pero que un día ocurre. Por eso miramos a derecha e izquierda antes de **cruzar la calle**, aunque estemos en un paso de cebra, por si un conductor no se ha dado cuenta de nuestra presencia. Por eso los aviones comerciales tienen **uno o más pares de motores**, por si falla alguno.

Este punto de la duplicidad del factor clave es la base del concepto de **fiabilidad** en ingeniería de procesos, que podríamos definir como la forma de conseguir que el proceso funcione en cualquier circunstancia, y esto se consigue teniendo más de una línea de producción, por si falla alguna. Incluso la naturaleza ha previsto que tengamos de algunas clases **órganos duplicados** (ojos, oídos) o incluso muchas parejas de ellos (dientes).

Recuerdo la primera visita que hice a una fábrica de papel que tenía **dos máquinas ¡pero *sólo un* refino!** para alimentar a ambas. En esa época no sabía que me dedicaría a la continuidad, pero me pareció una situación muy poco apetecible.

Si analizamos las distintas clases de talones de Aquiles con las que nos podemos encontrar en nuestros procesos, invariablemente la acción que se nos ocurre para protegernos es **evitar la exposición al riesgo**.

- Si hay un **punto débil** en el medio de trabajo, **reforzar** esa parte del proceso.
- Si se ve la **situación arriesgada**, utilizar medios de **protección** personal.
- Si podemos dar un **mal paso** al entrar en zona de peligro, **pensarlo dos veces** y no arriesgar.
- Si **nos podemos permitir** económicamente **multiplicar** los elementos clave, hacerlo.
- Si una **localización única** es problemática, tener **alguna alternativa** en otro lugar.

No se nos escapa que en general evitar la exposición al riesgo es una cuestión de **diseño**, más que una cuestión económica. Como argumento, deberíamos considerar cuánto costaría una interrupción por no haber previsto el coste de duplicar una línea del proceso, teniendo en cuenta la probabilidad estimada del suceso que lo puede interrumpir.

Así como **la búsqueda** de talones de Aquiles o puntos débiles puede empezar preguntándonos qué parte del proceso lo pararía todo si se parara esa parte, la búsqueda de **soluciones** pasará por preguntarse "qué haría yo" para evitar que parara el proceso en caso de que fallara el punto débil. La respuesta más general en una sola palabra para rebajar la exposición al riesgo es **DIVERSIFICACIÓN**, o sea, no apostarlo todo a una única forma de hacer las cosas.

El inventario

De momento, para poder planificar mejor las acciones que correspondan tras el análisis de los talones de Aquiles, lo que hay que preparar es una **lista de los procesos** (**un inventario**) de nuestra organización o negocio, detallando para cada uno las **operaciones** que los forman o subprocesos, e indicando en cada operación claramente **sus puntos débiles**. Es la mejor forma para poder **fijar prioridades** de actuación.

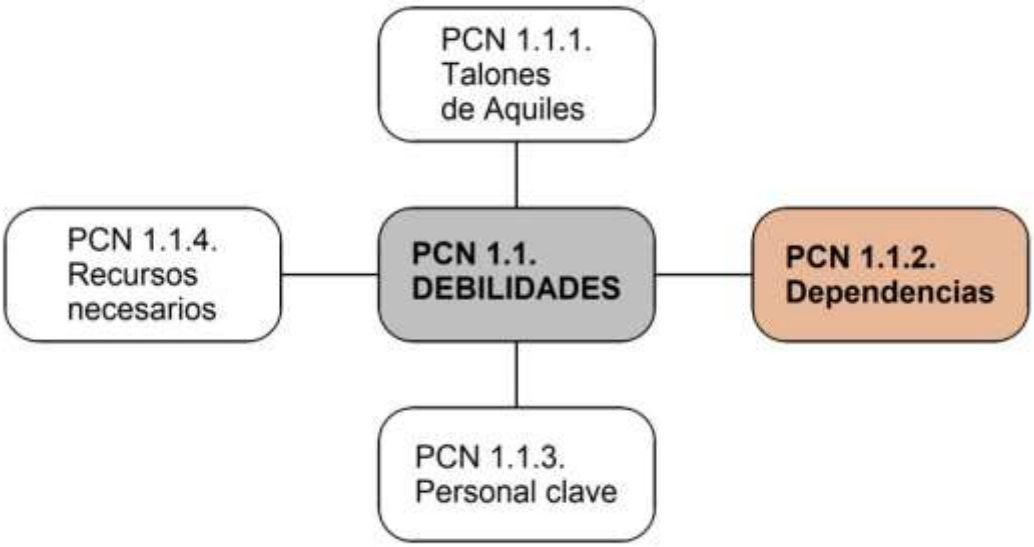
La **lista o inventario de los procesos** servirá también de base para cuando completemos una **aproximación más técnica** consistente en el conjunto de **Análisis de Impacto en el tiempo** (lo veremos en PCN 2.2.2), **Apreciación del Riesgo** (PCN 1.2.1), Determinación de **Escenarios** (PCN 1.2.4) y **Determinación de Estrategias** (PCN 1.3.1).

Esta lista de los procesos puede hacerse **en una hoja de cálculo**, empleando una **fila** para cada proceso y cada subproceso y empleando **las columnas** para indicar por ejemplo puntos débiles, dependencias, personal, recursos necesarios y las acciones a realizar, su prioridad, etcétera. Así se forma sin esfuerzo **una base de datos** del inventario.

PCN 1.1.2. Dependencias

Veremos hoy otras causas de debilidades en una organización o empresa. Las dos primeras acepciones del diccionario de la RAE dicen, sobre dependencia: 1. Subordinación a un poder, 2. Relación de origen o conexión. Una organización dependiente tiene condicionados los aspectos clave de su funcionamiento.

Las relaciones de dependencia en la empresa, sean **de tipo político, económico, comercial, industrial** o de cualquier otra clase, influyen en su capacidad de actuación, añaden **restricciones** y en general **dificultan** optimizar el funcionamiento. De la misma manera que otras clases de dependencias bloquean el desarrollo personal de quien las padece, las dependencias de una organización o empresa, configuran de gran modo sus fines, su rendimiento, incluso su pervivencia. Por eso las calificamos como **causas de debilidad**.



Las dependencias crean debilidad.

Se han elaborado incluso teorías sobre la dependencia. **Ver el artículo de Wikipedia**: "Teoría de la dependencia". De manera que es un tema estudiado por los economistas. El propio lenguaje nos está diciendo lo evidente: que **dependencia** es lo contrario de **independencia** o **libertad**. Veamos ejemplos junto con posibles actuaciones:

- Si dependemos de un tipo de **suministro** muy específico o que se ha de importar, a lo mejor es buena idea buscar proveedores cercanos, tener **proveedores alternativos** y asegurarse de su **solvencia** (de todos ellos). También puede ser una buena idea **aumentar las existencias** de esos suministros para poder terminar los compromisos y productos en los que intervienen, sin que su carencia en el mercado nos provoque interrupciones.
- Si en un país es **más escaso o caro el crédito**, ello dificulta y encarece operaciones de capital o de consumo. Habrá que incrementar la capacidad de **ahorro** para **autofinanciarse**. Como alternativa, si es conveniente debido a una alta necesidad de capital, la entidad buscará **radicarse donde haya menos dificultades** de financiación, a fin de evitar paradas o incurrir en más gastos por falta de liquidez.
- Si las **leyes y los costes laborales** de un país son *desmotivantes* para la contratación, suponen una alta presión fiscal o se crea un clima de

conflictividad laboral, se tenderá a **deslocalizar** la producción o los servicios, en busca de la flexibilidad de las actividades y de la mayor previsibilidad de los procesos.
- Cuando la actividad de nuestro proceso tenga **dependencia de otros procesos internos**, no podremos hacer nada mientras estos no terminen las fases previas a nuestra producción. Una adecuada **planificación** global de la producción o de la actividad y el recurso a la **investigación operativa** a escala de toda la empresa puede contribuir a solucionar la cuestión.

Las organizaciones siempre buscan alternativas que permitan librarse en la medida de lo posible de las restricciones a su actividad. En una palabra, buscan **la NO-DEPENDENCIA.** Todas las acciones que hemos indicado al lado de la enumeración de dependencias tienen como objetivo lograr mayores grados de **libertad** y de **opciones.**

¿Cómo va el registro?

Recordaréis que aconsejábamos ayer para el caso de los *talones de Aquiles*, emplear el **registro de los procesos** y sus subprocesos, creando una columna para registrar los que consideramos como puntos débiles de cada operación de la lista. Hoy, de la misma forma, **añadiremos otra columna** para **registrar las dependencias** que hayamos detectado, que consideramos relevantes de cada proceso, subproceso u operación.

Vemos que va resultando muy útil tener **registros** de lo que estamos haciendo. La memoria es limitada, no somos juglares que tengamos la virtud de recitar de memoria lo que hemos aprendido y sobre todo, lo que no figura en un procedimiento o en un registro es muy difícil probar que lo hemos logrado mejorar, porque no quedan trazas.

Podéis ver lo que dice **Wikipedia sobre los registros**: “Registro (base de datos)”. Nos asegura que son elementos de una **base de datos relacional**. Si diseñamos bien los registros de nuestro sistema documental, podemos manejar la información eficientemente porque la podremos integrar en una base de datos y además dispondremos de **evidencias** consistentes para el proceso de **certificación**, que podremos iniciar más adelante (hablaremos de la certificación en el punto PCN 3.6, el último capítulo del libro).

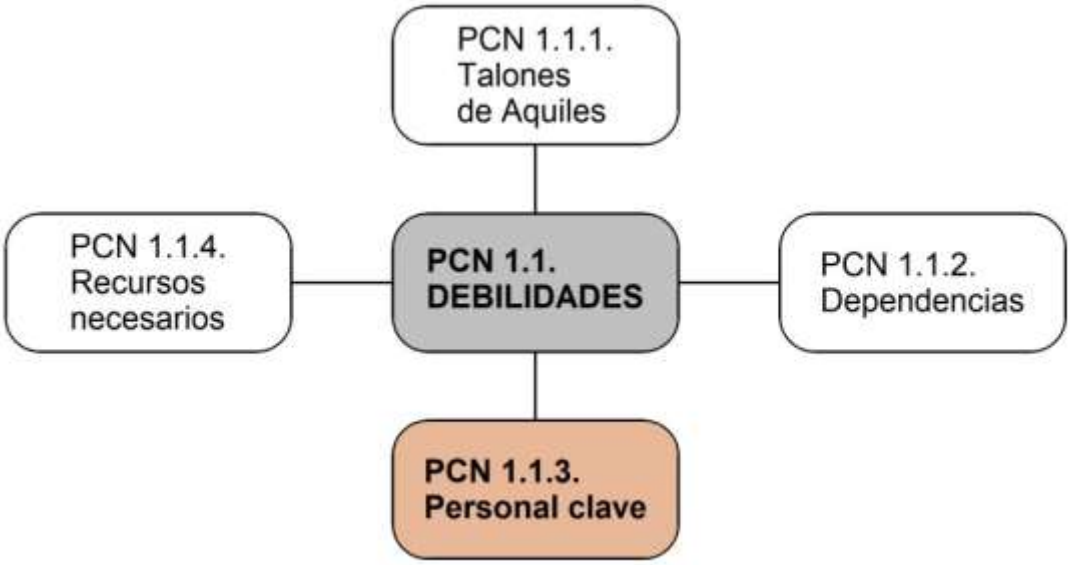
Lo que vamos haciendo hasta ahora, básicamente **ser conscientes de la realidad** de nuestros procesos en aspectos que puede que no les hayamos prestado anteriormente suficiente atención, en sí mismo y sin entrar en tecnicismos, ya nos **estará siendo útil** para mejorar la continuidad de nuestra empresa.

En el siguiente capítulo continuaremos la labor de ampliar nuestros datos sobre el proceso.

PCN 1.1.3. Personal clave

Siguiendo la descripción de las debilidades, llegamos al punto más importante: el del personal clave. En los libros sobre gestión empresarial se refieren al personal (metafóricamente) como el activo más importante, y no se equivocan (aunque no figure en los balances). Pero, como todo el que tiene un bien precioso, perderlo es mucho más impactante.

Cuanto más sofisticada es una organización, más importante es **el personal** que la compone. La tecnología, si no se tiene disponibilidad de tiempo ni se investiga, aun se puede comprar con dinero; es el famoso refrán «que inventen otros». Pero en una empresa que busque **la excelencia** se ha de cuidar al personal, incentivarlo, premiarlo cuando consigue un éxito, hacer que conviva o se relacione con otros profesionales para que puedan extraer todos el jugo del **conocimiento** que se comunica y del que se crea, para que se de a conocer y pueda lucirse. Se ha de ofrecer la posibilidad de desarrollar una **carrera profesional** en la empresa, sentirse partícipe de sus realizaciones.



El personal clave es el factor determinante del éxito empresarial, y su mayor debilidad.

En este punto vamos a definir mejor el concepto de ***personal clave***, para nuestro fin:

Personal clave:
-NO es en este contexto equivalente al que se fija por contrato con nombres y apellidos en un proyecto para que el cliente tenga garantía de profesionalidad,
-**ES simplemente el personal que consideramos mínimo para que nuestros procesos funcionen correctamente**.

¿Por qué el **personal clave** lo considero **una debilidad** de la empresa? Porque le sucede como a esa **pieza valiosa y única** de la que depende que todo funcione correctamente; porque o **no tiene fácil repuesto** o porque si se queda en *fuera de juego* temporalmente se compromete el funcionamiento de toda la organización. Más concretamente **la debilidad es que todo o parte del personal clave (simultáneamente) no esté disponible**. Es lo mismo que nos pasaba con los talones de Aquiles: **el problema** no es que tengamos una instalación *que hace funcionar* el

proceso, sino ***que pueda fallar*** esa instalación en un punto determinado que nos pare el proceso.

Hay fenómenos relativos al **personal clave** que nos muestran **facetas delicadas** de su relación.

- Un buen **profesional que no está motivado**, porque no se le tiene en cuenta, porque se le paga poco en relación con su responsabilidad, cometerá errores, descuidará obligaciones, se buscará otro empleo y abandonará la empresa dejándola **en jaque** en el momento más inoportuno. Evidentemente la solución es **compensar adecuadamente su trabajo** sin olvidar los aspectos humanos del **reconocimiento público**, aplicando los nombramientos de forma justa, **sin excluirlo** de las posibilidades de **promoción**, manteniéndolo **informado** de las estrategias y los planes de la empresa (en la medida que puedan compartirse).
- Una **enfermedad o accidente** incapacitante. Esto no puede excluirse nunca, pero es más aleatorio que el punto anterior. Tomarse muy en serio la **vigilancia de la salud del personal** y la **prevención de los riesgos laborales**. En estos casos, tener **suficiente personal** que en un momento dado pueda hacer sustituciones podría evitar el colapso de la actividad. Para ello, disponer de un buen **sistema de formación**, tanto presencial como on-line ayuda para formar y reclutar a personal de refuerzo, retribuyendo las jornadas de estudio. También ayuda la fijación de **guardias** (por supuesto retribuidas), e incluso la posibilidad de teletrabajar, según en qué trabajos.
- **Ambiente poco ético**, acoso, reproches. En este punto **la Dirección ha de dar ejemplo** y no tolerar ninguna situación poco ética, bajo ningún concepto, corrigiendo de forma firme cualquier comportamiento inadecuado, publicando los **principios éticos** de la entidad, para general conocimiento. Con una política ética potente, el puesto de trabajo se vuelve más agradable y se fomenta la asistencia al trabajo.
- **Ausencia de una carrera profesional**. Es tan sencillo listar los contenidos y méritos que debe tener alguien para ir escalando puestos en la empresa, que resulta triste ver que a veces se da prioridad a compromisos o mala información para ascender a la persona equivocada. Hay que fomentar el aprendizaje *in situ* y los **ascensos por méritos**. La **experiencia**, *a priori* vale más que el conocimiento que pueda traer alguien que no conoce la empresa y el personal recibe el mensaje de que si se esfuerza por trabajar bien, sale ganando.
- Falta de **transmisión del conocimiento**. Cuando alguien en la entidad haya tenido una experiencia rica y provechosa, debería sacarse el máximo partido de sus conocimientos para **traspasarlos a los que vengan**, los empleen o no. Porque igual que no se debe impedir la creatividad de alguien nuevo, también es un desperdicio no aprovechar lo que han aprendido los *senior*, aunque fuera válido para otra época.

En todos los casos la medicina es la misma: **VALORAR** (2º acepción del diccionario de la RAE: **Reconocer, estimar o apreciar el valor o mérito de alguien o algo**) **a los miembros del equipo profesional** en sus distintas facetas: promocionando justamente al personal, retribuyéndolo bien, haciendo que se sienta que la empresa también es suya. Una persona que se sienta valorada faltará menos al trabajo y será más productiva en su jornada, transmitirá a su alrededor buenas sensaciones de la empresa y estará más predispuesta a **crear equipo** con el resto.

Seguimos con el inventario

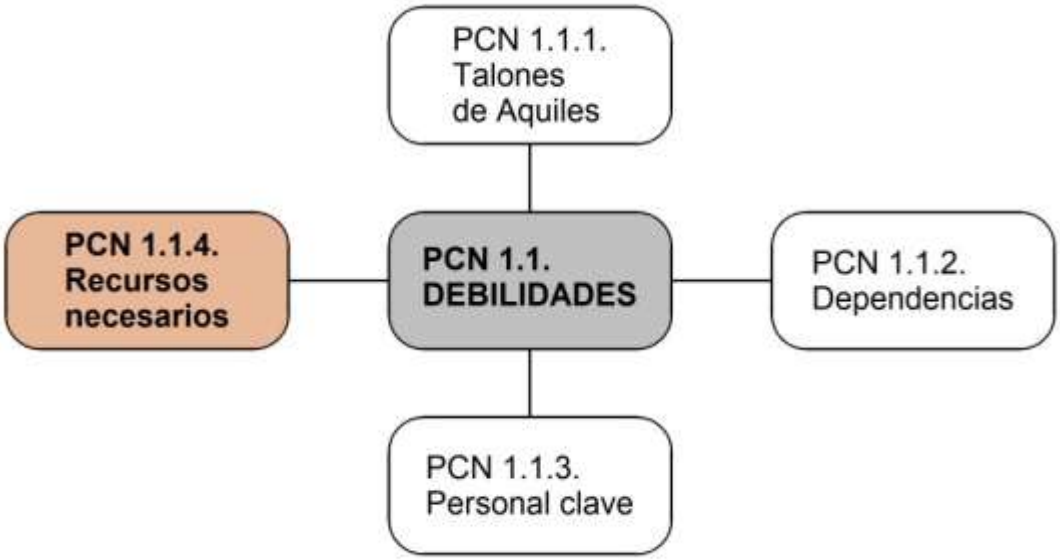
Debemos coger la hoja en la que hemos reflejado en cada fila un proceso y en sucesivas filas los subprocesos que lo componen y así sucesivamente; en distintas columnas ya hemos ido anotando los puntos clave o talones de Aquiles y las dependencias de cada uno de los procesos y subprocesos.

Ahora **añadimos una columna más** para **anotar los puestos clave para que funcione cada una de esas operaciones (procesos y subprocesos)**. Basta que indiquemos **cuántos puestos** de cada clase son clave para cada operación. Podemos añadir entre paréntesis los nombres a los que nos estamos refiriendo en cada caso, pero de momento bastará con **cuántas personas hacen falta** y son imprescindibles para que la operación pueda llevarse a cabo y qué **categoría** tienen (conocimientos + experiencia) para poner en marcha y mantener los **procesos en un nivel mínimo aceptable**.

PCN 1.1.4. Recursos necesarios

Para terminar con nuestro estudio de debilidades, trataremos el detalle de los recursos necesarios. Igual que en los otros tres puntos anteriores, *lo que es una debilidad* es la *ausencia* de alguno de los recursos que consideramos necesarios. Ahora se trata de hacer el ejercicio de listarlos.

En caso de un incidente se impone un primer *balance de daños*, pasando revista a ver si funciona todo lo que consideramos necesario. Esto puede ir desde un local que haya sido afectado por una inundación, a la integridad de los datos tras un **ciberataque**. Todo lo que entendemos imprescindible para *subir la persiana* e iniciar la jornada, debe estar accesible y en uso.



Los recursos necesarios como debilidad.

Ahora pasaremos revista a lo que no hemos tratado antes: ya nos ponemos en situación de que no ha fallado ningún punto clave o talón de Aquiles de los que tenemos identificados, que las relaciones de dependencia (suministros, contratos y condiciones, etc.) están en orden y se cumplen, que el personal clave está disponible, pero tenemos que asegurarnos también de que los demás **recursos necesarios** de nuestros procesos estén **operativos**. Para ello veamos antes qué pasa si esto no es así. Los recursos de los que vamos a hablar son genéricos y puede que en algún caso tengan más o menos relevancia. Por eso hay que hacer un balance previo de lo que es necesario en nuestro caso particular:

- Generalmente nos hará falta **un local**. Si el local está anegado por una inundación o ha sufrido un incendio, ¿podemos iniciar nuestros procesos con la parte que quede libre? ¿Tenemos algún espacio alternativo (o lo podemos tener fácilmente) con todo o donde se pueda llevar lo necesario para trabajar? Generalmente es esencial mantener la accesibilidad a los locales de trabajo.
- Los **suministros de energía** y de agua, también máquina de café y de tentenpiés. ¿Cuán necesario es el suministro de energía y con qué dimensionamiento? ¿Se precisa agua corriente, aseos, lugares de descanso con su máquina de café y suministros de ***catering***? Aunque, en principio y cada vez más, el suministro de energía eléctrica está garantizado, tenemos que tener

alguna alternativa. Lo mismo para el agua o los pequeños suministros que necesita el personal durante la jornada.

- Los **sistemas informáticos**. ¿Cuántos, de qué tipo, con qué software? Cada vez más son precisos los ordenadores para cualquier actividad. ¿Quién se encarga de que funcionen y se corrijan errores o malos funcionamientos? Tendremos que ver qué material informático hace falta para iniciar la producción.
- Las **comunicaciones**, que suelen ser algo más que un simple teléfono, deben garantizarse. Tanto los dispositivos móviles como los PCs y las impresoras, etcétera, deben estar operativos y accesibles.
- La **seguridad de la información** y del resto de las instalaciones. La más importante propiedad, aparte del dinero de la empresa o de la organización son **los datos**. ¿Qué se requiere para estar seguros de que siguen íntegros, no se pierden y están suficientemente protegidos ante miradas inconvenientes, en particular los datos que manejamos corporativamente de clientes y personas externas? ¿Con qué frecuencia hay que hacer **copias de seguridad**, cuántos ejemplares de cada copia y en qué sitios están custodiados? ¿***Todo lo demás*** de los locales está también seguro?

En esta parte de nuestro análisis, el resumen es que lo que se determina es **LA EXISTENCIA y SEGURIDAD** de todo aquello que funciona como elementos auxiliares de la actividad. Que no echemos en falta nada esencial.

Terminando el registro de procesos

Para terminar, de momento, el **registro de los procesos** y sus subprocesos, del que hemos estado hablando en los apartados anteriores, crearemos **otra columna** para registrar los **recursos** que consideramos necesarios añadidos a los que ya hemos indicado (talones de Aquiles, dependencias, personal clave). La columna de hoy incluirá de forma sumaria todos esos **recursos necesarios** de cada proceso, subproceso u operación. Esta información será vital para realizar correctamente el **Análisis de Impacto** en función del tiempo, que abordaremos en el punto **PCN 2.2.2. Análisis de Impacto I=F(t)**, ya que nos proporcionará toda la información relevante del mapa de procesos. Como vemos, hemos adelantado un buen trecho, conociendo mejor nuestros procesos, para prepararnos ante cualquier incidente que venga a interrumpirlos.

La estructura del registro o **mapa de procesos** puede ser como sigue:

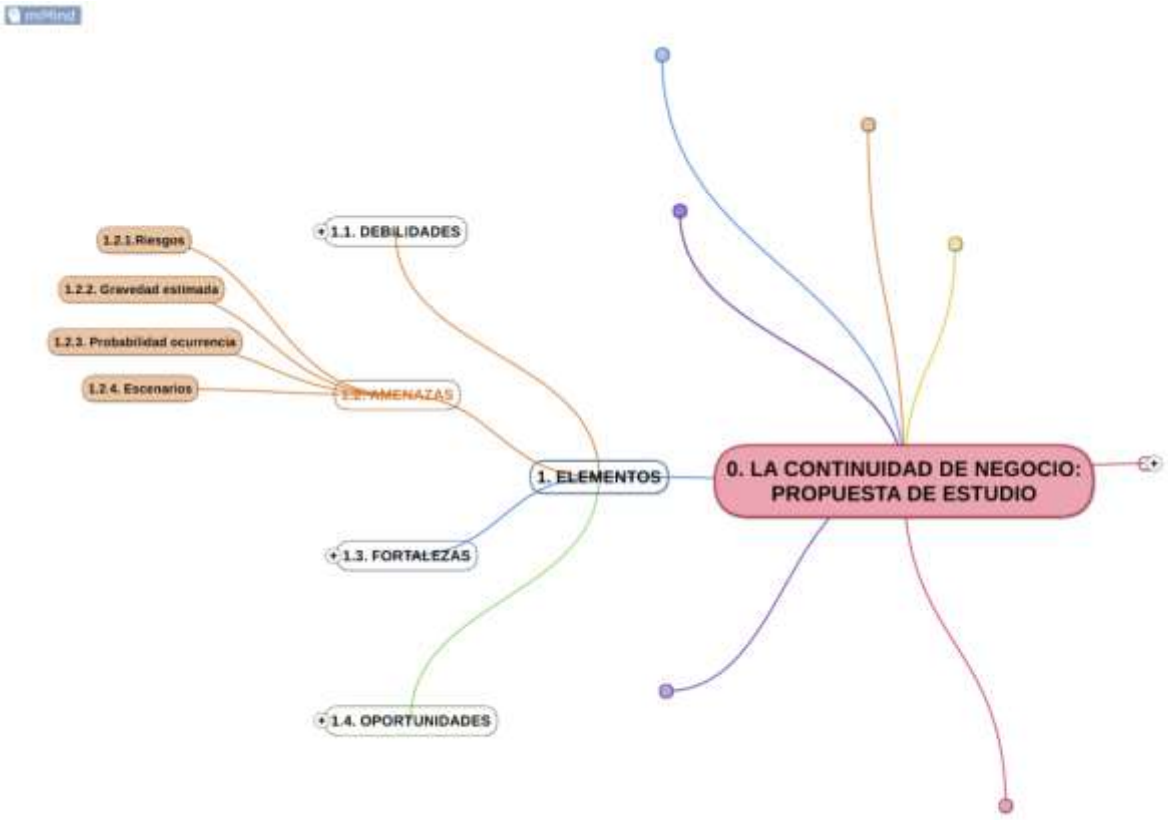
ID	PROCESOS	Talones de Aquiles	Dependencias	Personal clave	Recursos
1	**PROCESO 1**				
1a	Operación 1a				
1b	Operación 1b				
2	**PROCESO 2**				
2a	Operación 2a				
2b	Operación 2b				
2c	Etc.				
Etc.	**Etc…**				

Tabla con el mapa de procesos (estructura).

PCN 1.2. AMENAZAS

Inauguramos nueva sección, destinada a alojar la discusión de las amenazas, que equivalen a la segunda parte de un análisis DAFO. Son aquellas circunstancias del medio que pueden parar nuestros procesos. Suponen ocasiones de riesgo, actuando sobre nuestros puntos débiles. Aprenderemos a identificarlas y a clasificarlas según los escenarios en que se materializan.

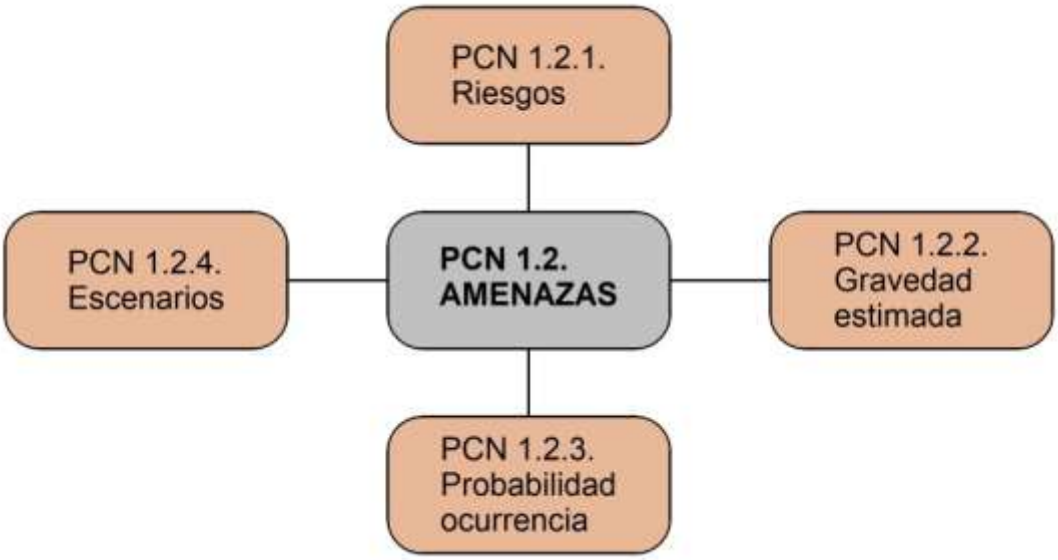
Antes de que empecemos a actuar sobre nuestros procesos para mejorar la continuidad, y una vez conocemos nuestras **debilidades**, es necesario que hagamos un inventario de aquellas fuentes añadidas de problemas sobre las que en primera impresión no tenemos capacidad de actuación, porque provienen *de fuera* y que llamamos **amenazas**.



La posición de las **amenazas** en el conjunto de estudio de la continuidad.

En esta sección veremos cómo definir las fuentes de riesgos y a clasificarlas según la **gravedad** que pueden suponer en caso de materializarse, y también según su **probabilidad**.

Además, introduciremos el concepto de **escenarios**. Todos estos conceptos que manejamos son equivalentes a los mismos conceptos que emplearíamos en el mundo real, aunque adaptados a nuestros fines. De los distintos significados que tienen nos decantaremos por el más apropiado. **La idea es ayudarnos de las palabras** y su **sentido** último. Teniendo en cuenta que las empresas y en general las organizaciones, se mueven en un mundo bastante **aleatorio**, que podemos directamente definir como **caótico**, y debido a las continuas interacciones con su ambiente, unos pocos conceptos sencillos ayudarán a hacer comprensible su comportamiento, si agrupamos acciones semejantes en el mismo nombre.



El grupo de estudio de las AMENAZAS.

Amenazas tipo

Lo primero será conocer **la naturaleza de los riesgos** y por qué suponen un problema para la vida de la organización. No es lo mismo si un riesgo es tan **grave** que puede poner en peligro el funcionamiento o la propia existencia de la empresa, que si se trata de una simple molestia que es bueno corregir. Como tampoco es lo mismo si su **frecuencia** o **probabilidad** de ocurrencia es tan alta que sucede cada vez que arrancamos el proceso o si por el contrario es tan reducida que se vuelve insignificante.

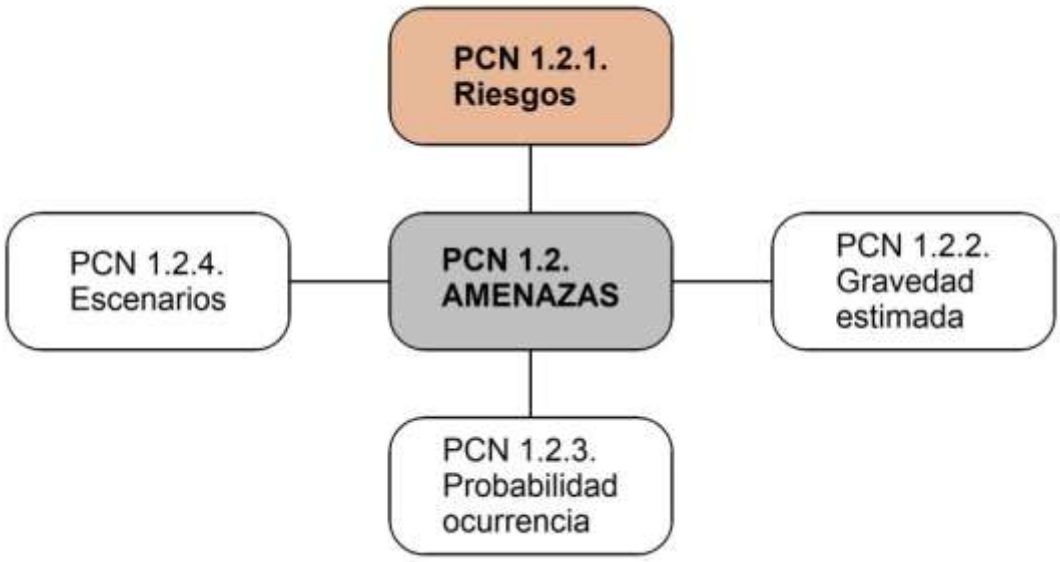
Una vez hecha **la lista** de los posibles riesgos, agruparlos de forma lógica y referirlos a debilidades concretas, los caracteriza como distintos **escenarios** en los que nos podemos ver involucrados. Por tanto, de un universo de posibilidades al principio, habremos evolucionado y aprendido lo suficiente para llegar a considerar distintas circunstancias concretas que nos permitirán fijar líneas de actuación o **estrategias** para construir nuestras **fortalezas**, o puntos fuertes de negocio, que serán objeto de PCN 1.3. FORTALEZAS. Usando las **estrategias** adecuadas podremos competir con ventaja en el mercado y aprovechar las opciones que tengamos, que llamaremos **oportunidades** y será objeto de PCN1.4. OPORTUNIDADES. Todo ello es preciso si queremos **planificar estratégicamente** nuestra organización, fijar **objetivos** y verificar los logros obtenidos, de forma explícita.

PCN 1.2.1. Riesgos

Los riesgos para nuestra organización, empresa o negocio vienen de la mano de amenazas. El principal mensaje que sacaremos en esta parte del estudio es que la más sensata actuación por nuestra parte es limitar la exposición al riesgo, manteniéndonos a salvo de las amenazas. Con esto habremos recorrido un gran trecho en términos de continuidad de negocio.

Hablamos de riesgos de forma genérica, sin prestar demasiada atención a lo que en realidad significan. La naturaleza del **riesgo** es la **incertidumbre**. La **norma UNE-EN ISO 22301**, que es la que trata del sistema de gestión de la Continuidad de Negocio, define

riesgo (risk): Efecto de la incertidumbre en los objetivos.



Los riesgos como materialización de amenazas.

Si seguimos el razonamiento de que **los riesgos son un resultado de la incertidumbre** y que para ayudar en la continuidad de nuestra actividad tenemos que **evitar la exposición al riesgo**, parece evidente que cuanto más **conocimiento** tengamos de nuestros procesos y del entorno, que limiten la **incertidumbre** sobre su comportamiento, mejor podemos garantizar la continuidad de negocio.

De aquí se deduce que necesitamos un **sistema documental**, es decir: una serie de **documentos**, que, si tienen suficiente entidad para facilitar su mantenimiento y consulta, pueden llegar a formar parte de una **base de datos documental**. Aunque no necesariamente tenga que ser algo complejo o caro, pues nos basta organizar un buen **archivo**, bien sea en papel o en ficheros informáticos. Habrá documentos que nos enseñen cómo tenemos que hacer las cosas, que llamaremos **procedimientos**, y otros documentos que guarden memoria de las comprobaciones y realizaciones efectuadas, que llamaremos **registros**. Esto es así porque los documentos son la forma más sencilla de acumular **conocimiento** que puede compartirse o emplearse como paso previo para adquirir más conocimiento. Si no tenemos escrito un procedimiento, ¿cómo podremos mejorar el procedimiento?

No hemos apenas entrado en qué hacen los riesgos, pero es fácil asumir que el **conocimiento** nos da **capacidad de predecir** en cierta forma los sucesos. Cuando

tenemos dominado un proceso, sabemos cómo se comportará, como cuando conducimos un vehículo *en condiciones de control*. El efecto de la **incertidumbre** es que **sucede algo completamente inesperado** en ese momento y entonces altera la marcha del proceso, provocando que durante un tiempo no tengamos el control.

Cuando se trata de un proceso de **producción**, la **incertidumbre** se traduce en que no sabemos si **la calidad** de lo producido se ajusta a las **especificaciones** y preventivamente habrá que desecharlo, reexaminarlo y posiblemente repararlo, con lo que se acumularán los **costes imprevistos. Si se trata de un servicio**, el cliente puede exigir el resultado que ha pagado o contratado. Casi siempre un efecto inesperado en el proceso va a suponer un **sobrecoste**, una **reclamación**, o la **pérdida de reputación**.

A efectos de conseguir emplear los recursos siempre limitados de las organizaciones o empresas, es importante poder ***categorizar los riesgos***, a fin de dedicar los recursos preferentemente en reducir la exposición a los riesgos que califiquemos como más importantes. Esta categorización, que tiene en cuenta la **gravedad** de las consecuencias y la **probabilidad** de la ocurrencia de una determinada **amenaza**, será el objeto de los dos apartados siguientes **PCN 1.2.2. Gravedad estimada** y **PCN 1.2.3. Probabilidad ocurrencia**. Al terminar los análisis indicados en dichos puntos seremos capaces de darles un **valor numérico** a los distintos riesgos.

Para empezar hay que **listar las distintas fuentes de riesgos**, igual que hicimos en el caso de la lista de procesos y sus correspondientes talones de Aquiles o puntos débiles tratados en **PCN 1.1.1. Talones de Aquiles**. Haremos aquí un **inventario de las amenazas**. A la lista de amenazas que tengamos, le añadiremos en etapas posteriores distintos atributos, en particular, la **gravedad** estimada de las consecuencias de cada una y la **probabilidad** estimada de su ocurrencia.

Listando fuentes de riesgos

Como **ejemplos** de las posibles **amenazas** o fuentes de **riesgo**, estarían las que se refirieran a problemas de **personal**, de **suministros**, de comunicación y **ciberataques** o de **cuellos de botella** que presenten nuestros procesos, así como las distintas subdivisiones de ellas. Por ejemplo:

- Personal
  - Pandemia
  - Huelga
- Suministros e instalaciones
  - Materiales
  - Energía
  - Locales
- Ciberataques
  - *Fishing*
  - Denegación de servicio
- Cuellos de botella
  - Diseño
  - Problemas de calidad
- Etcétera

En la segunda parte del libro **PCN 2. CASOS**, trataremos concretamente la forma de abordar problemas tipo de esas clases. Por ahora nos bastará tener **una lista que nos sea útil** para describir posibles **amenazas** que nos afecten a nuestro caso.

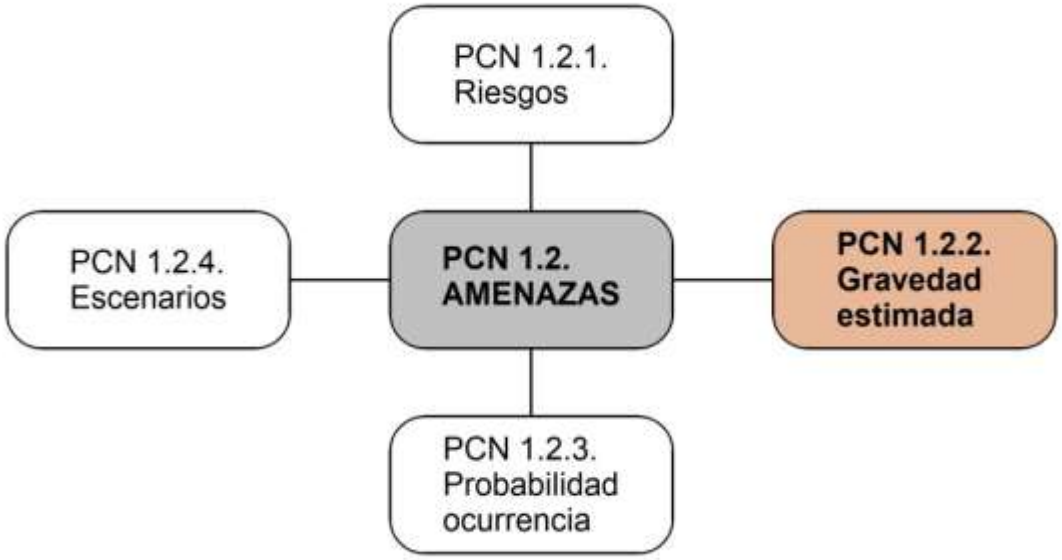
Por cierto, habéis visto que *casi confundimos* los términos **riesgo** y **amenaza**. Desde un punto de vista dinámico, de cómo ocurren las cosas,

RIESGO ES EL RESULTADO DE LA MATERIALIZACIÓN DE UNA AMENAZA.

PCN 1.2.2. Gravedad estimada

Para poder categorizar las amenazas necesitamos usar una escala de gravedad. Debe ser a la vez sencilla y práctica, fácil de entender y que permita añadir a nuestro inventario de amenazas atributos que nos orienten en las acciones prioritarias.

Suelo emplear un símil en estos casos que todo el mundo entiende: un accidente puede derivar en un arañazo o una contusión sin necesidad de ingreso en el hospital, que sería una consecuencia '**leve**' o '**menor**' (= **admisible**, aunque mejor que hubiera sido sin consecuencias); en una herida o la rotura de un hueso que sería '**grave**' o '**mayor**' (= ***inadmisible*** porque incapacita temporalmente); en conmoción con pérdida del conocimiento y daño multifuncional, con ingreso en la UCI, que sería '**crítico**' (= **peligro severo para la continuidad** de la vida del paciente).



La gravedad estimada permite categorizar las amenazas.

Ahora se trata de ponernos en situación y hacer, **para cada uno de los conceptos de la lista de amenazas que habíamos preparado en el punto anterior PCN 1.2.1. Riesgos**, una **estimación de la potencial gravedad** que se derivaría si se materializara. Hay una barrera mental para la clasificación del nivel estimado de gravedad potencial y es juzgar si un incidente determinado podría llegar a producir efectos **inadmisibles**, teniendo en cuenta nuestros **objetivos** y **presupuestos**. Un **incidente** sería **inadmisible** cuando tuviera capacidad de **incapacitar** temporalmente nuestros procesos por encima de lo que puede permitir nuestra **planificación** o **presupuestos**. Podemos también verlo como que sería inadmisible si nos hiciera **incurrir en costes** no presupuestados.

Escala de gravedad de la amenaza

- Si una amenaza potencialmente no produce ningún efecto negativo en nuestro caso, ni siquiera deberíamos considerarla. Sería **No Aplicable** (N.A.) y la calificaríamos con nivel de **gravedad '0'**.
- Si una amenaza pudiera llegar a producir daños admisibles o que tenemos previstos en nuestro presupuesto (a modo de autoseguro), sería '**menor**' y la calificaremos con nivel de **gravedad '1'**.

- Si una amenaza tuviera capacidad de producir daños inadmisibles, por encima de nuestras previsiones, sería '**mayor**' y la calificaríamos con nivel de **gravedad '2'**.
- Por último, si una amenaza pudiera ser capaz de producir daños de tal entidad que inutilizara permanentemente nuestra actividad o nos hiciera asumir costes por encima de nuestra capacidad y no pudiéramos cubrir con seguros de ninguna clase, sería '**crítica**' y la calificaríamos con nivel de **gravedad '3'**.

Esta **clasificación** es semi subjetiva y arbitraria, puesto que los valores que asignamos no guardan proporción (¿encajarían quizá mejor con una **escala logarítmica**, como los niveles de los terremotos en la **escala de Richter**?). Pero como se trata de nuestro negocio o actividad, la intuición nos orientará a otorgar el nivel adecuado para cada clase de amenaza, de forma que sea útil. Intentaremos acertar en la valoración, porque de ello se derivará la asignación de **recursos** y de **prioridades**.

¿Qué hay del **cisne negro**? Todo lo que hacemos en momentos 'de paz' sirve para estar prevenidos contra amenazas conocidas. Hay veces que se produce un acontecimiento completamente imprevisto que lo cambia todo *para mal*. Estamos preparados para prevenir y reaccionar frente a amenazas 'normales', pero no para contrarrestar incidentes totalmente inesperados. Al menos, con la preparación y la práctica que nos va a ir dando el sistema de continuidad que estamos creando, tendremos en general mejores perspectivas de supervivencia que si no hubiéramos hecho nada.

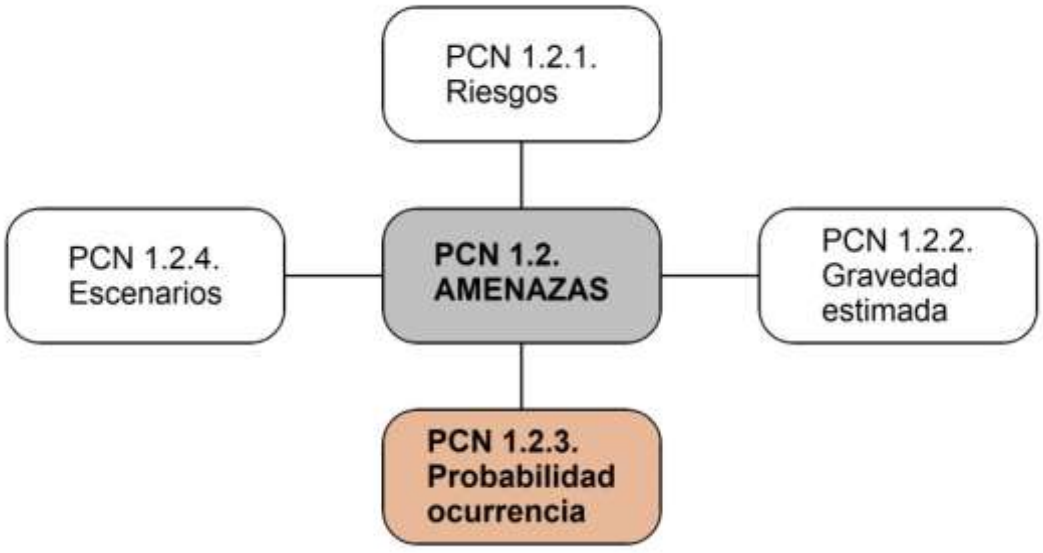
A veces, en lugar de sólo tener efectos indeseables, un incidente totalmente inesperado y disruptivo lo que hace es darnos una ventaja maravillosa sobre la competencia, porque precisamente somos buenos en lo que otros no han sido capaces de preparar, y nosotros somos precisamente los expertos en ello. Se llama **serendipia** y es la otra cara de la moneda en lo que se refiere a los fenómenos inesperados.

PCN 1.2.3. Probabilidad de ocurrencia

Las amenazas pueden calificarse también por su probabilidad de ocurrencia. Ante dos riesgos del mismo poder de distorsión de nuestros procesos, habrá que ocuparse con preferencia de aquel que pueda ocurrir más frecuentemente.

Igual que hemos hecho con la gravedad estimada del riesgo provocado por una amenaza en el punto anterior, haremos ahora lo mismo con su probabilidad de ocurrencia. Aplicaremos los datos conocidos, y si no los tenemos haremos una estimación subjetiva, para hacer una valoración numérica de su probabilidad, que cubra posibles incidentes **muy poco probables**, **repetitivos** y **continuos**, y nos conduzca a decisiones operativas.

De nuevo optaremos por emplear una forma sencilla de clasificación de probabilidad, siguiendo el mismo ejemplo de un accidente. La **probabilidad de ocurrencia** si históricamente ha habido alguna ocasión aislada sería '**leve**' o '**menor**' (= ***admisible***, porque ¿quién no ha tenido en su vida un accidente?); en caso de que pueda ocurrir en cualquier momento sería '**grave**' o '**mayor**' (= **inadmisible** porque indicaría que no siempre se tiene el control); cuando se ha perdido completamente el control y un incidente puede ocurrir (casi) siempre, tenemos una probabilidad '**crítica**' (=**riesgo severo para la continuidad** de la vida del paciente).



La probabilidad de ocurrencia aporta un nuevo matiz aplicable a las amenazas.

Volveremos a tomar **la lista de amenazas que habíamos preparado en el punto anterior** **PCN 1.2.1. Riesgos**, y, **para cada uno de los conceptos** anotados, haremos una **estimación de la probabilidad estimada de su ocurrencia** y la agregaremos al registro de dicha amenaza en la lista.

Nivel de probabilidad

Para cada proceso o instalación sabemos que puede ocurrir una cierta frecuencia de fallos que consideraríamos **admisible**. De la misma manera tenemos claro que una determinada frecuencia de interrupciones es **inadmisible**, teniendo en cuenta nuestros **objetivos** y **presupuestos**. Un **incidente** tendría una frecuencia de ocurrencia **inadmisible** cuando tuviera capacidad de **incapacitar** temporalmente

nuestros procesos por encima de lo que puede permitir nuestra **planificación** o **presupuestos**. Podemos también verlo como que sería inadmisible si nos hiciera **incurrir en costes** no presupuestados.

- Si una amenaza no tiene ninguna probabilidad de ocurrir, nunca produce ningún efecto negativo en nuestro caso, ni siquiera deberíamos considerarla. Sería **No Aplicable** (N.A.) y la calificaríamos con nivel de **probabilidad '0'**.
- Si una amenaza pudiera ocurrir naturalmente en un nivel de frecuencia muy bajo que tenemos previsto en nuestro presupuesto (a modo de autoseguro), sería '**menor**' y la calificaremos con nivel de **probabilidad '1'**.
- Si una amenaza pudiera ocurrir con una frecuencia **inadmisible**, por encima de nuestras previsiones, sería '**mayor**' y la calificaríamos con nivel de **probabilidad '2'**.
- Por último si una amenaza pudiera ocurrir siempre por una situación anormal, avería, mal funcionamiento incontrolado inutilizando de hecho permanentemente nuestra actividad o nos hiciera asumir costes por encima de nuestra capacidad y no pudiéramos cubrir con seguros de ninguna clase, sería '**crítica**' y la calificaríamos con nivel de **probabilidad '3'**.

De nuevo, igual que ocurría con la cuestión de la gravedad, esta **clasificación** es semi subjetiva y arbitraria, puesto que los valores que asignamos no guardan proporción (Recordemos lo que dijimos de una **escala logarítmica**, que se usa para definir los niveles de los terremotos en la **escala de Richter**). Pero como se trata de nuestro negocio o actividad, la intuición nos orientará a otorgar el nivel adecuado para cada clase de amenaza, de forma que sea útil. Intentaremos acertar en la valoración, porque de ello se derivará la asignación de **recursos** y de **prioridades**.

En el siguiente punto veremos cómo combinar ambos conceptos: gravedad y probabilidad y cómo entra en escena nuestra particular escala de Richter para las amenazas, que tiene valores para calificar riesgos que también nos parecerán familiares.

PCN 1.2.4. Escenarios

Los escenarios son situaciones de amenazas que pueden afectar a distintas partes de nuestros procesos. Nos interesa su estudio porque nos permite sistematizar todo el trabajo de defensa de nuestros procesos y de gestión de crisis.

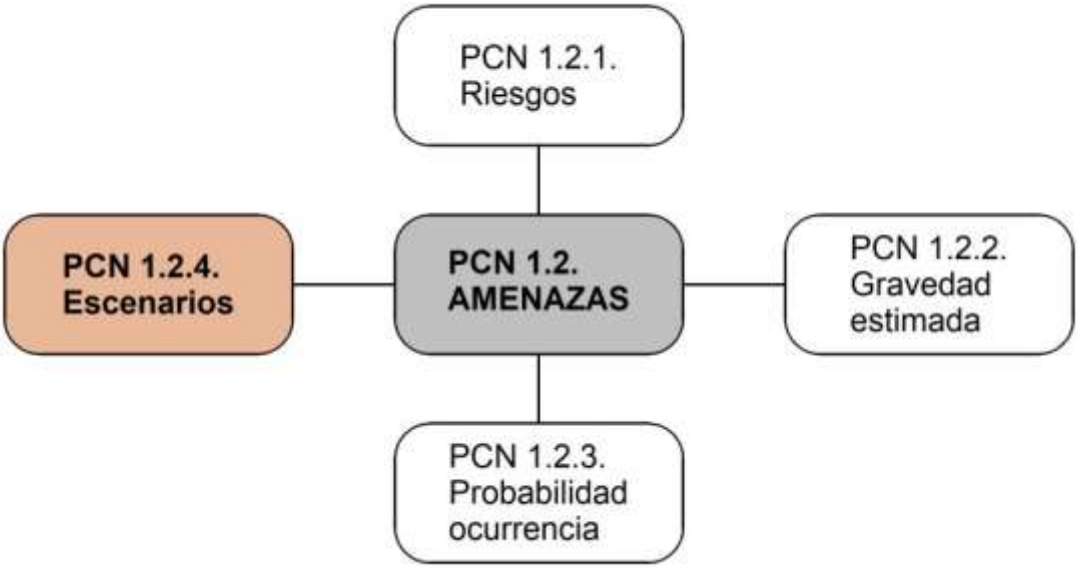
Retomamos todo el trabajo realizado según **PCN 1.2.2. Gravedad estimada** y **PCN 1.2.3. Probabilidad de ocurrencia** en lo que supone de calificación de las distintas **amenazas** o fuentes de **riesgo**.

En el punto anterior a los mencionados, **PCN 1.2.1 Riesgos**, dábamos **ejemplos** de las posibles **amenazas** o fuentes de **riesgo** que nos han servido de base en la descripción:

- Personal
  - Pandemia
  - Huelga
- Suministros e instalaciones
  - Materiales
  - Energía
  - Locales
- Ciberataques
  - *Fishing*
  - Denegación de servicio
- Cuellos de botella
  - Diseño
  - Problemas de calidad
- Etcétera

Lo que consideramos anteriormente como posibles **fuentes de riesgo**, los orígenes de las amenazas, **aplicadas a los puntos que consideramos debilidades** son lo que llamamos **escenarios**. Por ejemplo, un escenario sería la falta de suministros clave de nuestros procesos, sin los cuales tenemos que detener la actividad, como puede ser la falta de suministro eléctrico, que nos obliga a tener los ordenadores parados.

Por extensión, como la **lista de posibles amenazas** para nuestros procesos ya la elaboramos pensando en nuestra situación en particular, esa misma lista o inventario **nos servirá de lista de posibles escenarios**.



Establecer escenarios es la continuación de inventariar riesgos y establecer su gravedad y su frecuencia.

Veamos ahora una manera de **clasificar los riesgos de distintos escenarios por gravedad y probabilidad**: ya habíamos anunciado que los riesgos podíamos clasificarlos en función de la estimación de su gravedad y de la estimación de su probabilidad de ocurrencia. En el cuadro que veremos a continuación hacemos una lista de tres niveles de gravedad (en tres filas) y tres niveles de probabilidad (en tres columnas). **En cada casilla** correspondiente a cada nivel de gravedad y cada nivel de probabilidad **multiplicamos sus respectivos valores de gravedad por probabilidad**. El resultado son **nueve niveles de Escala de Riesgo** (del 1 al 9, aunque falten el 5, el 7 y el 8), **que van del 1 al 9**, que por motivos **mnemotécnicos** podemos asimilar a la **Escala de Richter** de los terremotos.

ESCALA DE RIESGO (= Gravedad*Probabilidad)	Probabilidad 1	Probabilidad 2	Probabilidad 3
Gravedad 1	1*1 = 1	1*2 = 2	1*3 = 3
Gravedad 2	2*1 = 2	2*2 = 4	2*3 = 6
Gravedad 3	3*1 = 3	3*2 = 6	3*3 = 9

Cuadro de Escala de Riesgo.

Podemos incluso **definir (arbitrariamente)**, ahora que tenemos un valor único para los riesgos considerados, que

- **Riesgo bajo = niveles 1 y 2** (en la tabla tonos de **verde**)
- **Riesgo medio y alto = niveles 3 y 4** (en la tabla tonos de **amarillo**)
- **Riesgo crítico = niveles de 5 para arriba** (en la tabla tonos de **naranja y rojo**)

Este **mapa de calor** que hemos construido nos lo encontraremos frecuentemente en la literatura del tema y ayuda a visualizar rápida e intuitivamente dónde está el problema.

Ahora podemos **completar nuestro catálogo de escenarios** con los valores de los riesgos que tienen asociados en este cuadro, asignando a cada uno de los escenarios de riesgo el valor resultante del producto de su gravedad por su probabilidad. **Ejemplo de tabla de escenarios detallados y su escala de riesgos resultante**. Esta sería una

primera **valoración inicial**. Los datos consignados son *no exhaustivos, totalmente imaginarios y solo sirven para explicar los contenidos*:

Catálogo de escenarios

CONCEPTO	Gravedad	Probabilidad	Escala
PERSONAL	---	---	>>> **4** (alto)
Pandemia	2	2	**4**
Huelga	2	1	2
SUMINISTROS E INSTALACIONES	---	---	>>> **3** (medio)
Materiales	2	1	2
Energía	3	1	**3**
Locales	3	1	**3**
CIBERATAQUES	---	---	>>> **6** (crítico)
Fishing	2	2	4
Denegación de servicio	3	2	**6**
CUELLOS DE BOTELLA	---	---	>>> **2** (bajo)
Diseño	1	1	1
Problemas de calidad	2	1	**2**

Tabla de escenarios, valorados (ejemplo no exhaustivo e imaginario, para explicar los contenidos del texto).

Puede que no parezca gran cosa, pero **hemos definido una escala de escenarios calificados según valores numéricos de sus riesgos y ya se ve a simple vista cuáles deberán ser las prioridades de actuación**, a fin de controlar la situación.

En este ejemplo, tenemos la calificación más alta para los **riesgos de ciberataque** (6 en nuestra particular escala de riesgos –si fuera un terremoto de nivel 6 podría producir daños notables en las infraestructuras) y luego viene la clasificación de riesgos que afectan al personal clave (4 en la misma escala –que es grave, pero no tanto).

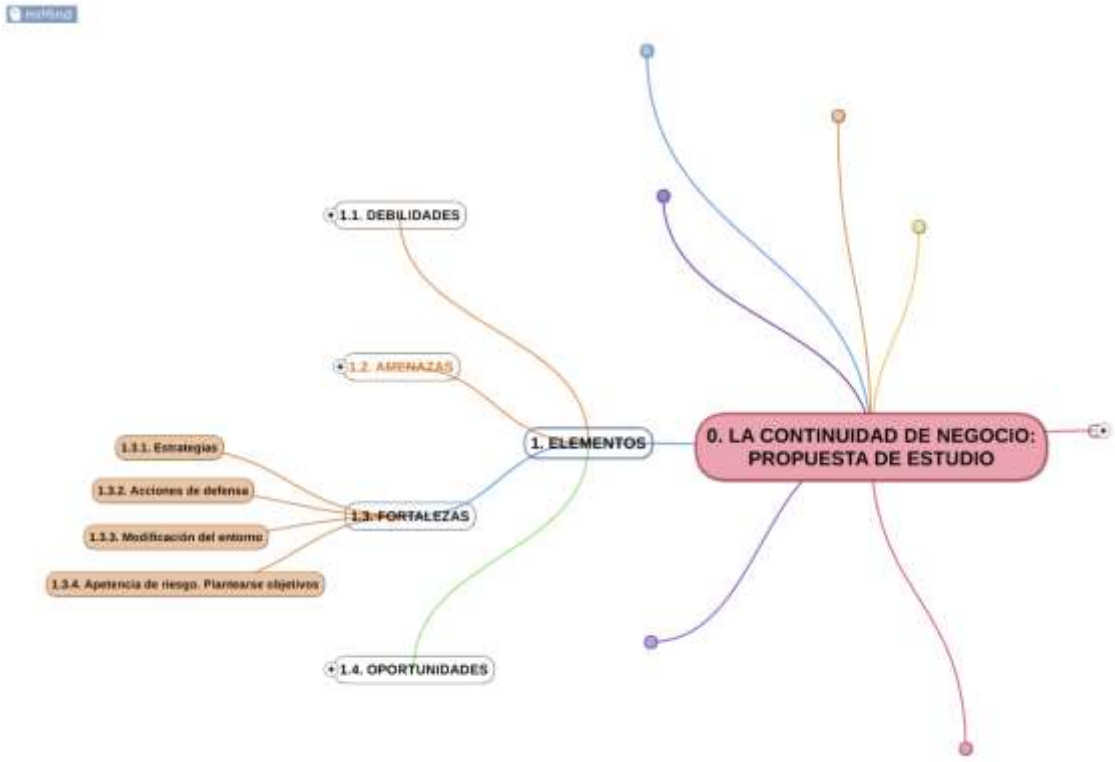
Tomo para **el valor de la escala de riesgo de un conjunto** de escenarios como **el más alto entre todos sus elementos**. Por ejemplo, para 'PERSONAL' 4 (alto) tomo la escala de 'Pandemia' 4, no la de 'Huelga' 2, o para 'CIBERATAQUES' 6 (crítico) la de 'Denegación de servicio' que afecta a los servidores de toda la compañía, no la de '*Fishing*' 4 que casi seguro afecta a cuentas personales individuales de los empleados).

En un próximo punto **PCN 1.3.1. Estrategias**, como parte de las **fortalezas** de nuestro sistema de gestión, empezaremos, por fin, a entrar en acción, después de todos los análisis que hemos realizado hasta aquí.

PCN 1.3 FORTALEZAS

Vamos a abordar el tercer bloque de un análisis DAFO en el que ya hemos analizado las debilidades y las amenazas. Ahora empezamos con el estudio de las fortalezas. Se trata de todo lo que tenemos a nuestro alcance para reforzar nuestros puntos débiles y afrontar los riesgos. Básicamente, las fortalezas son una suma de conocimiento y determinación.

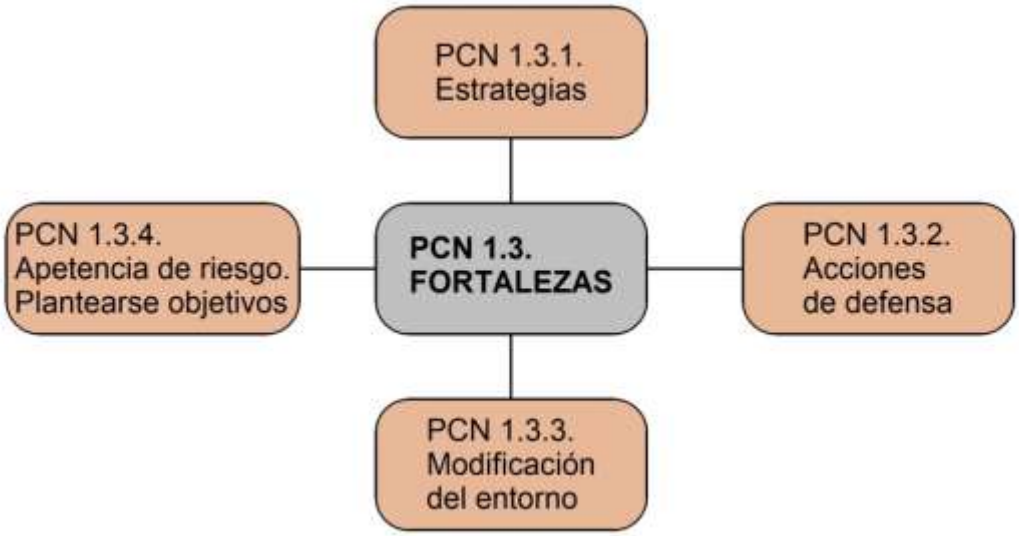
Con todo lo avanzado en los estudios efectuados anteriormente, estamos preparados para una actuación más dinámica, **planificando** cuál será nuestra línea de actuación como grupo a fin de fortificar nuestros procesos. Ya vamos teniendo claro que la base de cualquier actuación práctica es **el conocimiento** porque lo que hemos hecho hasta ahora es anotar lo que sabemos de nuestros procesos (debilidades y amenazas). Hacer **planes** previendo cuáles pueden ser los problemas que nos pueden resultar más dañinos o pueden tener más probabilidad de ocurrir hará que aumenten nuestras fortalezas. Este bloque nos mostrará la forma de enfocar los esfuerzos de un modo ordenada, basándonos en el conocimiento que se basa en la lista de **escenarios** que hemos preparado y valorado en el punto anterior **PCN 1.2.4. Escenarios**.



Tras controlar los aspectos negativos de nuestros procesos, empezamos ahora con las fortalezas los positivos.

Gracias al trabajo previo ya hemos identificado como **escenarios**, de entre los posibles **riesgos** que pueden comprometer la actividad en nuestros puntos más débiles, aquellos riesgos sobre los que resulta más interesante o prioritario actuar, porque tienen un valor de gravedad y probabilidad de ocurrencia combinados mayor. Ahora trabajaremos con las **estrategias**, pensadas para cada uno de dichos escenarios, teniendo en mente si lo que nos interesa es simplemente mejorar nuestra **resistencia** frente a los riesgos (lo que viene siendo la **resiliencia**), o si por el contrario planeamos actuar en caso de incidentes que pueden atacar masivamente a todo el sector en el

que trabajamos, de tal forma que **no sólo resistamos a los incidentes, sino que tomemos una ventaja sustancial sobre la competencia** (es decir, volvernos "**antifrágiles**" – concepto acuñado por **Nassim Nicholas Taleb** en su **libro del mismo nombre, 'Antifrágil' que ya tuvimos la ocasión de comentar en el blog unoydostres.com**–).



Grupo de estudio de las fortalezas.

Fortalezas tipo

Para ello analizaremos qué podemos esperar de las **estrategias**, cómo plantear las mejores **acciones de defensa** de nuestros procesos, dar un paso más y no quedarnos pasivamente a esperar ser arrollados por la inundación (figuradamente), sino que las defensas levantadas aprovechen la fuerza de las aguas (figuradas) en nuestro beneficio, **modificando nuestro entorno**. Un análisis más fino nos llevará a considerar hasta qué punto nos queremos proteger o más bien deseamos que las aguas se muevan (también de nuevo figuradamente) hasta cierto punto, planteando cuál es nuestra **apetencia de riesgo** (o sea, cómo de bien afianzados tenemos nuestros procesos, o cuan bien *flotamos* sobre los problemas). Completaremos nuestra acción **planificando objetivos** de acciones permanentes para **reducir la exposición al riesgo**, bien actuando sobre causas que **quitarían gravedad** a los daños o actuando sobre causas que **reducirían la probabilidad** de sufrir los riesgos que tenemos identificados.

Todo ello sin perder de vista que si sucede un **cisne negro**, o sea un *suceso inesperado de suficiente entidad para el que específicamente no hemos podido identificar la estrategia adecuada ni tenemos líneas de defensa, ni hemos podido mejorar nuestra posición en el entorno*, por lo menos tengamos suficiente práctica en **organizarnos** y estemos acostumbrados a **tomar decisiones eficaces** con suficiente rapidez, improvisando de la mejor manera que somos capaces para **gestionar la crisis**. En general no hay dos **crisis** iguales, pero suelen ser una **combinación de varias circunstancias**, para las que en algunas tomadas individualmente tendríamos remedios. Cuanto más conocimiento y experiencia de cómo lidiar con ellas, mejor parados podremos salir. Lo iremos viendo en apartados sucesivos.

No sólo eso: en caso de crisis es conveniente no dejarse guiar ciegamente por una ideología o prejuicios e ideas preconcebidas, sino que es mejor analizar y actuar en cada momento después de calibrar las **opciones** disponibles, de la forma que mejor se potencien nuestras posibilidades de éxito, incluidas las ventajas relativas que podríamos lograr frente a nuestros competidores.

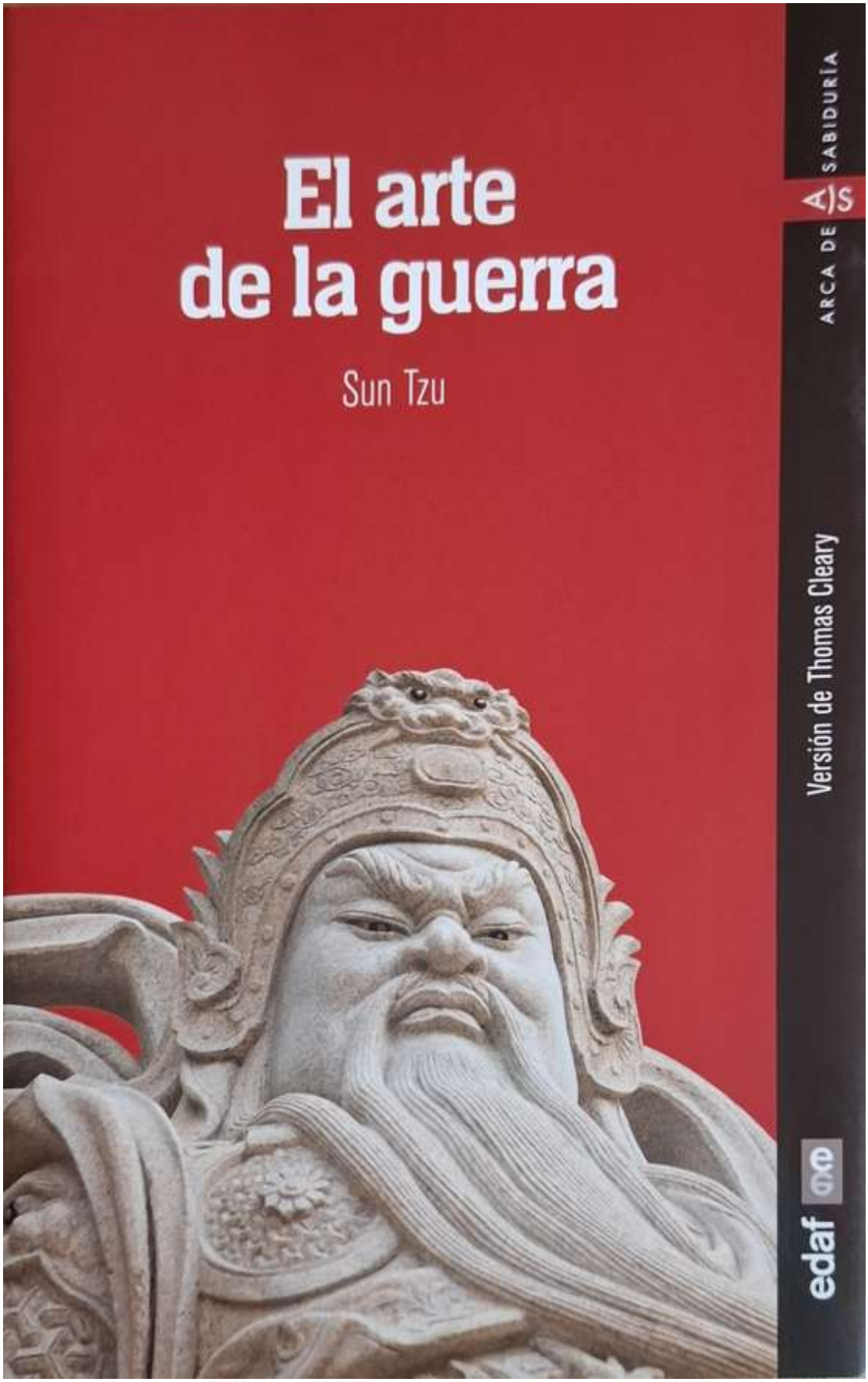
PCN 1.3.1. Estrategias

El término *estrategia* suena a teoría militar. Sin embargo, se ha generalizado a todos los ámbitos de la organización, tanto para la parte financiera, como de operaciones, la comercial, etc. Nosotros emplearemos este concepto para definir las líneas maestras de nuestra actuación en diferentes escenarios.

Para empezar, hay que distinguir entre **estrategia** y **táctica**. La **estrategia** está más ligada a **los objetivos y las intenciones** y la **táctica** a la **forma concreta** de obtener dichos objetivos mediante acciones prácticas. En un sistema de gestión, las **estrategias** marcarían las líneas generales de actuación en **documentos o procedimientos de alto nivel** y la **táctica** sería tratada en otros documentos que podemos llamar **procedimientos operativos**, fijando las actuaciones a realizar en cada proceso como forma de llevar a la práctica la estrategia elegida. Ambos conceptos proceden del ámbito militar, pero como *la lucha contra el mal* es también una clase de guerra, vienen al caso.

El arte de la guerra de Sun Tzu es un texto de referencia. **En este enlace** "25 Leyes de la Estrategia según Sun Tzu", se puede ver un resumen bastante bueno del libro. Una idea básica que impregna el texto de Sun Tzu es que es mejor ganar la guerra sin pelear, para lo que es imprescindible una preparación adecuada y exhaustiva antes de tener que llegar a la batalla.

La versión de la editorial EDAF, traducida por Thomas Cleary, comentada, es muy recomendable para meditar sobre su contenido y extraer enseñanzas que tienen aún validez para el mundo actual.



Sun Tzu, *El arte de la guerra,* EDAF (2020). Magnífica 8ª edición comentada. Fotografía de la cubierta.

.

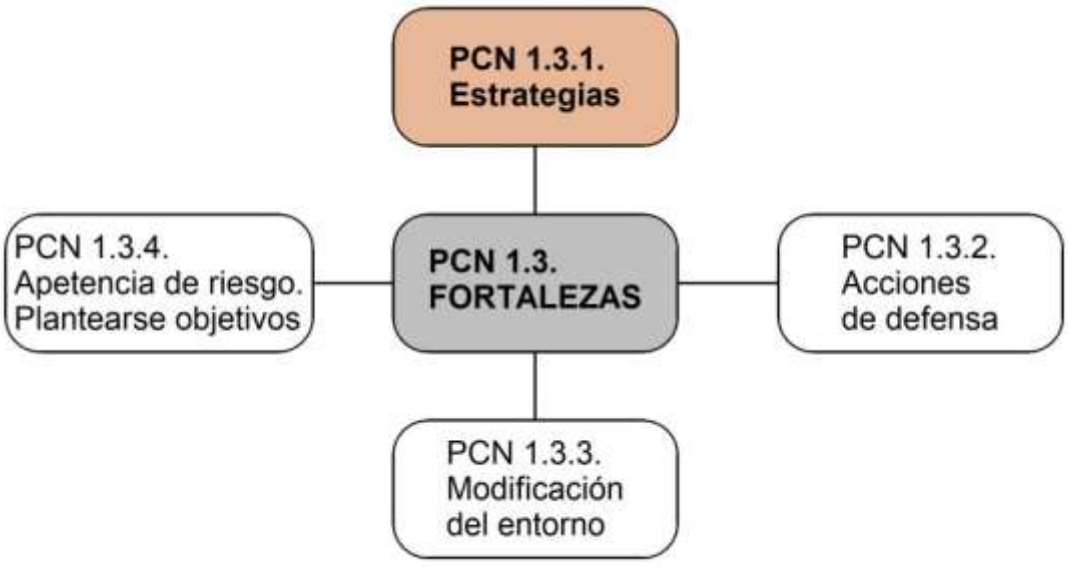
En cuanto a la **estrategia**, básicamente hay dos clases: estrategia **de vencedor** y estrategia **de perdedor**. Si todo lo que planeamos tiene que ver solo con defendernos, no tenemos confianza suficiente para tomar la iniciativa y en ese caso nos conformamos con un 'empate'; **somos perdedores**. Pero si la estrategia incluye actuaciones para **modificar las condiciones del entorno**, con el fin de **anticiparnos** a posibles efectos adversos y trabajamos también en **objetivos** para diseñar cómo será **el día después** de los posibles incidentes, avanzando en nuestra evolución y **crecimiento**, casi seguro que **nuestra estrategia es de vencedor**. Por cierto: la estrategia es **pública.** Supone **una declaración de hasta dónde** pretendemos llegar, sólo que no diremos (aún) cómo. Las empresas y organizaciones suelen publicar sus estrategias como parte de los documentos de **políticas** o de **responsabilidad social corporativa** para general conocimiento. Van *marcando el territorio,* que luego reivindicarán como propio.

Pero en cuanto a **la táctica** para aplicar la estrategia, los principios a emplear siguen siendo válidos los de la doctrina militar y afectan a todas las acciones. En este momento, **en España**, es muy interesante conocer los principios fijados por el Ministerio de Defensa en el documento "**Doctrina para el empleo de las FAS**".

Si queremos resumir los principios básicos de toda acción o *táctica militar* serían **VOLUNTAD, OPCIONES y MEDIOS**.

Se puede consultar también otro interesante documento, del Coronel de Infantería, **Salvador Fontenla Ballesta**: "**Un concepto de Acción conjunta**". Estos documentos de doctrina de Defensa, como otros que aparecen en Google con una simple búsqueda, todos apuntan a la bondad de aunar esfuerzos para vencer cualquier dificultad.

Evidentemente, en caso de acciones cuyo objetivo es superar a un adversario o enemigo, podremos descubrir nuestra estrategia, pero no daremos indicación ninguna sobre las acciones concretas que vayamos a realizar, que deben ser *secretas*. Si se dejan descubrir, posiblemente se trate de una treta para sacar partido de la desinformación.



Las estrategias como parte esencial de nuestras fortalezas.

Estrategias para distintos escenarios

Veamos cómo pueden ser las estrategias básicas para los cuatro escenarios tipo o ejemplo (totalmente imaginarios) que hemos elegido. Tomemos nuestra **tabla de escenarios** de **PCN 1.2.4. Escenarios**, y **añadamos una columna** en la que diremos en pocas palabras lo que serán nuestras **estrategias** para los cuatro escenarios que hemos contemplado. Añadiremos **otra columna** para explicar el presunto **efecto que pretendemos lograr**. Lo que queremos es rebajar el nivel de riesgo inicial que hemos consignado mediante, o bien reducir la gravedad de los incidentes que afecten a cada activo, o bien reducir la probabilidad de ocurrencia, o ambas cosas a la vez.

Ponemos aquí una versión reducida de dicha tabla con datos imaginarios al único fin de aclarar los contenidos. Evidentemente esto es una simplificación y en el documento real debe haber un poco más de detalle, pero tampoco mucho más si queremos que se comprenda y sirva.

CONCEPTO	Grave-dad	Proba-bilidad	Escala inicial	Estrategias	Efectos buscados
PERSONAL	---2	---2	>>> **4** (alto)	-Potenciar salud laboral e higiene -Equipos multidisciplinares -Guardias -Teletrabajo -Portal de empleo	Actuar sobre la gravedad, teniendo más personal formado o disponible en reserva y reducir la probabilidad de que afecte a porcentaje alto de plantilla
SUMINISTROS E INSTALA-CIONES	---3	---1	>>> **3** (medio)	-Proveedores alternativos -Aumento de existencias -Modificación del proceso	Reducir la gravedad del impacto de falta temporal de suministro mediante aumento de fuentes de suministro, aumento de stock y mejora del proceso
CIBERATA-QUES	---3	---2	>>> **6** (crítico)	-Mejora de la vigilancia y defensas -Copias de seguridad -Virtualización -Rápida actualización -Buenas prácticas	Mejorando las copias, la redundancia y la virtualización, los datos estarán a salvo yse reducirá la gravedad. Con la mejora de las defensas, la rápida actualización y las buenas prácticas se reducirá la probabilidad de ataque
CUELLOS DE BOTELLA	---2	---1	>>> **2** (bajo)	-Mejora del diseño del producto y proceso -Programación adecuada -Mejora de la formación	El adecuado diseño y programación convergen en la reducción de la gravedad de los incidentes y la mejora de la formación en la reducción de su probabilidad

Tabla de estrategias para distintos escenarios.

Podemos observar que, aunque se dice ***qué* se pretende**, no se aclara ***cómo* se va a conseguir** cada uno de los objetivos. Porque estamos hablando de **estrategias**. Esos *cómo* son los que se deben tratar como **documentos operativos o tácticos** a disposición de los técnicos y responsables de los procesos, siguiendo las doctrinas

presentadas arriba: con **VOLUNTAD** de vencer o determinación; asegurando la libertad de acción o sea siendo realistas con las **OPCIONES**; y aplicando los **MEDIOS** que resulten *razonables* para lograr los objetivos, *sin exagerar* (como dice un refrán español, "*no sea que cueste más el collar que el perro*" o que estemos "*matando pulgas a cañonazos*").

PCN 1.3.2. Acciones de defensa

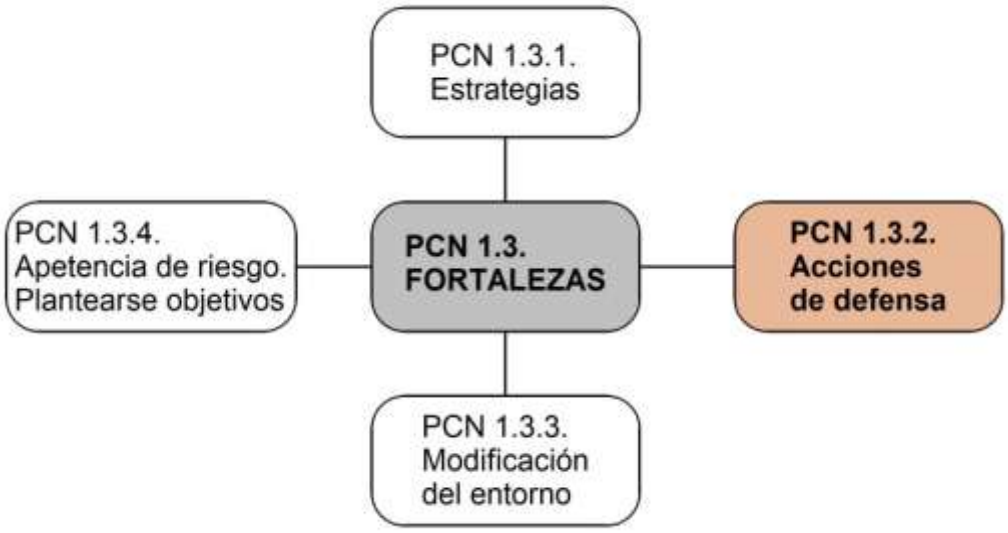
Las acciones de defensa suelen basarse en proteger nuestras debilidades, estableciendo mecanismos de vigilancia o control, definiendo umbrales de cambio de situación de '*normal*' a distintos niveles de '*incidente o crisis*', movilizando eficazmente nuestros recursos clave, estableciendo medidas efectivas para disipar o amortiguar los daños del incidente y fomentar la diversificación y transmisión del conocimiento.

La mejor **defensa** se puede lograr con una **organización en capas**, que una amenaza tendría que superar antes de llegar a afectar de verdad a nuestros procesos. Vamos a ver qué podemos hacer en cada una de esas capas, de 'fuera' a 'dentro' de nuestros procesos, siguiendo una secuencia lógica:

- Establecer **mecanismos de vigilancia**: para los distintos activos se trata de mecanismos distintos, por ejemplo, hacer un seguimiento como se indica a continuación:
    - Para personas, análisis de **salud** y del estado de la **prevención de riesgos laborales**, seguimiento de si están establecidas y se respetan las **carreras profesionales**, fomento de la **formación** y transmisión de **conocimiento** –> Con ello se mejora la salud y la satisfacción laboral, se mejora la capacitación y se reduce el **absentismo**.
    - Para los locales, controles de **acceso** y de presencia, de forma que sólo puedan acceder a los locales de trabajo las personas autorizadas y durante el tiempo establecido; **sensores** de temperatura, detección de humos, cámaras de **vigilancia** –> Con ello evitamos incendios, inundaciones, nos informamos de averías y evitamos que haya intrusiones o que personas ajenas puedan conocer detalles privados de nuestra organización.
    - Para las máquinas informáticas, control de **acceso a sistemas** y **aseguramiento de buenas prácticas** de uso, detección de tráfico anormal y niveles anormales de **actividad** de los ordenadores, detección de ***malware*** e intentos de intrusión, estado de las **actualizaciones** y ***backups*** –> Evitamos ciberataques y pérdida de datos.
    - Para los suministros, **niveles** de almacenamiento, **regularidad** de los suministros, **solvencia** de los proveedores –> Evitamos paradas por rotura de *stocks*.
- Definir **umbrales** de situaciones 'normal', 'incidente', 'crisis' para los distintos activos vigilados:
    - **Normal**: todo funciona correctamente
    - **Incidente**: hay algún problema, interrupción o avería, pero se tiene claro que su gravedad es baja y no afectará a la facturación ni a los costes presupuestados.
    - **Crisis**: el incidente se agrava y afectará a la facturación, a los costes y a los plazos de entrega o finalización que serán por encima de lo comprometido, produciendo uno o más **incumplimientos**.
    - **Catástrofe**: se trata de una crisis en que además se han producido daños en el personal o en las instalaciones que requerirán tiempo importante para resolverse y una cantidad económica importante.
- **Definir cómo movilizar** recursos clave: **en caso de que se superen los umbrales** establecidos y se llegue a un incidente grave tenemos que estar en disposición de convocar y emplear eficazmente todos aquellos recursos que

pueden contribuir a que los tiempos de interrupción y los costes globales del incidente estén contenidos. Ya veremos de ampliar este punto más adelante en **PCN 2.1.1. Alarmas: guardias y mecanismos de contacto**.

- **Establecer** medidas para actuar en la **gestión de la crisis** y para **recuperar** los procesos tras un incidente, según su estado: trataremos en detalle este punto en **PCN 2.1.4. Gestión de crisis y recuperación**. Estas medidas no serán nunca "milagrosas" ya que no se pueden prever todas las circunstancias que pueden darse en una crisis, pero servirán para poder **improvisar** con más soltura y mejores resultados, que sólo la práctica y la experiencia podrá facilitarnos.
- Fomentar la **diversificación** y la transmisión del **conocimiento**, con lo aprendido por la experiencia: estas medidas pasivas llevadas a cabo como **lecciones aprendidas**, son un clásico de la gestión. Muchas empresas se han podido salvar si los clientes han perdido el interés por alguno de sus productos cuando han sido capaces de suministrar **algo distinto** que ha seguido teniendo acogida. A veces esto solo se visualiza tras una crisis. También pasa con los productos que se introducen como consecuencia de un hallazgo inesperado o **serendipia**, de la que ya hemos hablado antes. En cuanto al **conocimiento**, despreciar en aras de *la modernidad* los conocimientos de los empleados más experimentados, que hayan sido capaces de salvar la entidad en situaciones comprometidas, es una especie de suicidio a cámara lenta.



Las acciones de defensa mejoran nuestras fortalezas, siguiendo las estrategias corporativas.

Gestión de proyectos

Para **implantar las acciones de defensa** que estimemos oportunas de forma sistemática, lo mejor es emplear un método de **gestión de proyectos**, con su planificación en el tiempo, designación de responsables, presupuestos y asignación de recursos, diario de las acciones que se van acometiendo, de tal forma que quede perfectamente documentado el proceso.

Este punto es complementario de todo lo que vimos en la primera parte del libro, dedicada a debilidades. Clasificábamos las debilidades en cuatro tipos principales:

- Talones de Aquiles
- Dependencias
- Personal clave

- Recursos necesarios

Tras haber fijado nuestras líneas de defensa, hagamos todavía como **segunda vuelta**, basándonos en nuestro registro, inventario o **mapa de procesos** (ver estructura de dicho inventario en **PCN 1.1.4 Recursos necesarios**), haciendo un **balance** mental de si lo dispuesto para prepararnos ante un incidente que afecte a alguna de nuestras debilidades fuera aún insuficiente. Si eso es así, deberíamos añadir nuevas acciones a nuestra gestión de proyectos para abordar las **vulnerabilidades aún no cubiertas**, de forma que se puedan llegar a corregir, antes de que sea tarde. No nos tiene que importar ser reiterativos, si con ello minimizamos los peligros para la entidad.

PCN 1.3.3. Modificación del entorno

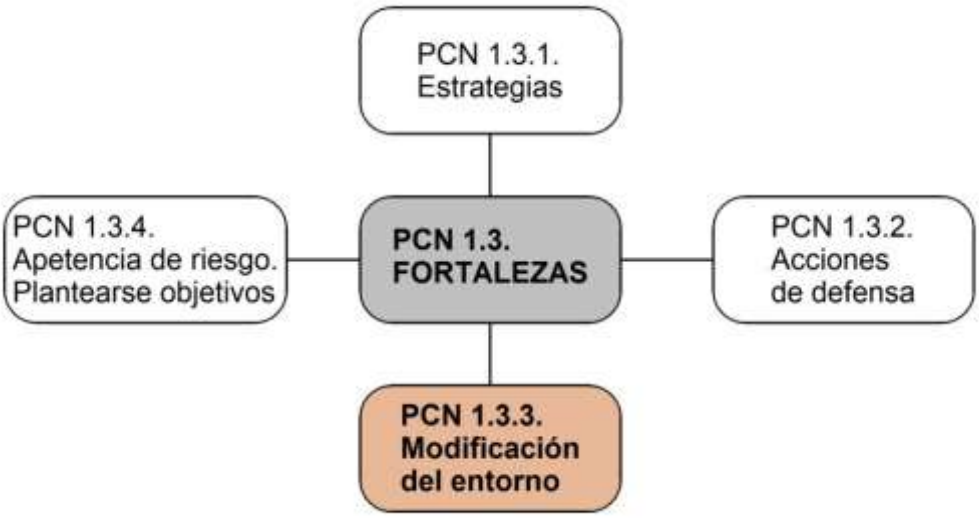
La modificación del entorno supone *actuar sobre las amenazas y sus efectos*, anticipándonos, para hacer que estas no tengan impactos tan dañinos sobre nuestros procesos. Para ello conseguiremos que el ámbito legal nos proteja y el contractual sea justo, tendremos una política de responsabilidad que ensalce nuestra imagen y reputación y mejoraremos la calidad y el cumplimiento para no perjudicar a nuestros grupos de interés en su operativa.

Si vemos la situación desde un punto de vista objetivo, no vamos a cambiar **el mundo** y las amenazas seguirán siendo aleatorias e incontrolables. Pero si que podemos cambiar **nuestro entorno**, controlando las cuestiones que nos pueden suponer un **impacto** en nuestro negocio en caso de incumplimiento, o sea de funcionamiento **inaceptable** debido a falta de calidad o de rendimiento. Aunque las fuentes de riesgo están ligadas a distintos escenarios, **los efectos** de una falta de continuidad de nuestro negocio casi siempre se traducen en **costes económicos por incumplimiento** de las leyes y reglamentos (multas); incumplimiento de las condiciones del contrato (penalizaciones); costes de imagen para mejorar la reputación (ofertas y reducciones de nuestros precios, campañas de *marketing*); costes de demandas de clientes (indemnizaciones).

En este contexto nuestra **línea de actuación** es **tratar todas esas dimensiones de impacto** sobre las que si que tenemos margen:

Rediseñando el entorno

- Eligiendo una **localización** en que las leyes y reglamentos sean más favorables a nuestros fines.
    - Buscar el mejor ambiente de **seguridad jurídica**.
    - Elegir un emplazamiento donde se garantice nuestra **seguridad física** frente a desastres naturales o frente a la delincuencia, con medidas adecuadas.
    - Asegurarnos de que cumplimos todas las **normativas** exigibles analizando el entorno, y si no cumplimos modificar nuestra actividad o cambiar de entorno.
    - Facilidad para contratación de **personal**.
    - Acceso a **suministros** y **fiscalidad** aceptable.
- Ajustando las **condiciones de los contratos** de los productos, considerando objetivamente las cuestiones de cumplimiento y régimen de **penalizaciones** aplicable.
    - Tomar **márgenes de plazos** de entrega o de servicio realistas.
    - Asumir penalizaciones **no abusivas** en caso de incumplimiento.
- Asegurarse de que se transmite una **imagen corporativa** conforme con las expectativas del entorno.
    - Tener un **portavoz** responsable del cumplimiento, con poder suficiente para que la entidad responda a sus requerimientos.
    - Responder a las **reclamaciones** y fallos con una información rápida y veraz, a ser posible en varios canales, incluidas las redes sociales.
- Cumplir escrupulosamente con los **plazos comprometidos** en los contratos o en la oferta al público.
    - Formar al personal para concienciarlos de la necesidad de cumplimiento de los plazos de entrega que se hayan pactado y de **la forma de lograrlo**.



Ya que no podemos cambiar el mundo, adecuemos nuestra actividad modificando el entorno.

Si los puntos anteriores creemos que no son suficientes, también podemos actuar **directamente** sobre alguna de las fuentes de riesgos, con calma. Recordemos que nuestros escenarios pueden provenir de fallos en alguno de los siguientes aspectos (no exhaustivos):

- Personal
- Suministros e instalaciones
- Ciberataques
- Cuellos de botella

De estos siempre hay alguno que nos parece más problemático. En el ejemplo de **PCN 1.2.4. Escenarios**, recordaréis que considerábamos más problemático un escenario de **ciberataque**. Entonces deberíamos **centrarnos en este punto** y darle la mayor prioridad, de forma que nos dotemos de la infraestructura y los mecanismos necesarios no sólo para defendernos, sino para **dominar completamente este escenario**. Ese dominio también logrará haber **cambiado el entorno a nuestro favor**.

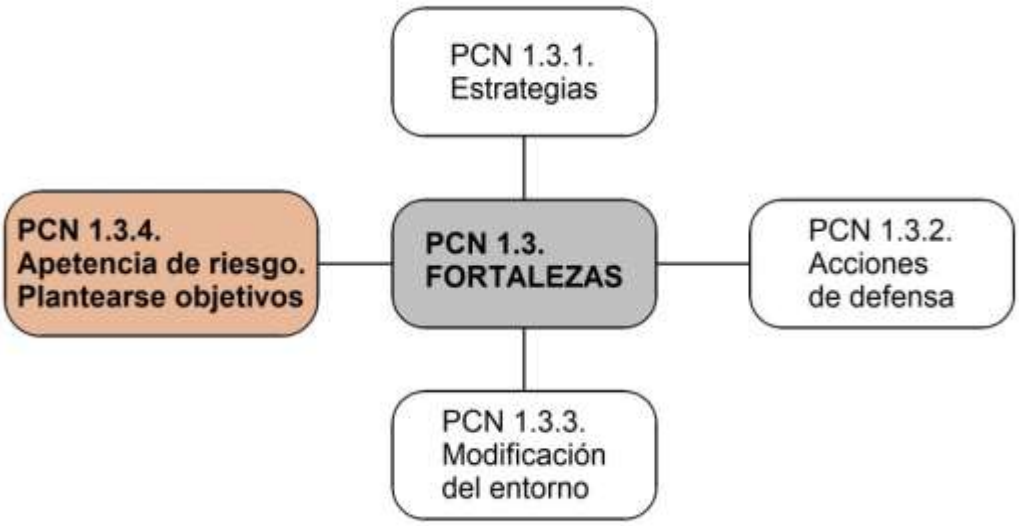
También en este conjunto de acciones, es de ayuda emplear un sistema de **gestión de proyectos**, planificando el trabajo en el tiempo, nombrando responsables para cada actuación, dotando de presupuestos y recursos suficientes, y manteniendo un registro permanente de las acciones realizadas y su grado de ejecución, para documentarlo todo.

PCN 1.3.4. Apetencia de riesgo. Plantearse objetivos

¿Cómo puede una entidad tener 'apetencia' de riesgo? Pues cuando una empresa es realmente innovadora juega con el riesgo, ofreciendo servicios para los que el público aún cree no tener necesidad, a fin de anticiparse a la competencia. Sin riesgo no hay ganancia, que puede ser mucha. El fracaso tiene un coste acotado.

Todos sabemos que hay empresas, sobre todo las tecnológicas punteras, que ofrecen a sus clientes productos o **servicios innovadores** que otros no pueden o no saben o no lo han pensado. Si parten de una posición solvente, el coste de la introducción de un nuevo producto puede ser limitado en comparación con el volumen de negocio global, pero los beneficios del éxito pueden ser inmensos, potenciados por las patentes registradas para un servicio en exclusiva y porque el primero que ofrece un producto es el que establece los **estándares** que otros tendrán que cumplir si quieren competir con ellos.

Diremos que entonces las **empresas innovadoras** tienen un **alta apetencia de riesgo** (también llamado apetito de riesgo). En general las **empresas que son tradicionales** tienen **poca apetencia de riesgo**, aunque su fuente de fortaleza puede ser que hacen realidad el mantenimiento de unos **procesos únicos y distintos**, apreciados en un mundo en que todo tiende a homogeneizarse. Como, desde que en **PCN 1.2.4. Escenarios** fijamos un **valor** para los distintos **escenarios** de riesgo, podemos referirnos a los riesgos numéricamente, ahora podemos fijar un nivel de apetencia de riesgo. Contando con una **escala del 0 al 9**, sería **bajo, digamos 2 ó 3**, para una empresa *tradicional* con **poca apetencia** por el riesgo y **alto, digamos 5 ó 6** para una empresa *innovadora* con **alta apetencia** de riesgo. Un nivel más alto sería rompedor y podría desembocar fácilmente en fracaso por efecto de riesgos incontrolados.



La apetencia de riesgos es parte de la apreciación de riesgos tras el análisis y asignación de valores.

Objetivos equilibrados

Una vez tenemos claro el concepto, uno de los factores de fortaleza es llevar a la práctica, **plantear objetivos**, de forma controlada, que incluyan nuestras acciones para reducir la **exposición al riesgo**. Por ejemplo, si fijamos que es aceptable un riesgo de valor 2 o menos, podremos **asumir riesgos iguales o más bajos** para centrarnos en **protegernos de los riesgos mayores** que nos pueden expulsar del mercado, no

disipando nuestros recursos en reducir **riesgos que son asumibles** y para los que podemos aceptar sus consecuencias.

Estos **objetivos** se han de **revisar a intervalos** regulares, por ejemplo anualmente, a fin de que tengan sentido y nos permitan adaptarnos a la situación real del medio.

Tanto la definición de la **apetencia de riesgo** de la entidad como plantearse **objetivos** para abordar la tarea de minimizar la exposición a riesgos que excedan la apetencia de riesgo de la organización, son muestras de **madurez y fortaleza** en continuidad de negocio porque indican que se tiene la **situación bajo control**. Sin lo uno y lo otro se está a merced de los acontecimientos, *esperando tener suerte* la próxima vez que se presente un problema de difícil solución, cosa que no sucede normalmente. Cuesta menos esfuerzo realizar actuaciones que se han previsto, aprendido y se tienen practicadas que tener que aprender sobre la marcha cuando no ha habido la suficiente previsión. Por eso disponer de un **sistema de gestión de continuidad** aumenta la **fortaleza** de la empresa.

En la siguiente parte del libro, la **PCN 1.4. Oportunidades**, veremos la forma de centrar las prioridades de actuación que se nos van a ir presentando. De momento, casi sin darnos cuenta, **hemos visto ya** a lo largo de los primeros puntos del curso:

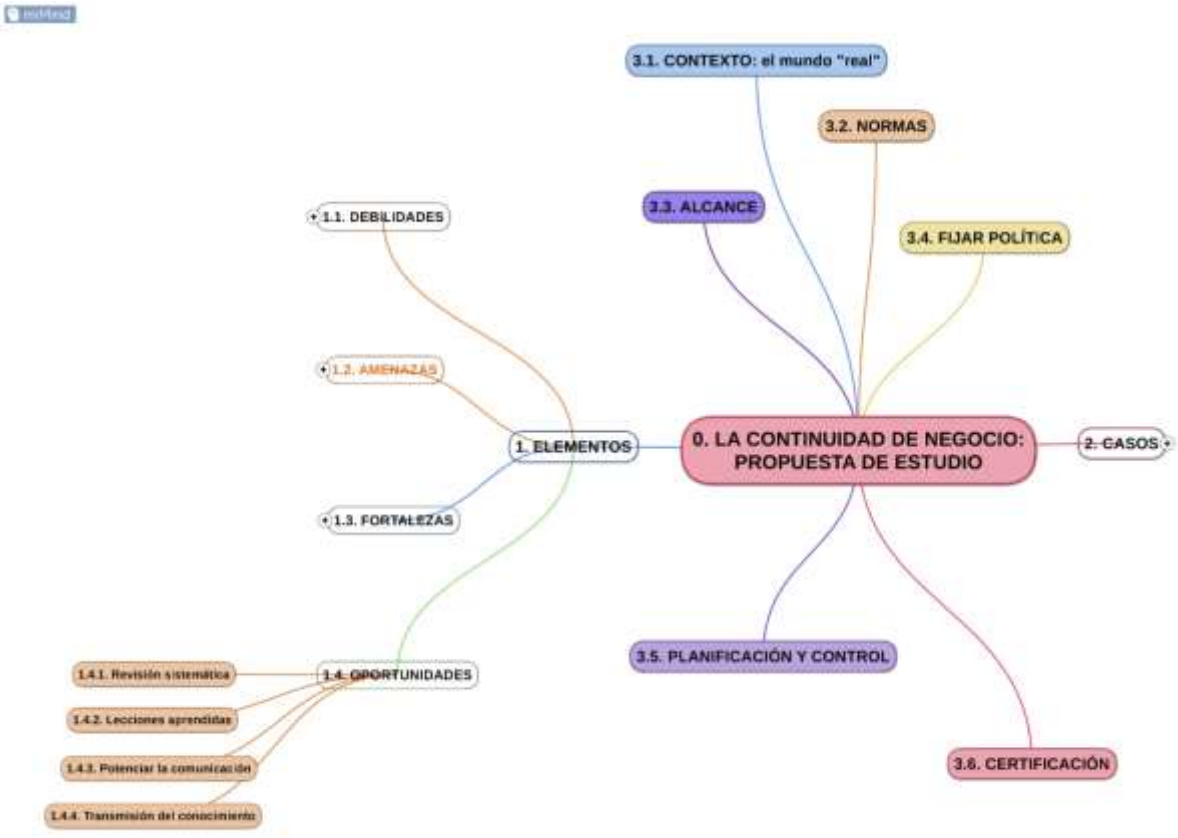
- La forma de conocer y registrar nuestras **debilidades**;
- Listar y tratar con las **amenazas** que se convierten en **riesgos** cuando se manifiestan en alguno de nuestros **puntos débiles**;
- Hemos sabido cómo evidenciar y clasificar nuestras propias **fortalezas** y aumentarlas mediante **gestión de proyectos**.

Cuando seamos ágiles en aprovechar las **oportunidades** y las **lecciones aprendidas**, después de los 5 siguientes capítulos, estaremos preparados para entrar *"a todo trapo"* en la gestión de cuatro tipos comunes de **crisis** elegidos para su estudio: epidemia, desabastecimiento, ciberataque y factor limitativo.

PCN 1.4. OPORTUNIDADES

En esta cuarta parte de nuestro análisis DAFO particular vamos a tratar las oportunidades, que en cuestiones de continuidad se nos van a presentar. Si en la parte de fortalezas mencionamos el conocimiento y la determinación como la materia de la que está hecha la fortaleza, en esta parte insistiremos en varias formas de comunicar, transmitir y dejar constancia de ese conocimiento de forma perseverante.

En efecto, en continuidad, como en casi todo, **las oportunidades no suelen venir por si mismas, sino que hay que trabajarlas** antes para que se presenten. Casi todo lo que ocurre aporta materia de reflexión que desarrollada convenientemente significa una oportunidad. **Cuando todo va bien, apenas aprendemos** más allá de comprobar que lo que estamos haciendo está correcto, pero **cuando todo va mal aprendemos más**, porque podemos conocer de primera mano qué es lo que hemos hecho mal y **corregimos**, es decir ponemos remedio para no caer otra vez en el mismo error. De todo se sacan **enseñanzas**, estando atentos podemos ver oportunidades, tener conocimiento de ellas, en cualquier circunstancia, pero mejor irlas preparando. Por ejemplo, de las crisis aprendemos, pero si montamos un **simulacro de crisis** aprendemos también sin arriesgar el funcionamiento de la empresa. El conocimiento, para ser efectivo, ha de ir seguido de la comunicación.

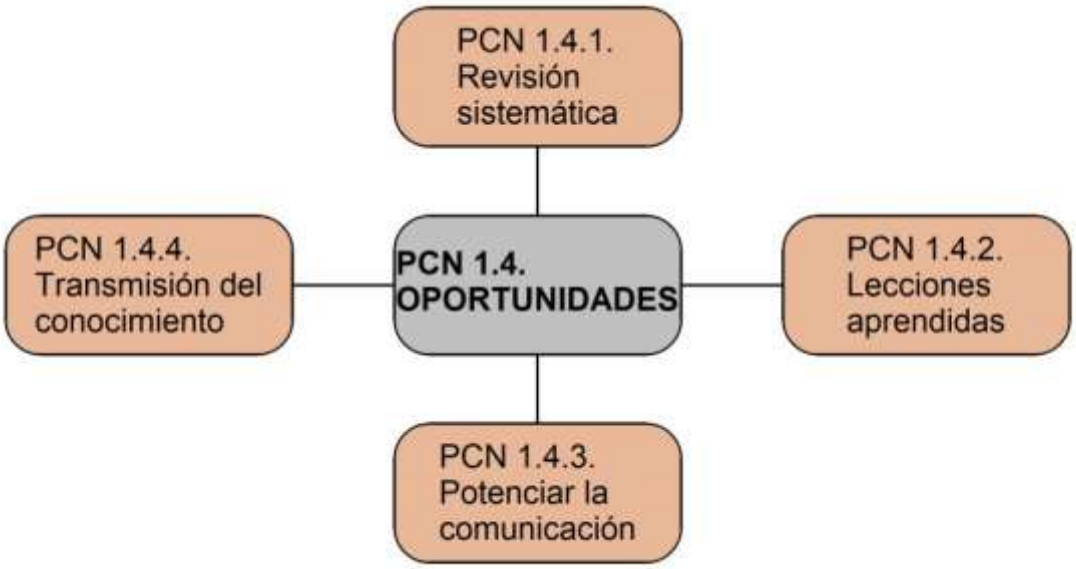


Las oportunidades y su relación con la comunicación en su contexto de la continuidad.

Tenemos que quedarnos con la idea básica de que sin una comunicación perfectamente organizada no puede haber oportunidades aprovechadas. Por eso todas las materias que trataremos próximamente tienen algo que ver o deben algo a la comunicación. Empezando en que para darnos cuenta de que hay una oportunidad nos tiene que llegar la información pertinente. El proceso de transmitir información es la

base de la comunicación. Para más abundancia, examinadas las actuaciones en **crisis reales** que se han resuelto de forma efectiva y en aquellos simulacros en que todo se ha desarrollado como debería haber sido si la crisis fuera real, lo que *ha cambiado las cosas de naturaleza* para dar una respuesta efectiva y satisfactoria ha sido la **comunicación a todos los niveles**:

- Comunicación **con el exterior** para conocer el estado del entorno;
- Comunicación corporativa **de 'arriba abajo'** para que la Dirección transmita datos de situación, llegue a acuerdos operativos con todas pas partes y pueda dar órdenes al resto de la Organización;
- Comunicación corporativa **'de abajo arriba'** para que los representantes de los empleados transmitan a la Dirección sus demandas o su conformidad;
- Comunicación dentro de **los equipos** y entre los equipos para coordinación de las actuaciones;
- Comunicación de las **buenas prácticas**, consolidadas como **procedimientos** seguros para uso de las nuevas generaciones de empleados, etc.



Las oportunidades en continuidad de negocio.

Listando oportunidades

En este momento de nuestro desarrollo vamos a tratar en sucesivas entradas, varios aspectos esenciales relativos a visualizar **oportunidades** como son:

- **La revisión** sistemática, que tratará de tomar conciencia de los cambios ocurridos en un periodo de tiempo en la Organización y adecuar los procedimientos y objetivos a la nueva situación.
- Las "**lecciones aprendidas**", y la práctica, concretamente "el juego" (que lo llamaremos "**simulacro**") que es la base de todo aprendizaje acerca de cómo hacer un seguimiento efectivo de las siguientes crisis.
- **La comunicación** y qué significa para nosotros. Partimos de la base de que las entidades tienen que tener **listas de contactos** para emplear en momentos de crisis, a fin de poder llamar a las personas clave que nos pueden recuperar los procesos. Incluye la **concienciación** que va sembrando las ideas de los conceptos de continuidad permitiendo una adecuada sintonía de significados

necesaria para referirse a los riesgos, impactos, crisis, recuperación, etcétera, de forma coherente.

- Algo más serio, que llamaremos **“transmisión del conocimiento”**, y su influencia en el funcionamiento estable de la entidad, de forma que lo aprendido en una etapa no se tenga que volver a experimentar y aprender en la siguiente.

Más adelante, en el punto **PCN 2.3.4. Esquema de portavoz**, detallaremos el papel y el contenido que debe orientar al que actúe de portavoz de la crisis, papel esencial para potenciar la imagen y reputación de la empresa.

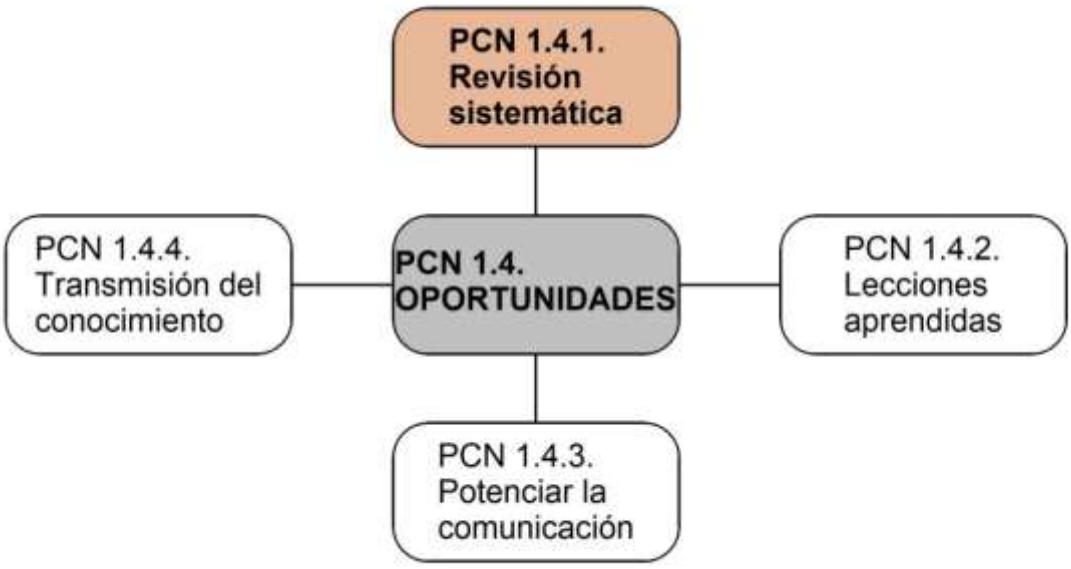
PCN 1.4.1. Revisión sistemática

La primera oportunidad que se nos ofrece en continuidad de negocio es aprovechar unas sesiones de reflexión sobre cómo está funcionando nuestro sistema de gestión y qué es lo que ha cambiado desde la última vez que hicimos balance de situación. Ello nos lleva directamente a plantear nuevos objetivos o revisar los existentes para corregir lo que no nos guste.

En las empresas, cuando se tienen sistemas de gestión establecidos, se realiza al menos anualmente lo que se llama **Revisión por la Dirección**. En resumen, se trata de analizar la **situación global** de la entidad y de su entorno, observar el **grado de cumplimiento** de los objetivos estratégicos y tácticos, así como **los planes** que se establecieron por parte de la Dirección el año anterior, para

- **Evaluar** el grado de avance,
- **Aprobar las actuaciones** que han sido eficaces en el periodo y
- **Plantear nuevos objetivos** para el año entrante.

Si mientras tanto ha habido **algún cambio significativo en los procesos**, que requiera otras formas de llevarlos a cabo, no se espera a la revisión anual sino que se elaboran o se revisan en esa circunstancia los procedimientos y la organización, para adaptarlos a la nueva situación, haciendo una **revisión complementaria** de la anual (es decir: *la Revisión* se puede hacer más de una vez al año por una necesidad concreta que surja, o incluso se pueden planear de entrada revisiones parciales a intervalos dentro del año). Este ejercicio realizado correctamente es muy completo y metódico y viene detallado en las normas aplicables al sistema de gestión, por ejemplo, la **UNE-EN ISO 22301** que rige los **sistemas de gestión de continuidad de negocio**. Pero si estamos montando nuestro sistema de gestión de continuidad y aún es el principio, faltarán algunos elementos porque no tendremos con qué comparar. Ya lo iremos perfeccionando en sucesivas ediciones.



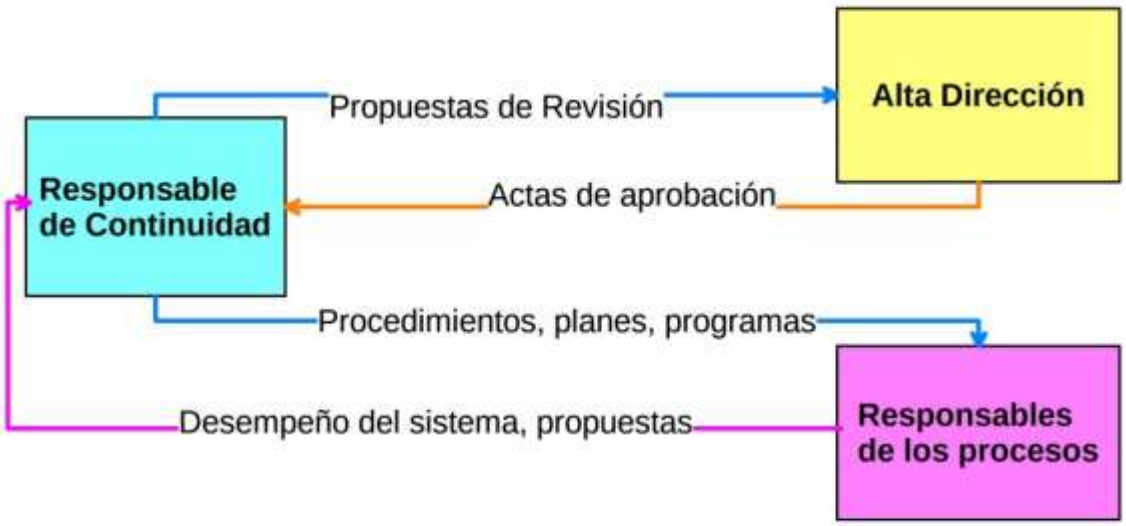
La principal oportunidad que se nos presenta anualmente es realizar a fondo la Revisión.

Preparando la revisión

Naturalmente el informe anual de revisión no surge espontáneamente, sino que surge del trabajo del equipo de continuidad de la compañía dirigido por un responsable. Anualmente (o en la frecuencia que proceda), la persona **responsable de la función de continuidad** elaborará el informe, consultando previamente con los distintos responsables de los procesos de la empresa, y sus propuestas, teniendo como referencia las indicaciones de la norma y los procedimientos de continuidad que se tengan redactados y vigentes. Formalmente hará en dicho informe las **propuestas de revisión del sistema por la Dirección**, para la consideración de la *Alta Dirección*, o sea, los directores o máximos responsables de la entidad. Planteará, junto a los nuevos objetivos propuestos, cuáles son **el personal y los recursos necesarios** para llevar a término las propuestas planteadas. Cuando el informe sea aprobado por la Dirección, preferentemente mediante un **acta** formal, que hace que todos los firmantes se comprometan y respalden la gestión del responsable de Continuidad, éste generará los correspondientes **planes de acción**, que deben controlarse mediante la adecuada **gestión de proyectos** que esté establecida en la empresa.

Junto al informe de **Revisión por la Dirección**, es costumbre que la Dirección apruebe o respalde explícitamente los **procedimientos nuevos** o revisados, la **forma de evaluar** el cumplimiento y de realizar un seguimiento permanente, los planes para la **formación** permanente del personal y el **programa de *juegos* o simulacros** que harán que el equipo esté preparado por si surge un incidente de gravedad o una crisis.

De esta manera se crean **"bucles" o circuitos de información** que *esparcen el conocimiento* por medio de **la comunicación** en todas sus formas: informes, actas, comunicados, procedimientos, registros de evaluación, etc. Visto desde esta perspectiva, se trata de un fenómeno de **autoaprendizaje** que afecta a toda la organización, que tiene sus *ritos y ceremonias*.



Bucle de Revisión por la Dirección.

Si está bien planteado, este movimiento genera un **conjunto de registros** que sirven para dejar trazas de lo realizado y que servirán para que expertos externos (auditores) puedan certificar en su momento el sistema y su funcionamiento. Cuando todo esto

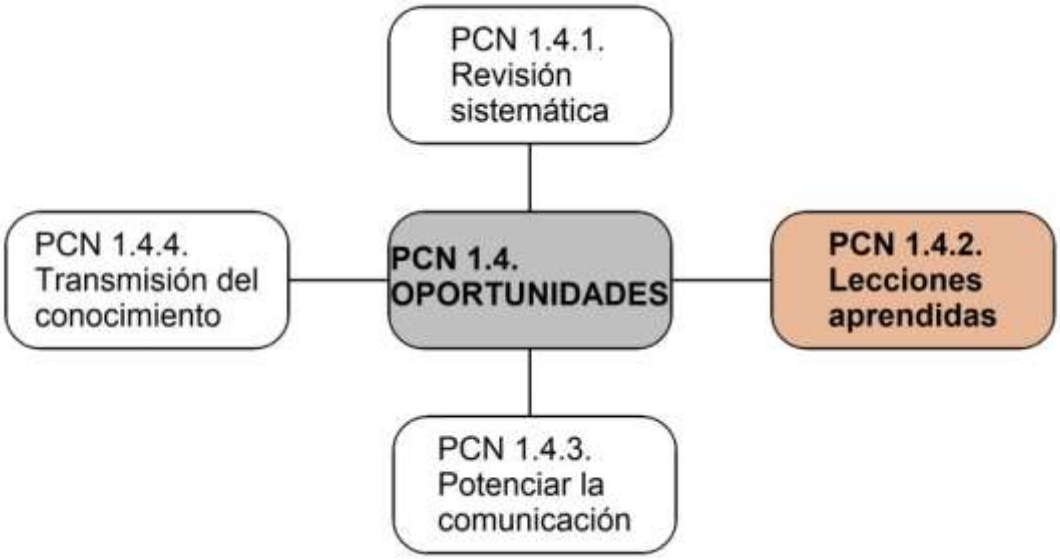
sucede de forma espontánea y se asume como parte esencial, que lo es, del funcionamiento de la Organización, esto indica un grado de madurez importante, un **control** sobre los medios propios y lo que pueda venir del entorno, que hace que la entidad entre en un **círculo virtuoso**, denominado "**Ciclo de Deming**", en recuerdo del ingeniero norteamericano que lo introdujo en la gestión empresarial, perfeccionado con la toma de conciencia y aprobación formal de las principales propuestas por la Alta Dirección.

PCN 1.4.2. Lecciones aprendidas

Cada vez que ocurre un incidente o una crisis, se viven una serie de experiencias que sirven para aprender. De la misma forma que los niños (*solo*) aprenden jugando, hay que aprovechar el suceso para conocer los fallos, todo lo que no ha salido bien, y corregir o perfeccionar los procedimientos que ayuden en futuras crisis "de verdad". Ese es el fundamento de realizar simulacros, que es como "jugar a que hay una crisis".

Es interesante el concepto de **lecciones aprendidas**. Está emparentado con la idea de que de cualquier circunstancia se puede **sacar provecho**. En efecto, es desagradable verse involucrado en un incidente en que se paraliza la actividad en la que estás trabajando. Pero hay circunstancias más fuertes que nosotros contra las que nada podemos hacer, y aleatorias, que son capaces de hacernos parar nuestro proceso: **una avería, un desastre natural, una enfermedad** que afecta a la mayoría de la plantilla. Si sufrimos una de ellas, hemos pagado involuntariamente un tributo. Este pago nos permite ver mejor, y también sufrir "en directo", cómo han actuado las **amenazas** sobre nuestros puntos débiles o **talones de Aquiles**, materializando un **riesgo** que parecía pequeño, cuán fácil hubiera sido (a veces) **proteger mejor** nuestros sistemas, **a quién necesitamos** realmente para ponerlo todo en marcha otra vez.

Exactamente lo mismo pasa y lo mismo aprendemos cuando preparamos **un simulacro**, pero con un coste infinitamente menor, sin tener que sufrir las consecuencias, porque los simulacros los hacemos en un ambiente y en circunstancias totalmente controladas y acotadas.



Las lecciones aprendidas son una gran oportunidad.

Por eso **no es** buena idea esperar a tener un incidente para empezar a mejorar o para que el personal coja experiencia y aprenda. La manera de tener soltura e iniciativa cuando se necesita es realizando un **programa de simulacros** que permita a todo el mundo practicar. La ventaja es que si sale mal no pasa nada. En realidad, es mejor que haya errores, porque permiten visualizar mejor lo que no ha funcionado. El programa de **simulacros** se suele preparar anualmente, pero se puede modificar según las necesidades de formación de grupos de personal o de variaciones en el proceso que hay que poner a prueba.

Quedamos al principio de esta parte del libro que la materia de la que están hechas las **oportunidades** es la **comunicación**. Ahora es esencial que todo lo que hemos podido recopilar, **tanto en una crisis real como en un simulacro**, sobre el origen, el desarrollo y la solución del incidente vivido lo reflejemos en un **informe escrito**, que se conoce genéricamente como **informe de lecciones aprendidas** (que podemos llamar también **informe de incidente**), con lenguaje sencillo, para compartirlo con la Dirección y con el personal técnico.

El Informe del Incidente o de las Lecciones Aprendidas

La estructura del informe de **lecciones aprendidas** que se hará **para cualquier incidente** tanto real como simulado debería incluir:

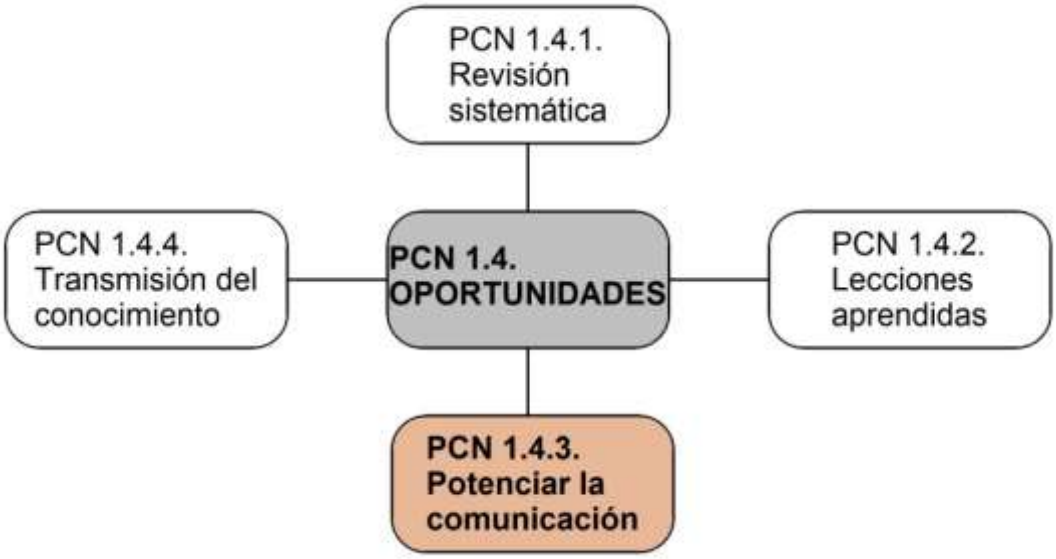
- **El relato histórico** de lo ocurrido,
- Qué cosas se hicieron **bien** y qué **objetivos** se cumplieron,
- Qué cosas salieron **mal** y por qué,
- Qué **conclusiones** hemos podido sacar del incidente y finalmente
- Una relación de **Acciones Correctivas** con sugerencia de **responsables**, **medios** necesarios, **coste** y **plazos** estimados, **procedimientos** que haya que corregir o preparar, para incluir las acciones en la **gestión de proyectos** de la entidad y poder hacer un seguimiento y control ordenado y eficaz.

Un extracto del informe de las lecciones aprendidas, que no incluya datos que puedan poner en peligro la confidencialidad de la información, ***debe circular*** para conocimiento de los participantes en el simulacro. De nuevo la **comunicación** aparece como la materia de la oportunidad.

PCN 1.4.3. Potenciar la comunicación

El uso de la comunicación es consustancial a cualquier agrupación humana, como una empresa. De hecho, es lo que hace que el esfuerzo conjunto produzca un resultado mayor que el que produce la suma de los esfuerzos individuales, porque consigue alinearlos en el sentido que favorezca el cumplimiento de los objetivos del grupo. Si ese objetivo es lograr la continuidad, es preciso tener una buena comunicación.

Podemos distinguir entre comunicación dentro del grupo y comunicación con el exterior. Requieren infraestructuras distintas, debido a las distintas naturalezas de la relación de sus actores.



La comunicación efectiva es una gran oportunidad para la continuidad.

La **comunicación interna**, tradicionalmente, se basaba en las *Comunicaciones Interiores* y en los tablones de anuncios. Eran relativamente *frecuentes reuniones de los jefes con sus equipos* para informar y coordinar trabajos. En el transcurso de una sola generación se han sustituido ampliamente por el **correo electrónico** y la **intranet** corporativa, y las reuniones, sean en persona o sean on-line se han vuelto más **reuniones de colaboración entre equipos** y demasiado numerosas y frecuentes. También son importantes las reuniones **sindicales** entre empleados y las de los representantes sindicales con la Dirección.

Siguiendo las reglas

Cada empresa tiene una cultura del uso de los instrumentos de comunicación, pero para conseguir que la comunicación sea efectiva se deben mantener unas ciertas reglas.

- El **correo electrónico** debe ser la forma de dejar constancia de propuestas y solicitudes, de respuestas formales, de avisos o notificaciones personalizados, sustituyendo las antiguas Comunicaciones Interiores. No es buen sitio para polémicas o ajustes de cuentas. Debe ir dirigido al mínimo de personas que

tengan que recibirlo y que tengan que ver con el asunto. No es buena práctica hacer hilos a todo un grupo numeroso, sin necesidad.

- La **intranet** es el mejor modo de comunicar a todos lo que antiguamente se publicaba en los tablones de anuncios. Debería funcionar como una especie de Boletín Oficial. Es un magnífico canal de comunicación de normas generales en vigor o de acontecimientos que afecten a todo el mundo. Una utilidad importante es que sirva de canal para que distintos grupos o departamentos den a conocer su trabajo o soliciten colaboración al resto de la organización. La colaboración de un equipo formado por un mínimo de personal especializado con conocimiento de comunicación, generando contenidos para la intranet, puede hacer de ella un instrumento profesionalizado y más efectivo.
- **Las reuniones** acaban siendo un verdadero cáncer de la organización, cuando exceden su concurrencia, su tiempo de duración, los contenidos no estén ajustados al fin previsto o no se cierren cuando se debe. Una empresa que tenga excesivas reuniones no tiene bien estructurados sus procedimientos y la gente no sabe cuál es su trabajo. En las convocatorias se debe enviar a los participantes la información de base, el tiempo y lugar previsto, las decisiones que se espera tomar. No se deben tolerar ataques personales y a su finalización el convocante debe escribir un resumen de los acuerdos alcanzados, a fin de hacer un seguimiento posterior.
- Las **reuniones sindicales** entre trabajadores y entre los representantes y la Dirección son imprescindibles cuando se trata de afrontar problemas de la entidad. Las normas son las mismas que las de cualquier reunión. En caso de crisis se resuelven muchos problemas fomentando **grupos de seguimiento** de un número pequeño de directivos y representantes para ir preparando los acuerdos entre ambas partes.

La **comunicación externa** que anteriormente consistía en la de la Alta Dirección en su relación con la propiedad y las **autoridades**, la que se mantiene entre los **proveedores** y la Dirección de Compras o de Logística y entre los **clientes** con la Dirección Comercial, actualmente se ha complicado bastante con la irrupción de las **redes sociales** y el fuerte **impacto reputacional** de cualquier error de la compañía en tales **redes sociales**. Es normal que las funciones básicas se mantengan, sin olvidar ahora los impactos reputacionales en internet:

- La comunicación **con autoridades** debe seguir siendo función de la Alta Dirección por cuestiones de protocolo y de interés legítimo de la propia empresa. En momentos de crisis es muy importante que en ciertas ocasiones participe en el grupo de contacto que se establezca con las autoridades algún Representante de los empleados para visualizar el compromiso.
- Los responsables de **compras** y **comercial** son las personas idóneas para la comunicación con proveedores y clientes. Pero dado el carácter cada vez más abierto de las comunicaciones de la empresa con la sociedad en general, se debería tener un servicio de **atención al público**, tanto tipo ***call center*** como en directo, para resolver cualquier duda de los servicios prestados, sobre todo si la empresa proporciona algún producto o servicio para el público.
- **Redes sociales**: la novedad en los últimos tiempos es la irrupción de internet como foro de discusión y de transmisión del agrado o la decepción de usuarios con las empresas y con cualquier institución. Nadie está al margen de este juicio público permanente. Antes de que un tsunami de mala reputación pueda arruinar el trabajo de un buen número de profesionales que trabaja en nuestra empresa o entidad es muy conveniente tener los medios, estar allí con una labor

de ***community manager*** eficiente, capaz de transmitir los valores de nuestra organización y de contrarrestar con datos cualquier ataque infundado.
- **Portavoz**: la Alta Dirección debe designar un portavoz que puede ser permanente o distinto para distintos tipos de crisis. Esta persona debe tener suficiente autoridad para negociar y conseguir que los propios responsables corrijan errores que están afectando a a la imagen pública de la entidad. Volveremos sobre este asunto en PCN 2.3.4. Esquema de portavoz.

Esto está bien, pero ¿qué hay de la **comunicación en caso de incidente o crisis**? Sigue siendo válido todo lo anterior, pero además la organización debe tener en cada uno de sus departamentos o grupos al cargo de los distintos procesos sus propios **procedimientos de comunicación**. Estos documentos deben contener listas con **datos de contacto** de los **responsables** del grupo a los que hay que llamar en caso de incidentes, y también de los **proveedores y clientes** a los que hay que contactar para avisar de problemas en la actividad que afecten a los procesos de forma inaceptable y para negociar en esos casos de qué forma se tendrán que adaptar los suministros y los servicios para evitar o minimizar penalizaciones.

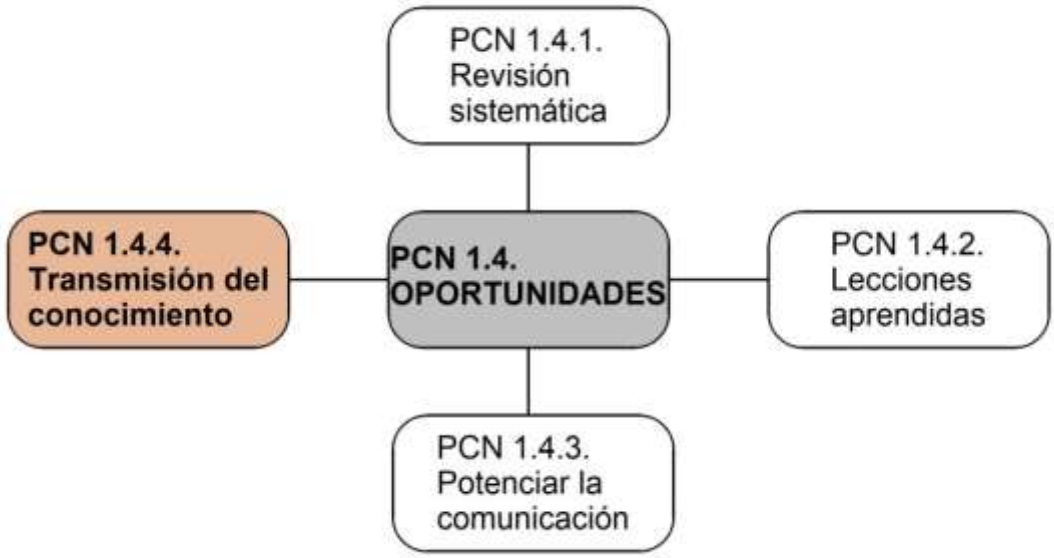
En caso de problema severo es inútil intentar ocultar la situación. Se adelanta más comunicándolo a las distintas partes y solicitando colaboración y comprensión. Y también, si el problema es generalizado y está afectando a la competencia, podemos ver en qué superamos a nuestros competidores para aprovechar la ocasión y darle un buen empujón a nuestra **imagen corporativa**.

PCN 1.4.4. Transmisión del conocimiento

Confirmando el hecho de que «nadie es profeta en su tierra» *(Lucas 4:24)*, las empresas en general prefieren contratar *un gurú* de ultramar para que les cuente a sus directivos «cómo triunfar en los negocios» al tiempo que ignoran el conocimiento acrisolado por sus profesionales veteranos. Con ello se pierde la gran oportunidad de tener a *los mejores* en los puestos adecuados formados por los que más saben.

Cuando un profesional lleva la mayor parte de su vida trabajando en un negocio, ha podido ocurrir que haya triunfado y todo sean reconocimientos, pero también, incluso habiendo triunfado, más frecuentemente puede llegar al final de su vida laboral con la sensación de desapego y la confirmación de que no han sabido aprovechar la **oportunidad** que suponen sus conocimientos y experiencia. Dado que el trabajo es una manifestación de la capacidad y la vocación profesional, sobre todo en personal veterano que hubiera podido en algún momento a lo largo de su carrera cambiar y dedicarse a otra cosa, resulta muy chocante que se llegue a la jubilación con la sensación de no haber podido sacar todo el partido a la potencialidad adquirida en muchos años de profesión.

En un punto anterior **PCN 1.4.2. Lecciones aprendidas**, tratábamos de **oportunidad** el conocimiento que vamos adquiriendo con la experiencia de haber pasado crisis y habernos formado en simulacros. Con más motivo se tiene que valorar lo aprendido no en una crisis, sino en **toda una carrera** profesional. Es una gran responsabilidad de los directores de personal y en general de la Alta Dirección, lograr que su personal esté motivado y se sienta respaldado y reconocido en proporción a lo que haya podido aportar en su vida laboral y **el conocimiento que pueda legar** a los recientemente incorporados. Si la conciencia de la entidad es el recuerdo de las vivencias que atesoran sus miembros, se puede llegar a un punto en que los que entren en la presente generación ya no tengan la conciencia de pertenecer a la misma empresa, por el **corte generacional** que con frecuencia se produce. Vamos a ver algunas cosas que se pueden hacer con esto.



La Transmisión del conocimiento es un filón de oportunidades, bastante desaprovechado en general.

Algunas propuestas para 'no perder el conocimiento'

A modo de propuestas, veamos unas cuantas cosas que se pueden hacer en las empresas para impulsar la **transmisión del conocimiento** de los que más saben a los nuevos.

- Por empezar de alguna forma, se puede fomentar la participación de los veteranos en **comités internos** (que se crean en todas partes),
    - preferentemente los más estratégicos,
    - aquellos que van a tratar de plantear proyectos de mejora sustancial de la empresa a medio y largo plazo
    - o que van a tratar de las políticas generales que marcarán la imagen y la misión de la entidad.
    - Para ello se debe asegurar la reserva de algunas plazas en estos grupos de trabajo corporativos para los más veteranos. Esto permitirá que intervengan proponiendo o matizando las actuaciones del grupo, a modo de *Senado* de la entidad.
- **Contratos de relevo**, el papel del aprendiz. Estos contratos pensados para que se vayan formando los sustitutos del personal que se jubilará en breve pueden servir para varias cosas:
    - La primera para que el profesional veterano **no siga agobiado** por la tarea diaria, a la que puede dedicarse con ventaja alguien que acaba de entrar en la escena laboral y tiene necesidad de darse a conocer y promocionarse.
    - La relación entre el aprendiz y el maestro permite adelantar en la formación del nuevo profesional sin que tenga que pasar por (todos) los fracasos de principiante, supervisado y aconsejado por un profesional veterano.
    - Se transmite más eficientemente la cultura empresarial si se tiene a quién emular, que es la relación que se produce entre el aprendiz con su maestro.
- **Charlas, coloquios, sesiones de formación**, todo retribuido. Si un profesional con amplia experiencia puede hacer algo bien es contar sus experiencias, porque no tiene que aprender antes la lección que va a impartir, ya que la ha vivido en carne propia. Eso sí, impartir una clase ha de ser una **actividad retribuida**. Puede ser genial aprovechar para **formar al personal en tareas no habituales suyas** a fin de reforzar la flexibilidad de formar equipos en casos como los de epidemia (ver **PCN 2.1. Epidemia**):
    - Porque así se le da importancia y porque es bueno que el trabajador cobre por su trabajo.
    - ¿Cuánto costaría contratar a un consultor que ha oído hablar de la empresa *de lejos*, para dar una charla? Eso mismo es lo que debe cobrar el veterano por dar su charla, que seguro estará mejor orientada para los fines de formación del personal propio.
    - Otra retribución que recibiría sería el **prestigio** frente a los suyos, al verse dando su charla, prestigio que no tiene precio.
- **Procedimientos** y documentos de trabajo. Los documentos que se generan en una organización han de cumplir una misión educativa al margen de su utilidad concreta y operativa.
    - Con todo el rigor que se pueda necesitar deben ser legibles y permitir a los que los empleen aprender sobre los procesos, no sólo seguir unas listas de obligaciones.

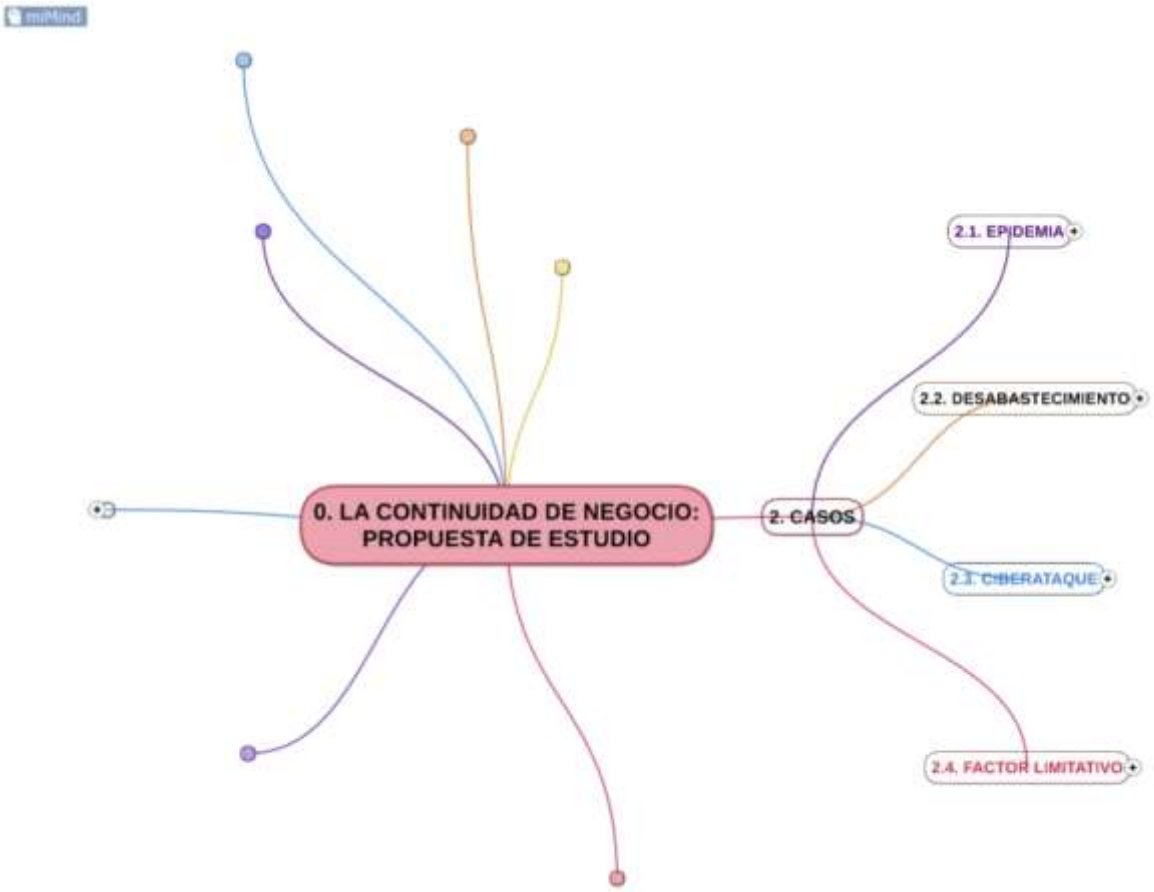
    - Un buen procedimiento evita tener que *inventar la rueda* cada vez que se hace un trabajo, sobre todo si es delicado y del mismo depende el éxito de la compañía.
- Presentaciones y **boletines en la intranet**, incorporación en el equipo de comunicación. Hemos hablado anteriormente de la **intranet**. Este instrumento tiene un enorme poder, no solo para aquello que es oficial. Utilizar la intranet para editar periódicamente **boletines o *newsletter*** que sirvan para ir familiarizando a los empleados con la terminología y con la utilidad de la función de continuidad (y de otras actividades en la entidad) es una buena idea, ya que
    - al no ser obligatoria su lectura, siempre es más agradable
    - y la difusión provoca menos rechazo instintivo que por aquello a lo que nos obligan.
- Homenajes y **celebraciones personalizadas**, detalles fomentando el espíritu corporativo ¿por qué no? Las empresas dedican mucho dinero a mantener sus instalaciones en los llamados “gastos generales” o “gastos corrientes”, por lo que es asombroso que no dediquen a veces casi nada a hacer a los más veteranos algún homenaje por sus aportaciones a la Organización.

PCN 2. CASOS

Hasta ahora hemos introducido cuestiones sobre continuidad que también podrían ser objeto en cualquier empresa en su gestión *ordinaria*. Hemos hecho un uso peculiar del análisis DAFO, por su sencillez y eficacia. Ahora trataremos de casos concretos de incidentes e introduciremos o profundizaremos en el uso de mecanismos más específicos de la continuidad.

Todo lo que hemos estado estudiando hasta aquí nos va a servir de base, pero a continuación ahondaremos en **estructuras y medios** concretos que nos van a servir para afrontar distintas clases de **crisis**. En realidad, cuando tengamos operativo nuestro Sistema de Gestión de la Continuidad, tendríamos que tener desarrollados todos los mecanismos que iremos viendo en esta parte a lo largo de las próximas 20 entradas (que nadie se asuste del número, porque iremos tratando los asuntos escalonadamente), pero de momento apenas tenemos ideas sobre algunos aspectos sueltos, a modo de **fundamentos** (los hemos llamado "elementos": debilidades, amenazas, fortalezas y oportunidades).

Gracias a la presión que se creará al plantear el **objetivo de resolver los problemas** concretos creados por los **incidentes** que iremos tratando, iremos ahora **creando las estructuras** necesarias. Como hay que empezar por algún sitio, aprovecharemos las peculiaridades de cada tipo de incidente para ir tratando y activando las que más pueden ayudar en cada caso.



Los casos de incidentes pueden ser infinitos, pero nos vamos a centrar en cuatro muy comunes.

Incidentes tipo para concretar el estudio

Desde el punto de vista de los activos involucrados los cuatro tipos de incidentes que vamos a estudiar tienen particularidades y nos permiten poner en cada caso el foco en distintas cuestiones que afectan a la continuidad:

- **Epidemia**. Afecta a **las personas**, que son la base de cualquier organización. Durante la pandemia de la COVID-19 se han podido poner a prueba muchas de las estructuras de defensa tanto a escala del sistema de salud nacional de los distintos paises como de las empresas. Hay todavía muchas secuelas que soporta el personal y la economía ha recibido enormes girones. Aquí introduciremos la organización de las **alarmas y llamadas** al personal, el organigrama y distribución o mapa de las **responsabilidades** que son efectivos y cómo proceder a la propia **gestión de las crisis** y de la **recuperación**.
- **Desabastecimiento**. Afecta a **los suministros**. El atasco en el canal de Suez por el encallamiento del Evergreen hizo ver claramente la dependencia de las empresas en Europa de los suministros provenientes de Asia. Posteriormente la invasión de Ucrania por Rusia ha traído cambios más profundos en la geoestrategia del comercio mundial. Haremos un repaso a fondo de la lista de **amenazas**, el Análisis de **Impacto como función del tiempo**, la **apreciación de los riesgos** y estrategias y finalmente cómo debemos plantear el sistema para revisarlo mediante **auditorías**.
- **Ciberataque**. Es un ataque a **los sistemas**. Esta es hoy en día la principal amenaza global para la actividad de las empresas en su relación con un mercado *super-tecnificado*. Esto no ha hecho más que empezar. Da la sensación que en lo que respecta a la información estamos en un mundo "medieval" de *firewalls* haciendo de castillos y de *passwords* como acceso y peaje simbólico de las entradas a las fortalezas de las empresas. No hemos llegado a la liberación de las murallas porque el sistema esté lo suficientemente protegido para que la presencia de "los malos" esté controlada por la "policía" de la red, capaz de mantener el orden. Haremos en este apartado énfasis en la importancia de los **métodos y procedimientos**, la utilidad de las **listas de chequeo o de comprobación**, la **simulación** de incidentes para preparar las defensas y la función y operativa del **portavoz**.
- **Factor limitativo**. Relativo al **diseño y programación** del proceso. Este es un mal, generalmente oculto a nuestros ojos que va minando la actividad de la empresa hasta que ésta se derrumba en medio del caos. Introduciremos este curioso problema casi al final del texto, cuando ya hayamos hablado de los otros tres problemas más fáciles de identificar. Para abordar este punto trataremos el concepto de **capacidad**, cómo se diseñan los **circuitos** de materias y de justificantes, el uso de la **investigación operativa** y la forma de proceder a plantear **objetivos y controles**.

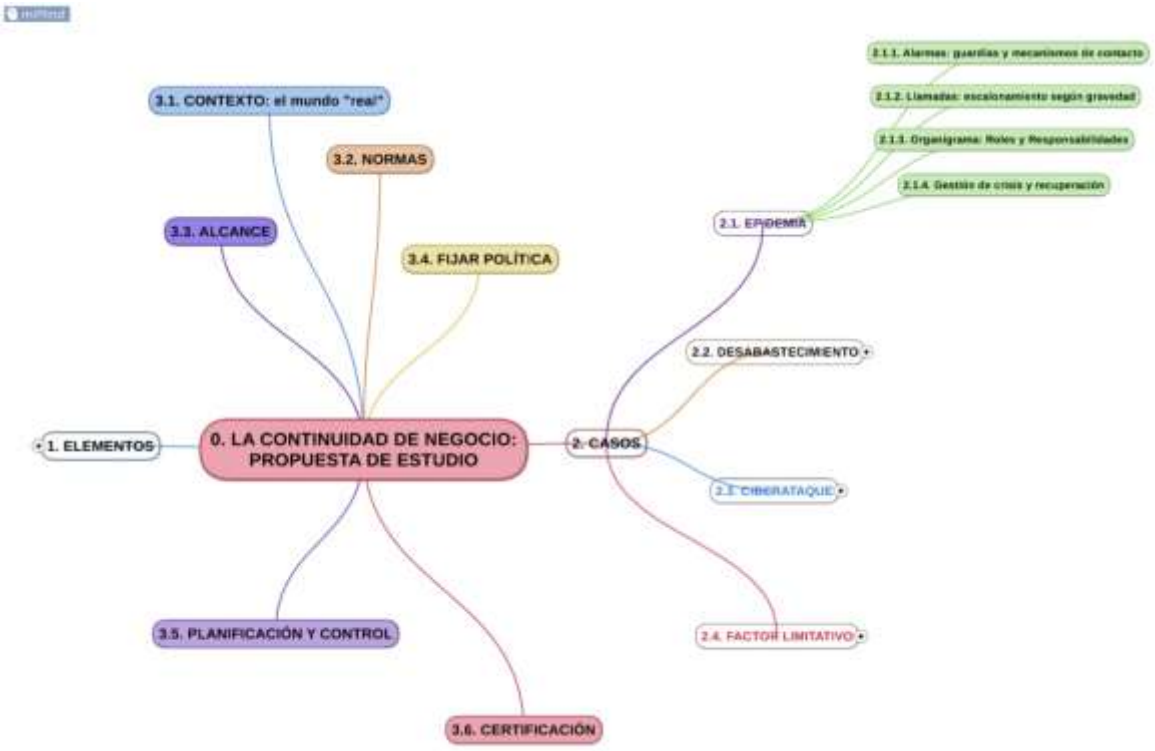
La vida en las agrupaciones humanas es movimiento. Si vemos los casos en perspectiva, todos tienen una cosa en común: **la forma en que afectan a la marcha de la empresa**, organización o entidad, que es parando o **interrumpiendo la actividad** normal o **continuidad** de sus procesos. Cuando vemos una ciudad desde arriba parece un inmenso hormiguero. Las crisis pueden afectar a la **continuidad** de la actividad hasta acabar con su funcionamiento normal. Por eso el **impacto de un incidente** en el funcionamiento de una organización tiene **una unidad de medida universal que es el tiempo de interrupción, que en caso de crisis supera el periodo admisible de**

interrupción (distinto para cada proceso), produciendo un incumplimiento de nuestros **objetivos** y de nuestros **presupuestos**.

PCN 2.1. EPIDEMIA

El escenario de epidemia lo hemos sufrido recientemente con motivo de la COVID-19. Como tiene una gravedad media (la mayoría acaba recuperándose) y su probabilidad es media (puede afectar aleatoriamente a cualquiera de nuestros efectivos clave), multiplicamos su calificación de gravedad 2 por la de probabilidad 2 para obtener un valor de 4, considerado riesgo alto.

Nos referimos a un apartado anterior, el **PCN 1.2.4. Escenarios**, para fundamentar por qué calificamos numéricamente, en un escenario de **epidemia, el nivel de riesgo como alto** para la continuidad. Ahora vemos que el trabajo realizado en aquel momento nos resulta útil para poder dedicar nuestro interés y actuaciones en términos de prioridades abordando primero el tratamiento de escenarios con riesgos más altos en lugar de intentar hacerlo *todo a la vez*.



El estudio de la epidemia aprovechará para introducir varias partes de la estructura del sistema de continuidad.

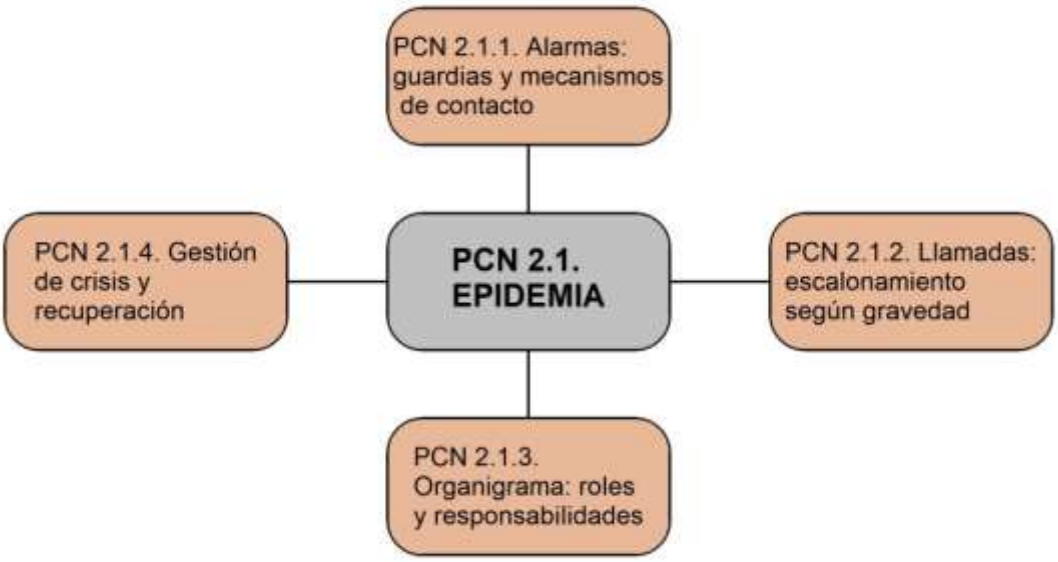
Para tratar un **escenario de epidemia** tenemos que actuar sobre la composición de los **equipos de personal** y su organización en el tiempo. El objetivo será disponer del personal necesario en cada momento para mantener la actividad en un nivel que consideremos aceptable. Aquí, y en general a lo largo de todo lo que sea abordar distintos escenarios de riesgo, va a ser **mucho más importante tener unos principios de actuación o estrategias probadas como válidas, mejor que tener una serie de actuaciones previstas**, que se van a quedar desfasadas rápidamente con la sucesión aleatoria de acontecimientos. Tiene más potencia y da más fortaleza basarse en buenas estrategias que prever absolutamente todo, como si fuera un guión.

Estrategias básicas para epidemia

Las estrategias básicas pueden ser perfectamente las de esta lista (cada organización debe establecer las suyas):

- Aplicar aquellas **medidas de tipo sanitario e higiene tanto preventivas como correctivas** recomendadas por las autoridades, siguiendo pautas de buenas prácticas que minimicen las posibilidades de contagio, según el tipo de **patógeno** activo.
- Mantener una actuación activa de **salud laboral** facilitando los servicios médicos y de prevención y control adecuados permanentemente, para que el personal esté y se sienta seguro.
- Tener **equipos multidisciplinares** capaces de trabajar en distintos procesos y operaciones si es necesario. Alguna cadena de tiendas por ejemplo tiene como estrategia habitual para el personal, que todos puedan hacer cualquier tarea dentro de la organización. Esa estrategia, además de facilitar la activación de equipos con distinto personal, hace que los empleados se sientan todos participes de la marcha del negocio. En instalaciones industriales de algunas marcas se ha sustituido la cadena de montaje por equipos multidisciplinares que cada uno de los cuales construye el producto completo autónomamente. En ambos casos la ausencia de una parte de la plantilla no es un obstáculo para seguir operando.
- **Establecer guardias** capaces de atajar cualquier eventualidad que les ocurra a los procesos en el mínimo tiempo posible. Naturalmente las guardias del personal propio hay que pactarlas con los representantes de los trabajadores y retribuirlas de forma justa para que sean aceptadas y efectivas. Este recurso no puede suplir una falta de personal prolongada o permanente. En ciertos tipos de incidentes, las guardias se pueden contratar con empresas especializadas en dar ese tipo de servicios (semejante a lo que ocurre en los servicios de asistencia en carretera). En trabajos a turno, los miembros de otros turnos pueden suplir con horas extras la falta de personal de un equipo.
- **Tener personal en modo teletrabajo** para distintos equipos en rotación, a fin de que, si se contagian los de un equipo, los de otro sigan estando disponibles. El teletrabajo, para que funcione hay que prepararlo siguiendo unas pautas concretas de soporte y control y también debe pactarse con los representantes.
- Establecer o relacionarse con un **portal de empleo** existente, para disponer rápidamente de posibles empleados que entrarían para sustituir a los que temporalmente estuvieran de baja. Sería también una oportunidad para poner a prueba a los aspirantes a un puesto, que podrían quedarse en la entidad en el momento en que cese la epidemia, para contratos de relevo o para ampliaciones de plantilla.

Cada una de las estrategias anteriores requiere tener una **organización** específica y adecuada al caso y trabajar permanentemente para su puesta en activo, por ejemplo disponer de un **servicio de prevención** de riesgos laborales capaz y efectivo en la organización, **preparar al personal** formándolo para tareas habituales y otras que normalmente no son las suyas (aquí tiene todo el sentido lo visto en **PCN 1.4.4. Transmisión del conocimiento**); **negociar con los representantes de los trabajadores** las medidas organizativas que puedan afectar a los horarios y salario resultante de aplicar las distintas medidas organizativas; **preparar todo lo necesario** (sistemas, equipos, formación, acuerdos) para que parte del personal pueda pasar a trabajar en su domicilio cuando sea necesario; **reclutar permanentemente personal** nuevo con criterios de igualdad de oportunidades, mérito y desempeño, para conocer posibles candidatos a incorporar en caso de necesidad.



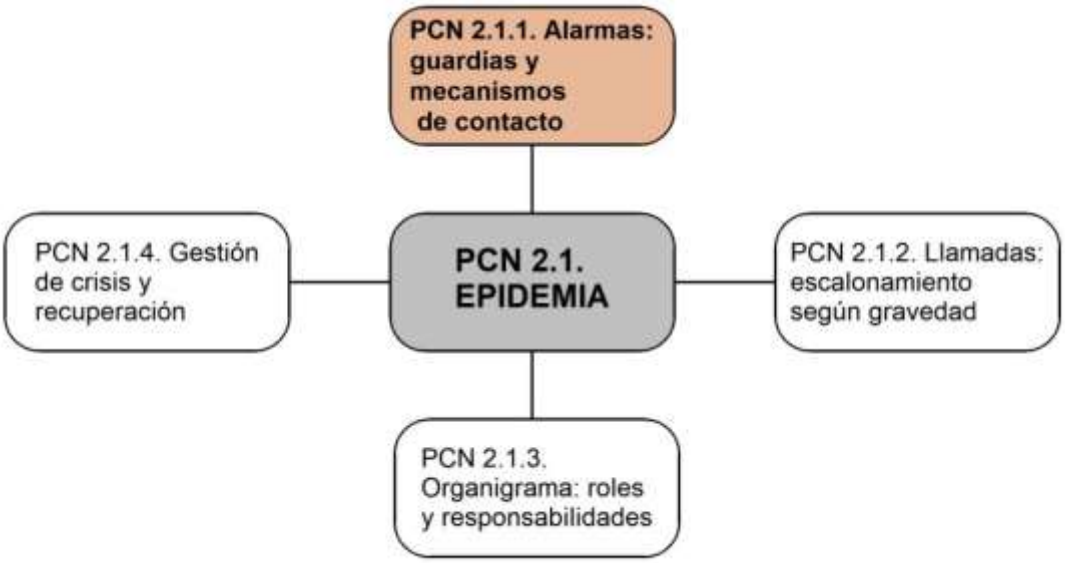
Elementos del Sistema de Gestión que introduciremos en el estudio de las epidemias.

En sucesivos capítulos iremos viendo concretamente cuestiones como de qué forma establecer las **alarmas**, cómo **escalonar las llamadas**, qué **organización** se necesita para abordar la situación de crisis y cómo es la secuencia de actuaciones típica en caso de **incidentes, crisis y recuperación**.

PCN 2.1.1. Alarmas: guardias y mecanismos de contacto

Cuando hay una alarma por un incidente en los procesos, lo primero que hay que tener es un mensaje que dar a las personas que pueden ayudar a restablecer o recuperar el funcionamiento de las operaciones interrumpidas. Puede que baste con acudir a personal de guardia o a personal asignado a otro turno. Para la transmisión del mensaje se necesita un canal o mecanismo.

El asunto del mensaje no es menor, pues éste ha de tener varias características. En el punto anterior **PCN 2.1. Epidemia** hablábamos de recurrir a **las guardias** de personal como una de las estrategias para atender la falta puntual de personal provocada por una pandemia. Esta estrategia, aun sabiendo que no es para uso permanente o continuado, puede servir en general en cualquier tipo de escenario. Para que empiece a actuar el personal de guardia ha de recibir un **mensaje de alarma**.



El escenario de epidemia se presta a todas las estrategias en las que interviene preferentemente el personal, en particular las alarmas.

Las alarmas pueden adoptar cualquier formato en el que se transmite lo que ocurre a las personas que pueden y deben intervenir para sofocar el incidente. Pero **el formato y contenido** del mensaje por un lado y **las personas objeto** del mismo por otro configuran dos de las características a tener en cuenta en el mensaje. Entonces es buena idea lograr un grado de **normalización** a la hora de considerar los mensajes a preparar. Para que las alarmas sean efectivas y cumplan la misión de informar a las personas que deben informar, lo mejor es preparar los mensajes en el momento en que **aún no se necesitan**, de tal forma que **queden listos para su uso** si se produce un incidente. Esta normalización puede incluir **algún tipo de codificación** que sea ***mnemotécnicamente*** fácil de recordar para mejorar la identificación y evitar improvisar. Vamos a ver estos aspectos de los mensajes de alarma.

Tabla ordenada de alarmas

Habría que redactar mensajes que fueran válidos para cualquier proceso, que correspondan a incidentes con **distintos niveles de gravedad** (que definiremos más adelante) y que vayan precedidos de una indicación de **a qué procesos afectan**. Algo así como la **tabla de esquema de alarmas** que sigue a continuación:

Tabla de alarmas según nivel de Incidente	Proceso A	Proceso B	Proceso C	...
0. simulacro	A0	B0	C0	
1. bajo	A1	B1	C1	
2. medio	A2	B2	C2	
3. alto	A3	B3	C3	
5. crítico	A4	B4	C4	

Sugerencia de tabla ordenando los mensajes de alarma de forma lógica.

Los contenidos de los mensajes han de ser de tal forma que indiquen claramente el objeto de los mismos, sin causar inquietud añadida, para que no produzcan pánico. Han de **orientar a la acción**. Si se trata de un **simulacro** se ha de aclarar desde el principio en el propio mensaje. Además del **inicio del incidente**, debe haber un mensaje **final que de por cerrado el incidente**. Aparte de mensajes distintos para diferenciar entre procesos, debería haber **mensajes dirigidos a la totalidad del personal**, a fin de no tener que repetir una y otra vez lo mismo para todos los procesos de la entidad. Los mensajes pueden estar **almacenados** en el medio que se empleará para las alarmas, para que la **disponibilidad** sea máxima. Si la empresa o entidad tiene personal de **vigilancia** es buena idea que sean ellos quienes manejen los avisos, a fin de centralizar la operación.

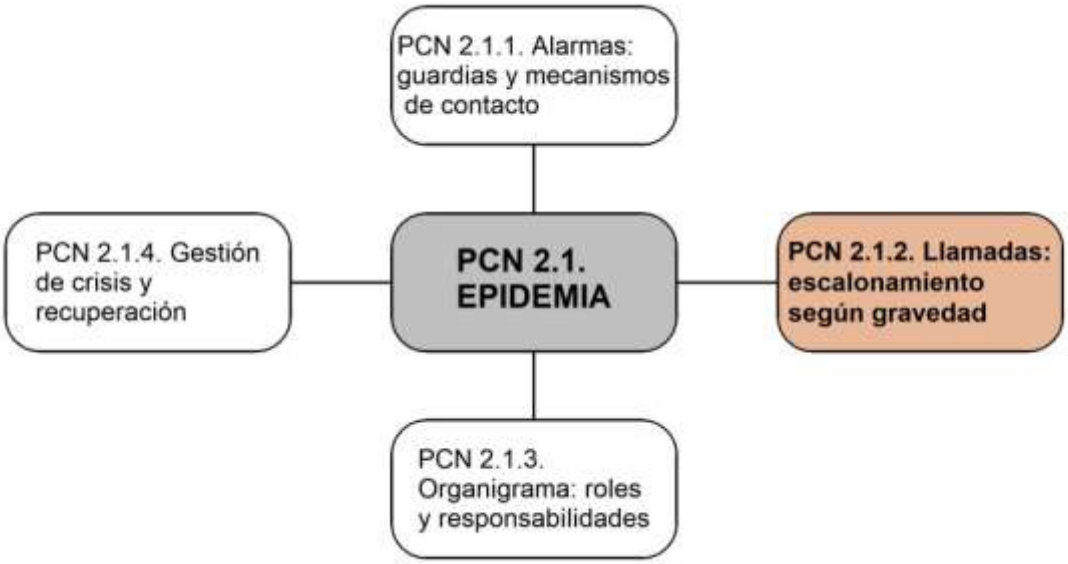
En cuanto a **los mecanismos** para lanzar las alarmas **dependen de la complejidad** de la empresa, de su extensión y de los medios disponibles. Bastaría con unas listas de mensajería a **grupos**, según quienes sean los responsables de los distintos procesos, y el uso de simples teléfonos o sistemas de mensajería (grupos de Telegram, por ejemplo) si se trata de una empresa pequeña de unos pocos empleados. Pero si queremos hacer un trabajo completamente profesional y con muchas más prestaciones, existen **soluciones profesionales de empresas que se dedican a comunicaciones corporativas** especializadas en tratamiento de incidentes y crisis.

En el siguiente punto veremos **cómo pueden establecerse los niveles de los incidentes**, que pueden evolucionar conforme avance el caso y posibles criterios de escalado para determinar las alarmas a lanzar. Según el nivel de riesgo y la evolución del incidente, los destinatarios de los mensajes de alarma pueden ser distintos y *escalar* desde personal **técnico** (normalmente si el nivel es bajo), a **directivos** (si el nivel es medio o alto) y en caso de crisis a la **alta dirección** de la empresa (nivel crítico). Por lo que la tabla del **esquema de alarmas puede tener algo más de detalle** de lo que da a entender el cuadro incluido arriba.

PCN 2.1.2. Llamadas: escalonamiento según gravedad

Distintos niveles de la organización deben tomar distintas clases de decisiones. Es por ello que, según sea la evolución y el estado del incidente, las llamadas deben también escalar los diversos niveles de decisión. No es lo mismo una avería que se prevé resolver en un tiempo 'normal' o 'admisible' que un incendio que está destruyendo una nave industrial. Tampoco es igual el primer aviso que el de fin de incidente.

En el punto anterior dábamos por supuesto que habría **varios niveles de incidente** sin entrar en detalle sobre cómo definirlos. Vamos intuyendo que debe haber una **forma objetiva de determinar en qué estado** estamos y cómo se activan los dispositivos para actuar en función de la gravedad del incidente. Hemos estado tratando, en la primera parte del libro, de calificar *a priori* posibles riesgos de los escenarios que se nos pueden presentar y hemos hablado en el punto anterior de los incidentes que provocan con los mismos calificativos. Ahora veremos de qué forma **calificaremos con más precisión** los **incidentes que 'ya' se han materializado**, no según nuestra estimación previa de gravedad y de probabilidad sino **por el daño que están causando en nuestra actividad**, porque según sea esta calificación se requerirán actuaciones distintas precedidas de las alarmas distintas que ya habíamos definido en el punto anterior.



Un incidente como la epidemia nos invita a calificar las interrupciones por los daños causados.

Para calificar los daños producidos por un incidente que causa una interrupción (tanto de los que pueden afectar al **personal**, como **epidemias** causadas por un patógeno o **huelgas** por conflictos sociales; a los **suministros**, por **desabastecimiento**; a los **sistemas** por un **ciberataque**; o a **factores limitativos** por un **diseño** incorrecto de los procesos), no debemos olvidar que según nuestra **planificación y presupuestos**, las interrupciones de la actividad pueden considerarse **inaceptables** si superan un determinado **tiempo**, que afectará a la **facturación** y a otros **costes** (multas, penalizaciones, indemnizaciones). Además, habrá ocasiones en que ni siquiera tendremos la **capacidad para resolver** la situación en el tiempo admisible de interrupción con nuestros medios.

Para colmo puede ocurrir que se produzca un deterioro crítico de difícil recuperación de nuestros procesos y se necesite la ayuda de las **autoridades o socios externos** en forma de bomberos, de préstamos de capital, o de quienes tengan la capacidad de recuperar los procesos reparándolos o reponiéndolos. Un **modelo de calificación del nivel del incidente** puede ser el siguiente:

Tabla de niveles de incidente

Calificación nivel de incidente materializado	Afectada facturación	Tiempo de interrupción	Medios propios o controlados	CALIFICACIÓN
0. simulacro	No	Acordado	Si	N.A.
1. bajo	No	Admisible, dentro de presupuesto	Si	Incidente menor
2. medio	Si, pero recuperable	Admisible	Si	Incidente GRAVE
3. alto	Si	Inadmisible	No	CRISIS
5. crítico	Si, y muy afectadas las instalaciones	>> Inadmisible	No. Necesaria ayuda de las autoridades	CATÁSTROFE

Niveles de incidente, posible clasificación.

En cuanto a los **destinatarios de las alarmas**, un criterio general, que se adaptaría según las circunstancias y el tipo de organización puede ser el siguiente:

- Las **alarmas de simulacros** irán dirigidas a todos los participantes, tanto alta dirección, directivos y mandos y técnicos, incluso al resto de la plantilla de los procesos afectados.
- Las de **bajo nivel** irán dirigidas preferentemente a técnicos clave de los procesos y a los equipos multidisciplinares que haya establecidos.
- Si el incidente escala a **nivel medio** se incluirá generalmente a los técnicos y directivos de los procesos.
- Un incidente de **nivel alto** tendrá que comunicarse no solo a los técnicos, mandos y directivos al mando de los procesos afectados, sino también a la alta dirección.
- Un **incidente crítico** tendrá los mismos requerimientos que uno de nivel alto, y deberá comunicarse también a la propiedad, mediante el Consejo de Administración u órgano semejante. Además, mediante la figura del **portavoz**, muy probablemente a los medios de comunicación, por la repercusión social que pueda suponer y a nuestro portal de empleo para poder disponer temporalmente de los efectivos necesarios.

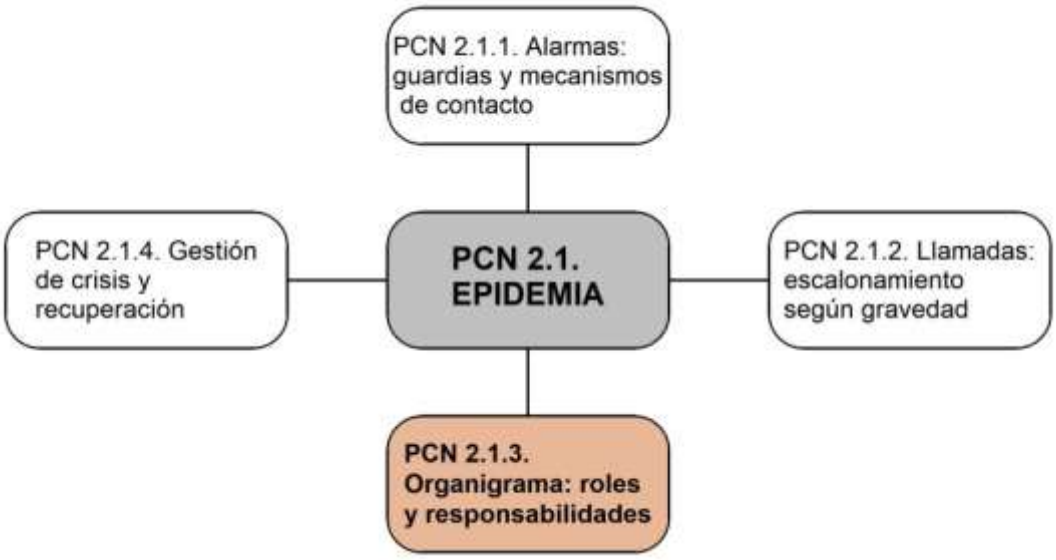
Haciendo balance, **ya tenemos las alarmas creadas** siguiendo un esquema lógico como el sugerido en el punto anterior, hemos decidido cuáles será los mecanismos de contacto y los destinatarios **y ahora sabemos cómo calificar los incidentes** por el daño que están produciendo en nuestros procesos. Todo ello nos va a dar más **oportunidades** en caso de interrupción (que tendríamos que haber explorado con simulacros). Pero no hemos definido **quién** ha de hacer esta calificación ni **qué responsabilidades** tienen otros miembros de la organización y tampoco la secuencia lógica de actuaciones en caso de crisis. Estos aspectos del **sistema de gestión de**

continuidad los trataremos en los puntos siguientes, donde vamos a repartir los distintos papeles (**PCN 2.1.3. Organigrama: roles y responsabilidades**) y e*l* guion (**PCN 2.1.4. Gestión de crisis y recuperación**) a seguir a distintos órganos o partes de la empresa.

PCN 2.1.3. Organigrama: roles y responsabilidades

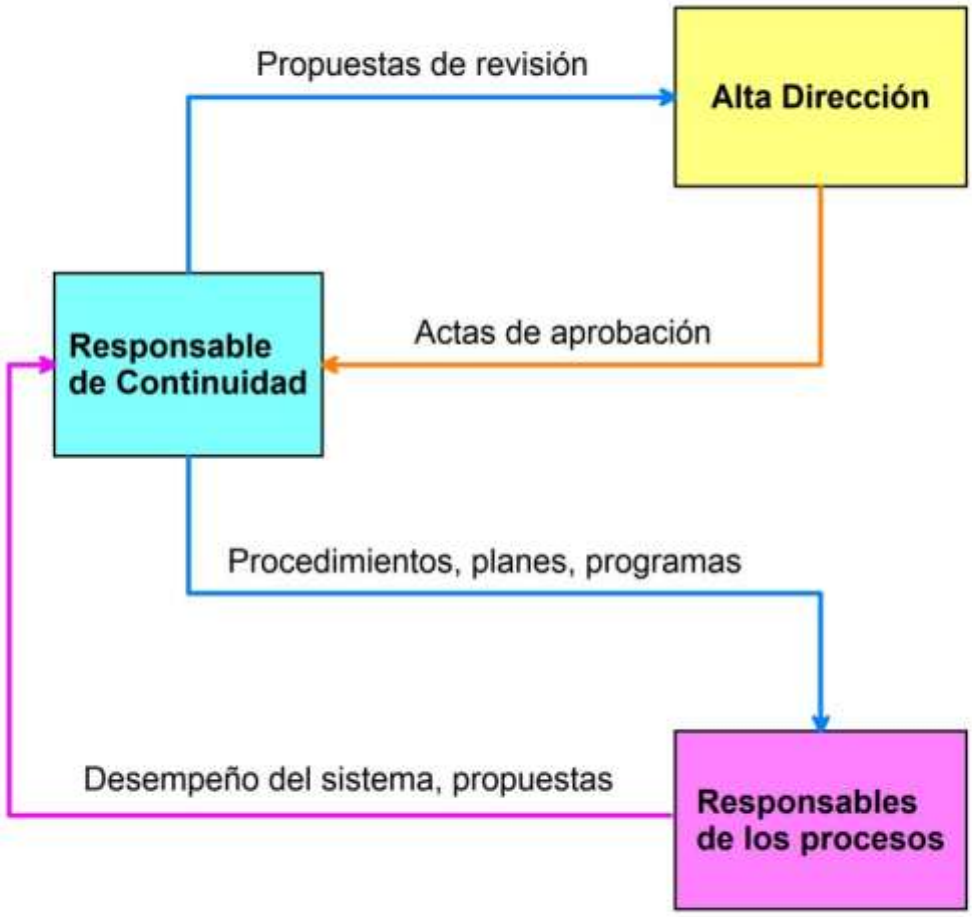
Cuando hay una situación que sobrepasa lo que es normal en el funcionamiento de una empresa o institución, se requiere una forma de organización específica para decidir de forma ágil y efectiva las mejores actuaciones. Para ello se constituye el gabinete de crisis.

No es lo mismo hacer funcionar rutinariamente una organización, que dirigirla en caso de crisis. En el funcionamiento normal cada directivo se encarga de una faceta del negocio y sigue las pautas que se han vuelto habituales, pero **en una crisis** las circunstancias han cambiado. Se necesita que cada acción que se decida se haga contando en ese momento con el **mayor consenso posible** considerando todas las implicaciones en las distintas facetas de la compañía, ya que se trata de unas circunstancias nuevas y el tiempo apremia.



Introducimos el organigrama que nos resuelve la cuestión de quien debe hacer qué cosas en un incidente.

Recordemos que en **PCN 1.4.1. Revisión sistemática**, introducíamos un esquema de los bucles de comunicación que se establecían para los procesos de revisión, que reproducimos ahora:



Bucles de comunicación para la revisión del sistema.

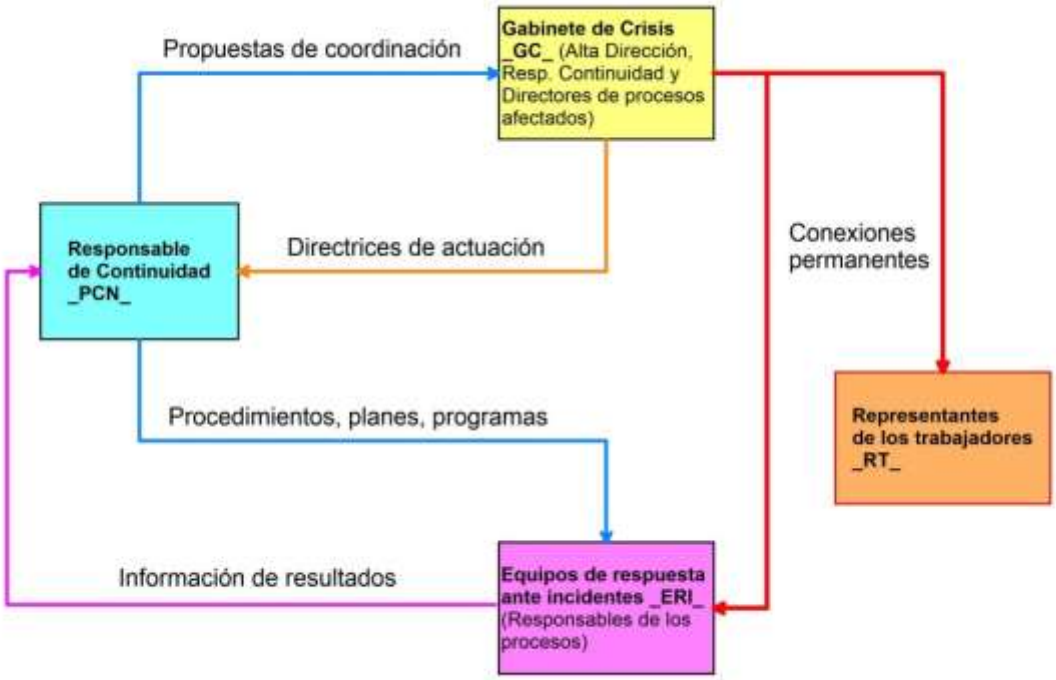
Aquello era en 'tiempo de paz', pero ahora la cosa se complica porque ha surgido un incidente grave, que lo hemos calificado de 'crisis' (Ver la entrada anterior **PCN 2.1.2. Llamadas: escalonamiento según gravedad**), y terminábamos la entrada sin haber determinado quienes han de actuar en estos casos. Quedaba claro que contamos con una Alta Dirección, que se reúnen periódicamente constituidos como Comité de Dirección, que hay un **responsable de la gestión de continuidad**, que representaremos por **_PCN_,** que generalmente es un director (si la empresa tiene suficiente tamaño) y que tenemos responsables de los procesos.

Organización y flujos de comunicación en caso de crisis

Cuando hay un incidente que puede derivar en **crisis** o en **desastre**, **se forman otras agrupaciones** en la empresa con la única misión de gestionar la situación. Aunque todos los demás órganos y departamentos habituales en la entidad siguen teniendo sus responsabilidades y siguen trabajando en ellas, **se agrupan la Alta Dirección, el responsable de continuidad _PCN_ y el responsable de los procesos afectados formando el gabinete de crisis _GC_**. Además, **los responsables de los procesos y sus técnicos y empleados clave forman los equipos de respuesta ante incidentes _ERI_**. Estos equipos están dirigidos por el director del proceso o departamento afectado y coordinados por su segundo en el escalafón y pasan a tener una línea directa con el **_GC_.**

Además, **entran en escena los representantes de los trabajadores _RT_** para tratar las cuestiones que afecten a la seguridad del personal y la organización del trabajo,

que tienen también una línea directa con el _**GC**_. Veamos cómo se modifican los bucles de relaciones:



Bucles de comunicación en tiempo de crisis.

Como puede verse, permanecen muchos de los bucles de 'tiempo de paz' con contenidos de la misma naturaleza, pero más frecuentes y ligeramente distintos

- Las propuestas de revisión del responsable de continuidad a la Alta Dirección, pasan a ser **propuestas *de* coordinación** al gabinete de crisis, porque se trata de trabajar lo más coordinados posibles, potenciando la acción de conjunto. Las actas de aprobación por parte de la Alta Dirección se transforman en **directrices de actuación** concretas para aplicar en el momento.
- La información de desempeño y propuestas que proporcionan los departamentos se convierte en información de los **resultados** (y **lecciones aprendidas**) de lo que se ha hecho para corregir el incidente que se pretende acabar.

Pero lo más significativo es los enlaces de comunicación directa entre el _**GC**_ **y los** _**ERI**_ , así como entre el _**GC**_ **y los** _**RT**_. Es decir: **se potencia la comunicación** a gran escala. Esta comunicación sirve:

- Para que el más importante órgano de dirección (_**GC**_) esté **informado** puntualmente de la situación por parte de los equipos que están trabajando en las tareas de recuperación de la actividad (_**ERI**_) y
- para que en el momento en que se necesite, se puedan **aprobar rápidamente medidas organizativas** de las que puede depender el éxito de las actuaciones.

Las funciones de cada grupo en caso de crisis se deducen de sus relaciones con los demás grupos, que como ya hemos dicho incluyen el desempeño normal de todos los demás departamentos.

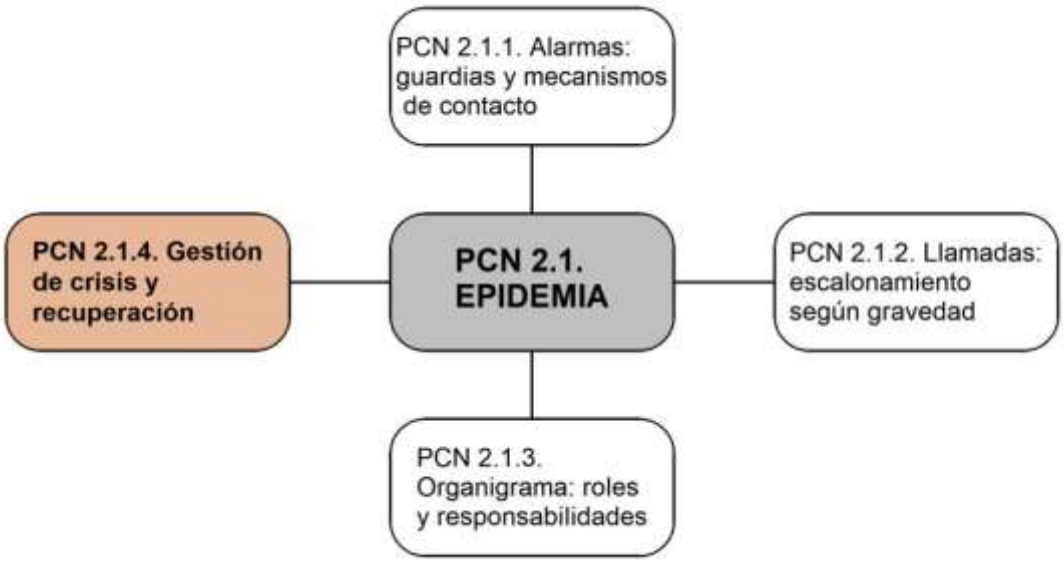
Podemos ahora aclarar que en **las alarmas** que definíamos en **PCN 2.1.1. Alarmas: guardias y mecanismos de contacto**, cuando hablamos de responsables de los distintos procesos, estábamos hablando de los _**ERI**_ correspondientes a los distintos procesos (Proceso A, Proceso B, etc.).

Ya tenemos definidos los **escenarios**, los **niveles de gravedad** de los incidentes, sabemos cuáles son los **mensajes** que debemos transmitir según los niveles de gravedad y tenemos identificados los **grupos** que van a actuar en caso de incidente (a los que les hemos asignado personaje en este *drama*) así como el contenido de **las comunicaciones** en sus relaciones. En la próxima entrada veremos cual será el guión, con la descripción de los distintos *actos en caso de crisis*.

PCN 2.1.4. Gestión de crisis y recuperación

Gran parte de los preparativos realizados hasta ahora nos ayudan para el tiempo en que tenemos que gestionar una crisis y su proceso de recuperación posterior. Según lo que hayamos aprendido estaremos en distinta disposición y con distintas posibilidades de éxito.

Para acabar de aprovechar y *sacarle todo el jugo* al caso de ***epidemia***, podemos tratar en esta entrada la **gestión de crisis**. Nos vendrá bien lo que hemos adelantado en entradas anteriores en la cuestión de las alarmas tanto en el contenido de los mensajes, como su escalado por gravedad. Ahora todo eso nos va a sonar en la puesta en práctica de estas técnicas cuando surja una cuestión que ponga a prueba nuestra capacidad de defensa y recuperación



La gestión de una crisis ya declarada es la parte nuclear de las actuaciones para las que nos hemos preparado

Las fases de la crisis

Las crisis, aunque tengan diversas causas, pasan por fases semejantes, de forma que los principios de actuación son también semejantes: Los resumió magistralmente **Julio César** tras su triunfo en la **batalla de Zela**, en Anatolia, en su conciso informe al Senado de Roma:

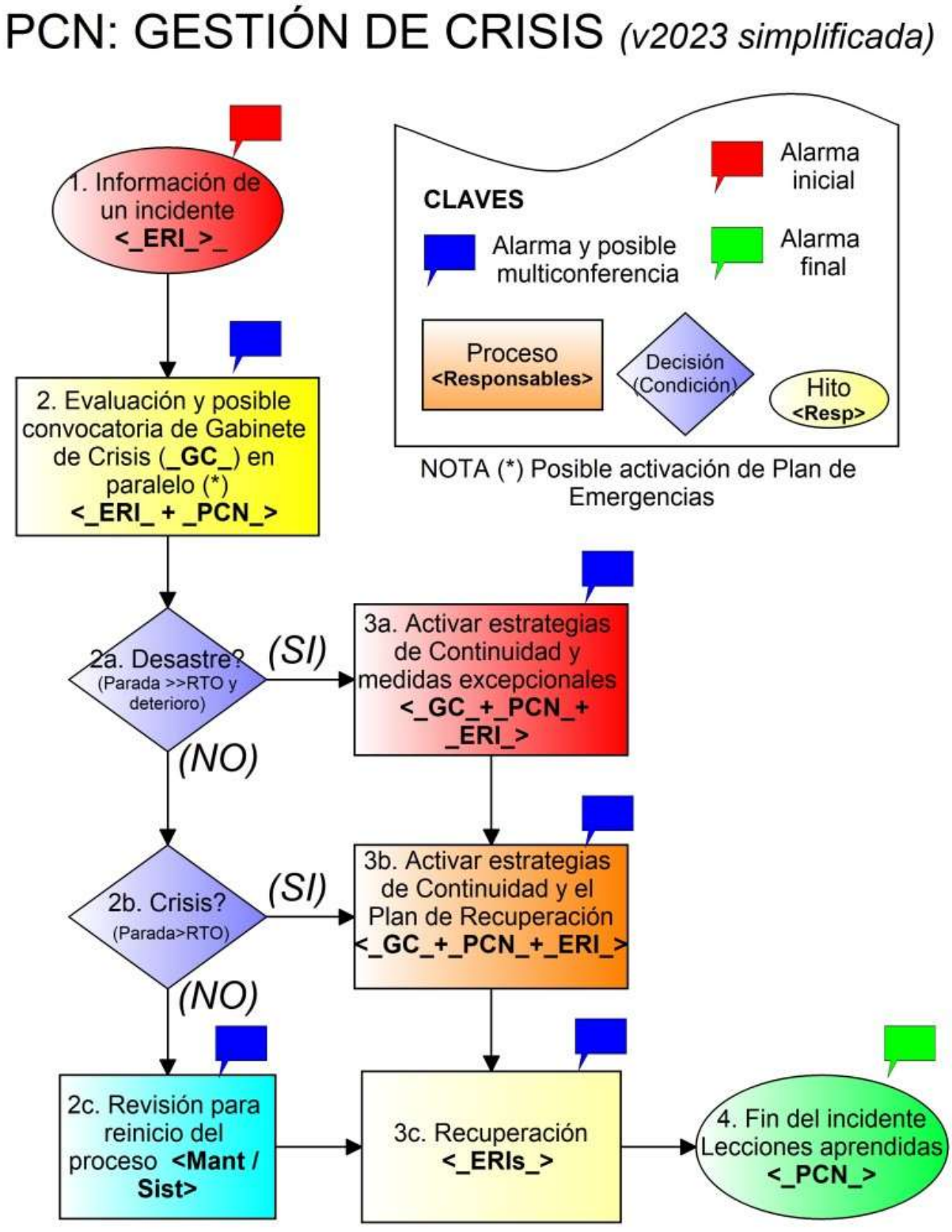
"(1.) **VENI,** (2.) **VIDI,** (3.) **VICI"** (Es decir: Llegué, vi y vencí).

Igual tenemos que hacer nosotros en nuestras crisis, y en general en cualquier actividad que requiera analizar una situación ante la que hay que dar una respuesta. Adaptado a nuestro mundo actual las fases serían las siguientes:

1. En la **primera fase** tomamos conciencia de que **tenemos un problema**.
2. Hay una **segunda fase** en que analizamos la situación y **determinamos la mejor estrategia** a emplear.
3. Posteriormente, en una **tercera fase**, tratamos de **resolver** la cuestión que afecta a nuestros procesos hasta lograr un resultado aceptable. Esta fase será más o menos compleja según sea la naturaleza y extensión del incidente.

4. Por último, en una **cuarta fase**, faltaría hacer balance de nuestra propia actuación para obtener las **lecciones aprendidas**, que dejaremos escritas como registro para estar mejor preparados en una futura ocasión.

Para más información sobre esta forma de pensar, podemos visitar lo publicado en **VENI, VIDI, VICI, (pero también SCRIPSI)**. Veamos cómo puede hacerse esto en el mundo actual, detallado en el flujograma del siguiente gráfico.



Gestión de crisis y de recuperación, explicada mediante un diagrama de flujo.

Las fases que se muestran en el gráfico significan lo siguiente en la terminología propia de continuidad de negocio, numeradas para relacionarlas con las fases indicadas arriba:

1. El relato de la **gestión de crisis** comienza con **un aviso** procedente del equipo que está a cargo del proceso afectado, por simplificar consideraremos que es el propio Equipo de Respuesta ante Incidentes _**ERI**_.
2. La fase de **evaluación** se inicia con una serie de apreciaciones realizadas en grupo, participando ***colegiadamente*** el responsable de continuidad _**PCN**_ y el _**ERI**_ del proceso afectado. *Primero se ponen en lo peor*, determinando sucesivamente si estamos ante un **desastre**, una **crisis** o un **simple incidente** tipo avería o error que no llegará a interrumpir el proceso por un tiempo inaceptable.
3. En función del nivel de gravedad del incidente, se activan las **estrategias de continuidad** previstas en los **planes de continuidad** establecidos para el escenario del incidente, y en su caso medidas excepcionales para reparar las instalaciones; o el **Plan de Recuperación** para el proceso afectado; o directamente se procede a la Recuperación si ni siquiera se ha llegado al nivel de crisis; todo ello en manos de los _**ERIs**_ correspondientes.
4. Por último, cuando se restablecen los procesos, el responsable de continuidad _**PCN**_ decreta el **final del incidente** y dirige la elaboración del informe de **lecciones aprendidas**, para registro del incidente y memoria posterior, que sirve para aprender de la experiencia.

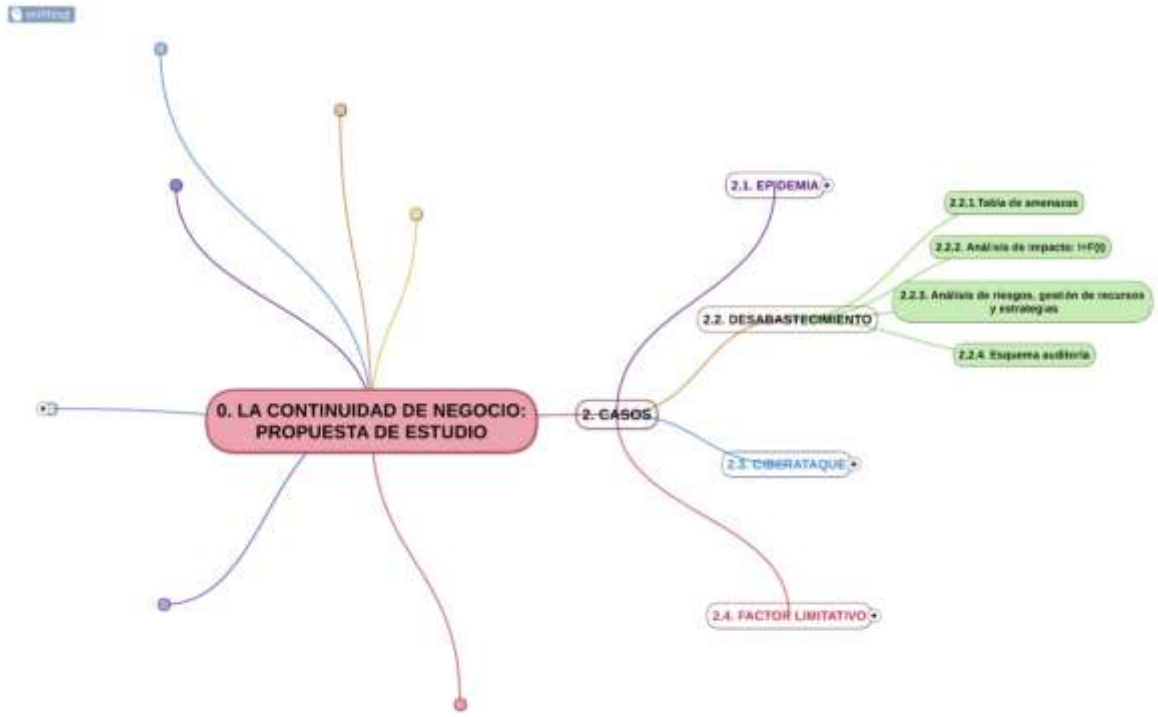
Todo el proceso está jalonado de ocasiones en las que se pueden lanzar distintas **alarmas** (que son en síntesis avisos para un grupo y pueden servir también para dar información del estado de avance de las acciones) a petición del responsable de continuidad _**PCN**_. Alguna de estas alarmas puede convocar reuniones o multiconferencias que pueden ser tipo **videoconferencia** o presenciales. Dada la experiencia durante la COVID-19 que las reuniones se realizaban mayoritariamente por videoconferencia on-line, hemos incorporado esta forma de comunicación que resulta práctica cuando queremos inmediatez y los asistentes están cada uno en un sitio.

En el apartado **PCN 2.3.1. Pirámide de procedimientos**, veremos cómo son todos esos procedimientos que hemos mencionado, que han de estar disponibles para su empleo en el momento en que son precisos, tanto para la gestión de crisis, como para recuperación. El primer tipo de procedimiento (el que trate sobre la gestión de crisis), seguirá el esquema aquí descrito. El segundo tipo (el que trate sobre la recuperación) dependerá totalmente de la naturaleza de cada proceso.

PCN 2.2. DESABASTECIMIENTO

Hemos tratado el caso de la falta de personal por una pandemia, que hemos aprovechado directamente para ver las formas de tratar con la crisis. Ahora empezaremos una serie de entradas sobre el caso de desabastecimiento, que nos permitirá explorar las herramientas de previsión, a fin de controlar mejor nuestros procesos y nuestras dependencias antes de que se produzca una crisis.

Los suministros pueden ser nuestras **dependencias** más delicadas, ya que en gran medida tenemos poco control sobre ellos puesto que no dependen de nosotros y suelen suponer una proporción alta de los costes, e incluso ser exclusivos y difíciles de sustituir. Pero podemos hacer mucho por asegurarnos que no van a causar más problemas de los necesarios. Recordemos el **PCN 1.2.4. Escenarios**, para fundamentar por qué calificamos numéricamente, en un escenario de **desabastecimiento de suministros, el nivel de riesgo como medio** (3) para la continuidad. Naturalmente, todo esto es un ejemplo y cada entidad debe adaptar a su caso a la situación lo más aproximadamente a la real.



Prepararnos para un caso de desabastecimiento pondrá el foco en el Análisis de Impacto y de riesgo.

Estrategias en caso de desabastecimiento

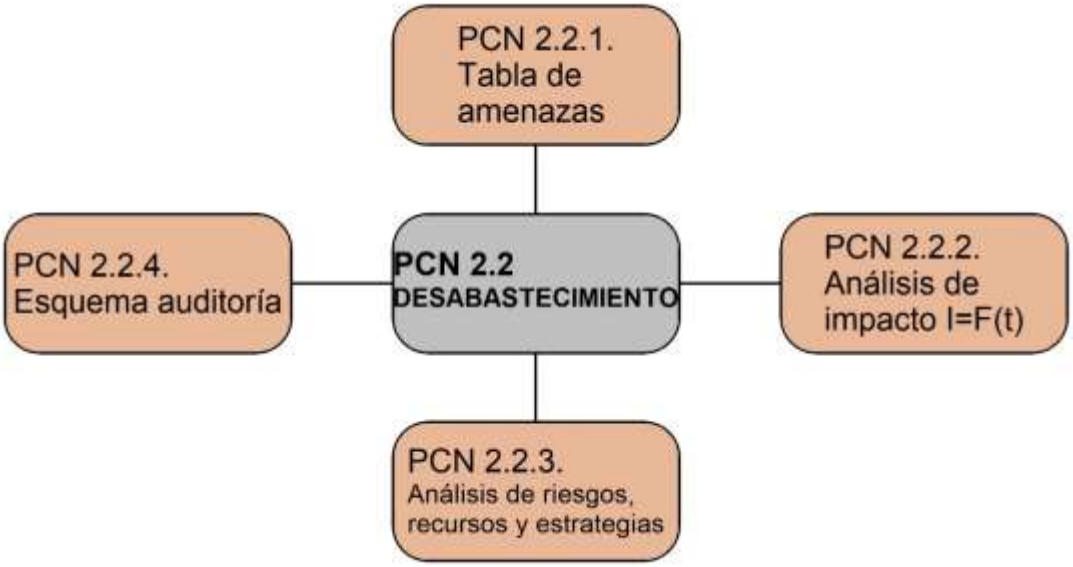
Las **estrategias básicas de continuidad** para un caso de **desabastecimiento** pueden ser las siguientes:

- **Proveedores alternativos**, proveedores en la proximidad, autoproducción de los componentes clave. La **globalización** y la deslocalización han hecho que muchos de los suministros provengan del otro lado del mundo. Los incidentes de las rutas comerciales y los escenarios de guerra están cambiando esto. Mientras tanto, siempre queda **buscar otros proveedores,** aunque no tengan precios tan bajos, y asignarles una parte de los pedidos de suministro a fin de

que se conviertan en habituales y puedan suplir en caso de necesidad a los lejanos más económicos.

- **Aumentar existencias** de suministros clave para cubrir toda una serie completa que deban incorporar los mismos componentes. Esta es una estrategia que puede dejar sin liquidez a la compañía, durante un tiempo, pero puede tener la ventaja de disponer de algo exclusivo que sea capaz de diferenciarnos de otros productores. También está el peligro de que las oscilaciones de precios conviertan esta actuación en *suicida* si no somos capaces de predecir con exactitud la evolución del mercado y compramos (involuntariamente) suministros en lo alto de la ola de sus precios. Aunque si en lugar de verlo como peligro, acertamos en comprar a un precio que resulta ser bajo respecto del precio futuro, puede que sea la más rentable de las decisiones. Los *stocks* son activos que, aunque quitan **liquidez**, en un momento dado pueden salvar la empresa de tener números rojos en un mal año.
- Fijar en los contratos con proveedores **penalizaciones suficientes** para desmotivar la falta de suministro por parte de los proveedores. Este tipo de decisiones tiene el inconveniente de que en realidad estaremos subiendo los precios, que nos los repercutirá el proveedor a modo de autoseguro. Tampoco evitará la falta de suministro, sólo que no lo hará tan impactante en un periodo corto de tiempo en nuestras cuentas.
- Diseñar nuestros procesos para **reducir el impacto** de la falta de ciertos suministros. Esto es un movimiento básico de la genialidad de quien, usando elementos comunes, es capaz de vender algo extraordinario. Muchas veces avances de este tipo se protegen con **patentes**, porque el empleo de elementos corrientes está al alcance de cualquiera.
- Asegurar los lugares de **almacenamiento** distintos de los lugares de producción, a fin de que una indisponibilidad de acceso a un local no impida seguir accediendo al resto de los suministros en otro. Una frase muy larga para decir que no hay que jugárselo todo a una carta. La **diversificación** es interesante en la resolución de este tipo de situaciones.
- Hacer **análisis de solvencia** económica y de producción de nuestros proveedores. Esta es una gran tarea en manos de los gestores de compras, si pueden obtener los datos necesarios, para asegurarse de que nuestros proveedores no van a dejar de serlo por problemas económicos o por "caprichos" de sus directivos, en busca de una mayor rentabilidad si deciden suministrar a partir de un momento otro tipo de productos en lugar de los que necesitamos.

Nos va a ayudar a evitar o minimizar el efecto de distintos incidentes con los suministros, todo lo que aprendimos cuando elaboramos en **PCN 1.1.1. Talones de Aquiles** la tabla **inventario de nuestros procesos** y en **PCN 1.1.2. Dependencias** invitábamos a asociar en ese inventario de procesos y de operaciones nuestras posibles **dependencias**. Deberemos estudiar ahora en detalle esa **tabla**, que se convertirá en una **tabla de amenazas**, para estar seguros de que nuestras debilidades clave no queden al descubierto frente a amenazas de desabastecimiento, tenga este el origen que tenga.



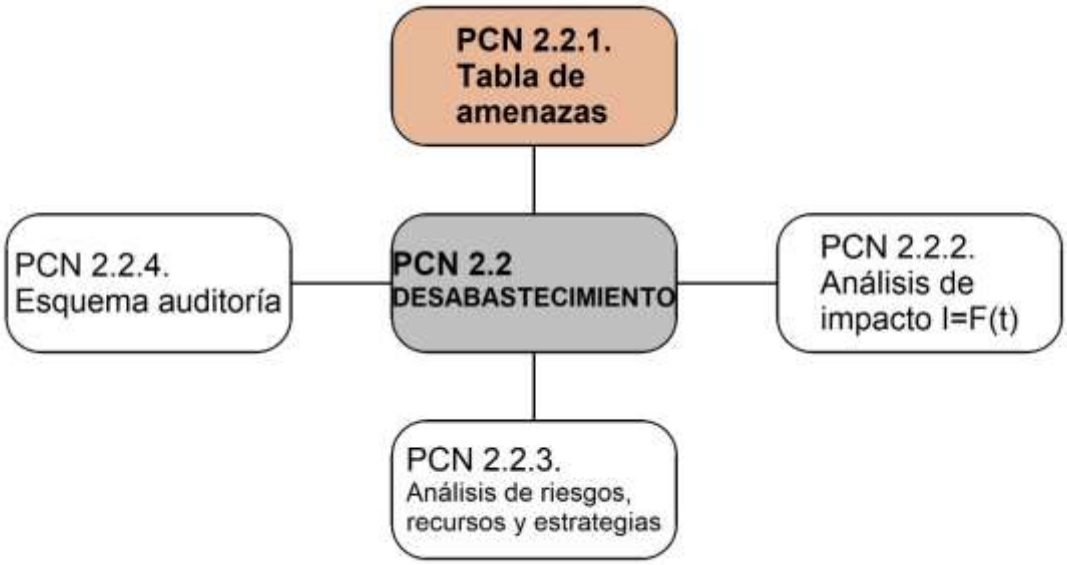
El caso de desabastecimiento y las herramientas que tenemos para prever cómo mitigarlo.

En las próximas entradas veremos justamente la **tabla de amenazas** adaptada a nuestro negocio, haremos más objetivo nuestro **Análisis de Impacto referido al tiempo** de interrupción, analizaremos y adaptaremos los **riesgos y estrategias** a nuestra tabla de amenazas en un ***proceso recursivo*** que no deje ningún aspecto al azar y comprobaremos la solidez de todo ello con una **auditoría interna**.

PCN 2.2.1. Tabla de amenazas

Una epidemia, que es el caso que hemos visto primero, tiene un comportamiento bastante aleatorio. Pero el desabastecimiento, que veremos ahora, puede tratarse de una forma más previsible porque depende más de decisiones tomadas por nuestra organización. En esta parte del libro, trataremos de prevenir todo lo que está en nuestra mano.

En **PCN 1.2.4. Escenarios**, manejábamos una **tabla de amenazas o escenarios** simplificada para poder introducir una evaluación numérica de los distintos **escenarios de riesgo**, que son las manifestaciones de las **amenazas** en los procesos. El escenario de epidemia era la manifestación de una enfermedad infecciosa a gran escala que afecta severamente incapacitando a nuestro personal, que es siempre la parte más importante de los procesos de la organización. De forma semejante, el escenario de **desabastecimiento** es la manifestación de la carestía de suministros en las partes clave de nuestro proceso en que entran esos suministros. La **tabla de amenazas** a la que nos referimos es la **lista de los escenarios** y *subescenarios* que presumiblemente pueden afectar a distintas partes de nuestros procesos.



La tabla de amenazas detallará casos o escenarios que importan en nuestros procesos y operaciones.

En la entrada citada, **PCN 1.2.4. Escenarios**, ya hicimos una primera aproximación para tener un inventario simplificado de escenarios, creando una **tabla de amenazas o escenarios** con solo cuatro supuestos (epidemia, desabastecimiento, ciberataque y factores limitativos), que son los que han dado origen a esta segunda parte del libro. Continuando con la idea de aprovechar los supuestos para ampliar las técnicas que se suelen manejar en continuidad de negocio, ahora lo que nos hemos propuesto es ver qué tenemos que hacer para mejorar nuestra **tabla de amenazas – Análisis de escenarios**, nuestro Análisis de **Impacto**, la Apreciación de **Riesgos** y la **Auditoría** del sistema.

Identificando amenazas

En el caso de la **tabla de amenazas o escenarios**, resulta muy efectivo partir de un esquema o **diagrama de flujo** detallado del proceso, como los que se incluyen en las empresas cuando se definen los componentes o composición de los productos. Hay

en internet **aplicaciones especializadas** para crearlos. Estos esquemas, representados de forma gráfica, dan cuenta de las operaciones y los componentes o características que se agregan en cada operación o fase del proceso (por ejemplo, **ver este esquema de Wikipedia** "Archivo: Esquema Proceso Monitorio en España"). Pueden tener también indicación de la parte de las instalaciones, maquinaria o sistemas participantes en cada operación (como **este otro ejemplo**: "Archivo: Diagrama Proceso Kraft.jpg.") y cuántos operarios se precisan en cada operación, con detalle de sus categorías o atribuciones.

Basta con observar un diagrama bien elaborado con idea de continuidad, para determinar si el proceso tiene **puntos susceptibles o sensibles ante distintas amenazas**, que pueden provenir de distintos orígenes dependiendo de la parte del proceso que se trate. Cualquier experto que trabaje en el proceso sabe, en qué fase, una interrupción puede suponer la parada de todo el proceso.

Valorando cada una de las amenazas específicas de nuestros procesos, tenemos un baremo interesantísimo para decidir **prioridades** de actuación en nuestro afán de proteger de la mejor forma todos los procesos con el mínimo de recursos. Como ya hicimos también los deberes de conocer para cada proceso y operación cuáles eran nuestros talones de Aquiles y sobre todo sus dependencias, esto servirá para preparar los cambios en los procesos y en sus dependencias, con tal de **evitar la exposición al riesgo**, que gracias al diagrama del proceso podemos ahora visualizar gráfica e intuitivamente de un vistazo.

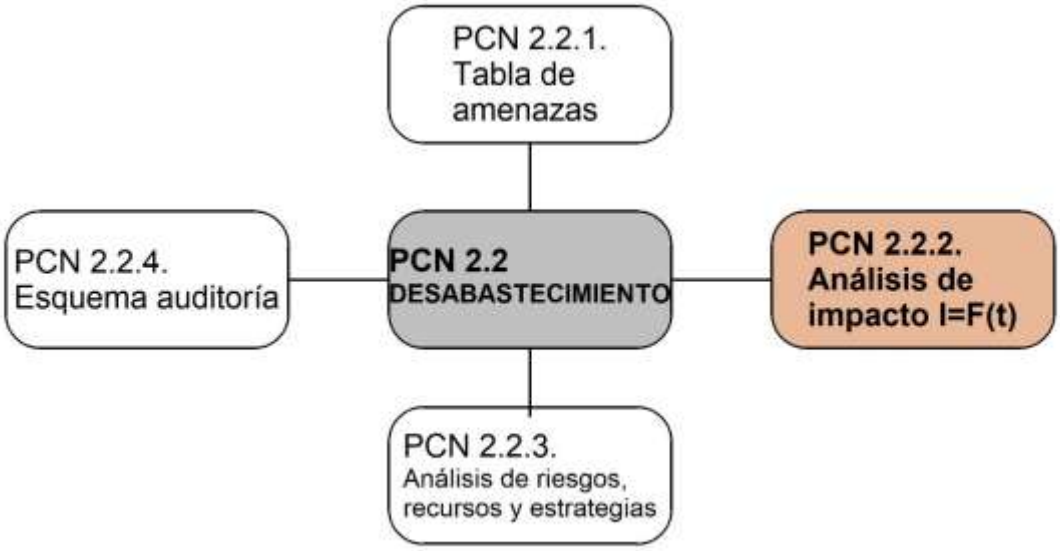
Vemos que la continuidad de negocio es un **proceso reiterativo**, que empieza de forma bastante general, para acabar detallando todos los puntos de interés. Si en una primera aproximación, el análisis de escenarios nos valía para tener una idea de qué tipo de problemas o riesgos nos preocupaba más y saber aproximadamente cuales eran los tipos de riesgos más dañinos, expandiendo más el análisis a las partes que forman los procesos podemos llegar a una situación en que tenemos toda la capacidad para detener o mitigar cualquier amenaza de forma efectiva. Seguimos básicamente, y en nuestra peculiar forma, el **ciclo de Deming**.

PCN 2.2.2. Análisis de Impacto I=F(t)

Continuaremos aquí lo que empezamos en nuestro análisis de debilidades. Ya vamos viendo que la gestión de continuidad es un proceso reiterativo, con el que en cada vuelta vamos ahondando más en las cuestiones tratadas. El Análisis de Impacto es el tipo de análisis más característico de la continuidad y define las exigencias de disponibilidad de cada proceso.

En el punto **PCN 1.1.4. Recursos necesarios** remitíamos al punto actual para tratar las debilidades de nuestro sistema después de haber recopilado información para cada proceso y operación, de los **talones de Aquiles, dependencias, personal clave y recursos necesarios.** Estas eran nuestras fuentes de debilidades. Conocerlas nos servirá para fijar los **Tiempos Objetivos de Recuperación (RTO)** cuando determinemos primero de un modo objetivo el periodo de tiempo en el que una interrupción nos lleva a un **estado inaceptable** o **Periodo Máximo Permisible de Disrupción (MTPD)**. **Disrupción** es interrupción o mal funcionamiento que aparece en un momento inoportuno, no planificado. Para simplificar diremos a veces simplemente ***interrupción*** del servicio *normal*.

Se trata de conocer los **requisitos** de nuestros procesos a fin de fijar las **prioridades**. Cada proceso quedará así caracterizado por un valor de MTPD, que es una medida de la exigencia de disponibilidad. Cuanto más corto sea ese MTPD, más alta es la exigencia de disponibilidad. Cuando tengamos esa información de todos los procesos, tras una parada generalizada de la compañía como la que puede producirse por un **desabastecimiento** (pero también en caso de epidemia, de ciberataque o de factores limitativos de la producción), sabremos qué procesos necesitan **atención prioritaria** para arrancar primero.



El Análisis de Impacto en función del tiempo lleva implícita la determinación de la disponibilidad.

Evaluando el impacto

Nos interesa una valoración de impacto objetiva y que emplee el valor de una variable que afecte a todos los procesos. Ya tenemos determinados los procesos a los que les aplicaremos el estudio, que son los de la lista que elaboramos en **PCN 1.1.4.**

Recursos necesarios. Como el estudio ha de determinar el impacto en función del **tiempo** de 'disrupción', elegiremos esta variable como principal. Vamos a elegir **tres dimensiones de impacto** y estudiaremos su evolución a lo largo del tiempo de interrupción. Cada empresa debe elegir las que considere importantes para su tipo de actividad. En este ejemplo serán:

- **Impacto económico**: será cualquier *extracoste* no previsto que se origine como consecuencia de la interrupción. Puede deberse a una **multa** por incumplir las normas o leyes aplicables, una **penalización** por retrasos en una entrega, una **indemnización** por perjuicios a otras entidades, un coste excesivo de **mantenimiento**, etcétera.
- **Impacto reputacional**: es el que se produce por la actividad en **redes sociales** o en prensa por perjuicios o falta de atención producida por nuestra interrupción. Este impacto, para corregirlo, requiere un coste de la campaña de imagen que se lanza para compensarlo una **rebaja** de los precios de venta, **ofertas** y compensaciones de cualquier clase no previstas para hacer más atractivos nuestros servicios.
- **Impacto operativo**: se trata de perjuicios **en el programa de clientes** que necesitan nuestros productos o servicios en fechas determinadas y que tienen que optar por parar o por encontrar alternativas en la competencia con repercusión en futuros pedidos o encargos.

El tiempo como variable principal

Una interrupción afecta de distinta forma a los distintos procesos, pero cualquier **incumplimiento** puede definirse en función del tiempo, es decir, ocurrirá fatalmente un incumplimiento si transcurrido un determinado tiempo no hemos resuelto aún el problema.

Vamos a emplear una tabla, por ejemplo, la que se muestra abajo y vamos a determinar qué nivel de impacto tenemos tras distintas unidades de tiempo de interrupción. El tiempo de interrupción lo valoramos en principio como **minutos, horas, días, semanas, meses, trimestres**... (podemos detallar más las unidades, por ejemplo 1 día, 2 días, etc., pero lo que nos interesa es la escala de tiempo en la que se mueve el proceso en estudio (cuán corta o larga es), para poder comparar distintos procesos. Es evidente que una disrupción en unos procesos producirá un impacto inaceptable en cuestión de minutos, en otros casos en cuestión de horas, en otros días, y así sucesivamente. Consideraremos que una disrupción tiene uno de los tres niveles siguientes:

- **Un nivel 1**, si el impacto **no** llega a un valor inaceptable, porque **no** se produce ningún incumplimiento.
- **Un nivel 2**, si la interrupción da como resultado **un incumplimiento** o una situación **inaceptable**.
- **Un nivel 3**, cuando la interrupción da como resultado que nuestro proceso queda *fuera del mercado* y vamos a perder los pedidos o el servicio que prestamos porque perderíamos la confianza de los clientes. Es equivalente decir que 3 es un nivel ***crítico***.

Dimensión	Nivel	minutos	horas	días	semanas	meses	trimestres	Detalle	Conclusión
Impacto económico	3								
	2								
	1								
Impacto reputacional	3								
	2								
	1								
Impacto operativo	3								
	2								
	1								
Total de puntos									
MTPD									
RTO									

Ejemplo de tabla para cálculo del Análisis de Impacto (es una hoja de cálculo).

Conforme vayamos añadiendo los valores que consideramos que han de tener las calificaciones de las distintas dimensiones al ir aumentando el tiempo de disrupción, podemos haber programado los rangos de la hoja con un ***formato condicional*** (consultar con el informático de la casa), para que coloree las casillas en función de los valores. La disposición de los valores bajos en una fila, los medios en otra y los altos en la tercera para cada dimensión hace que se vea de forma gráfica (y escalonada) el resultado. Si hemos dejado espacio para comentarios podremos justificar de manera más precisa los valores que asignamos.

Periodo Máximo Permisible de Disrupción (MTPD) y Tiempo Objetivo de Recuperación (RTO)

Al final podremos sumar los valores para cada unidad de tiempo del impacto en cada una de las dimensiones. Como un solo incumplimiento elevará la calificación de una dimensión de '1' a '2', si la suma para un periodo de tiempo supera '1'+'1'+'1' = '3' (es decir, si la suma es 4 ó más) habremos alcanzado el **Periodo Máximo Permisible de Disrupción (MTPD)**. Luego, como pretendemos recuperar la producción normal antes de que se alcance el MTPD, fijaremos el valor del **RTO** en un periodo menor. En el ejemplo, el escalado de impacto de '3' a '4' se produce en 'días' (concretamente 3 días) y entonces fijamos el RTO en un tiempo menor de días (concretamente 2 días o 48 horas).

Dimensión	Nivel	minutos	horas	días	semanas	meses	trimestres	Detalle	Conclusión
Impacto económico	3							Penalización si t> 3 días	La penalización económica determina el MTPD y el RTO en este caso
	2			2	2	2			
	1		1						
Impacto reputacional	3							Por encima de 3 días crítica en redes	
	2				2	2			
	1		1	1					
Impacto operativo	3					3		Clientes necesitan servicio en pocos días	
	2				2				
	1		1	1					
Total de puntos		0	3	4	6	7		Tomamos 3 días como máximo periodo permisible con el objetivo de restaurar el servicio en 48 horas	
MTPD				3 días					
RTO			48 horas						

Ejemplo de Análisis de Impacto para un proceso. Hay que hacer el análisis para cada proceso.

La hoja de cálculo conteniendo la tabla se puede también preparar para que nos calcule las sumas y coloree con un mapa de color los resultados, con lo que facilita la identificación de los tiempos. Podemos incluso sofisticarla más para que calcule los **RTO** más convenientes, si bien yo prefiero determinarlos según la experiencia de los técnicos del proceso.

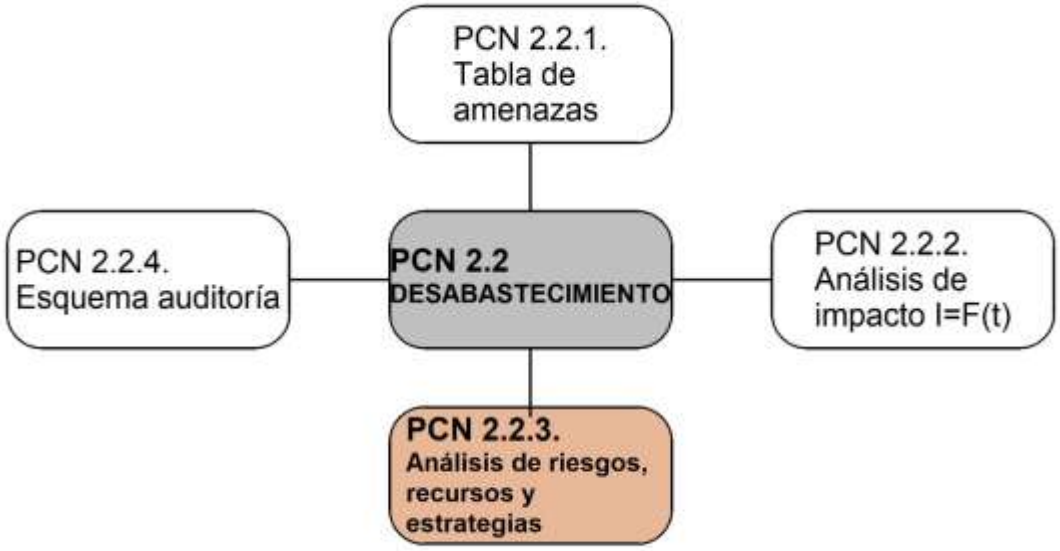
El **Análisis de Impacto** no ha incluido cuál es la amenaza o el escenario que produce el problema, en nuestro caso de estudio que recordemos era el desabastecimiento, pero en este punto ya resulta irrelevante. Esa información será importante para los procedimientos de recuperación. Por esta parte, la información de los valores de **MTPD** y **RTO** que hay que **determinar para cada proceso** de nuestro inventario, constituye un *mapa de la situación de los procesos* que los clasifica inmediatamente por **disponibilidad** y los resultados son **válidos para cualquier escenario**. Cada información tiene una utilidad. En el siguiente punto veremos nuestra ampliación de la apreciación de riesgos.

Por ahora, lo que nos debe quedar claro es que una simple tabla, como la de nuestro inventario o mapa de procesos, del que hablábamos en **PCN 1. 1. 4. Recursos necesarios,** en donde hayamos añadido otras dos columnas, con los datos de **MTPD** y **RTO**, nos da una información valiosa de por dónde tenemos que empezar en caso de crisis para controlar la situación y también para fijar qué inversiones se requieren planificar para reforzar los procesos que tengan un RTO más exigente. Es decir: esta herramienta, la del Análisis de Impacto sirve de hecho para fijar **prioridades de actuación** a corto y medio plazo.

PCN 2.2.3. Análisis de riesgos, recursos y estrategias

Siguiendo con el supuesto de desabastecimiento, y una vez hecho nuestro Análisis de Impacto en función del tiempo I=F(t) en el punto anterior, hemos de ver de qué forma establecemos concretamente los riesgos y habilitamos recursos y estrategias, engarzándolo todo mediante procedimientos operativos y de recuperación en caso de que se materialice la crisis.

Estamos en disposición de preparar los procedimientos concretos empezando por aquellos que vimos que tenían más prioridad tras elaborar en **PCN 2.2.1. Tabla de amenazas** nuestra lista de posibles fuentes de problemas, en particular los suministros más relevantes; conociendo en detalle cuáles son las necesidades de disponibilidad que vimos en **PCN 2.2.2. Análisis de Impacto I=F(t)**, ahora que ya sabemos con cuánto tiempo contamos; y el personal y los recursos necesarios para cada proceso, que ya conocemos desde **PCN 1.1.4. Recursos necesarios**. Por tanto, para preparar ahora los procedimientos disponemos de mucha información y muy precisa acerca del proceso y sus implicaciones, que nos va a servir para que los operarios de los _**ERI**_ puedan actuar de la forma más adecuada para resolver los problemas planteados si se produce una interrupción y el Gabinete de Crisis _**GC**_ tenga en su mano toda la información de base para tomar las mejores decisiones. **Ver PCN 2.1.3. Organigrama: roles y responsabilidades**, donde se introducen las funciones de los distintos actores en caso de crisis.



El Análisis de riesgos, recursos y estrategias como complemento operativo de la Tabla de amenazas y del Análisis de Impacto.

La agenda de los riesgos

Es el momento de hacer varias cosas **en relación con los riesgos**:

- **Evaluar los riesgos** específicos de nuestro proceso, como por ejemplo determinar qué suministros pueden ser más problemáticos.
- Determinar qué **actuaciones preventivas** realizaremos para tener más seguridad. Es decir, fijar cuales de las estrategias típicas para conjurar un desabastecimiento nos interesan más.

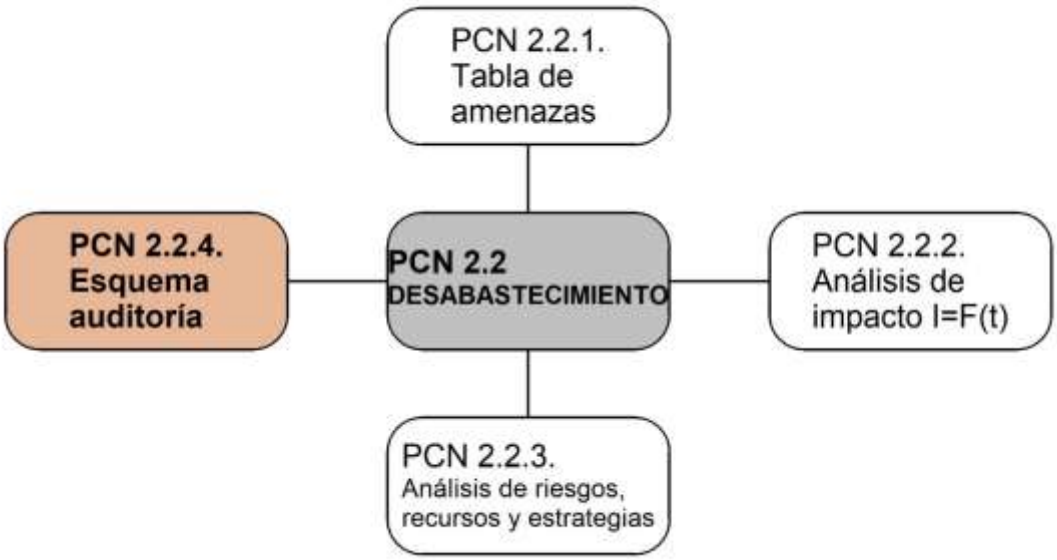
- Determinar **cuánto riesgo estamos dispuestos a correr**, asumiendo las consecuencias, en relación con la apetencia de riesgo de nuestro negocio.
- Determinar por tanto cuáles serán estratégicamente los **riesgos que vamos a reducir actuando** sobre mecanismos que eviten la exposición al riesgo y que reduzcan su probabilidad de ocurrencia.
- **Redactar procedimientos** que digan a quién avisar en caso de incidente, lo que hay que hacer si, a pesar de todo, las amenazas se materializan y se llega a un incidente grave. Incluirán cuáles serán puestos clave y sustitutos, operaciones a efectuar, controles, cómo determinar si la situación escala a crisis y si se ha normalizado, qué información se debe dejar registrada en caso de incidente y a quién habrá que informar, etc.

A medida que vamos volviendo de forma repetitiva, sobre los problemas que ya fuimos tratando, se va creando la **estructura del sistema de gestión** específico de la continuidad. En el caso de la epidemia nos centramos en las cuestiones que más tenían que ver con el personal, fijando la organización y las responsabilidades, las alarmas y sus contenidos y las estrategias básicas de incidentes relativos al personal. Ahora hemos ampliado el círculo añadiendo la estructura que afecta más a la parte de las instalaciones y sus suministros. Nos quedará por introducir, aprovechando el escenario de un ciberataque, pautas que nos van a ser útiles sobre todo en sistemas y seguridad de la información. Pero antes veremos en el siguiente punto cómo nos pueden ayudar las **auditorías**.

PCN 2.2.4. Esquema de auditoría

La forma más rápida de verificar la validez de los trabajos realizados para preparar un sistema capaz de gestionar la continuidad de negocio es hacer una auditoría. La auditoría compara el sistema establecido con las prescripciones de la norma y como resultado pone de manifiesto las carencias o desvíos de lo que deben ser buenas prácticas, ayudando a plantear objetivos para corregir.

Es una tendencia natural, excepto en las personas que por su naturaleza son pesimistas, pensar que en un determinado asunto hacemos las cosas bien, y si no es así tampoco debe ser tan grave. Por eso es buena idea dejarse aconsejar por alguien que sabe del asunto, para saber su opinión de lo que no está bien y cómo cree que se tendría que hacer para corregirlo. Este es el trabajo que realizan los **auditores**. Se trata de expertos con suficiente **independencia e inmunidad**, con un amplio conocimiento del sistema de gestión y de las normas de aplicación, que elaboran informes útiles para corregir y mejorar la forma de hacer las cosas y el sistema que sustenta las operaciones.



La auditoría para comprobar si lo estamos haciendo bien y qué hay que corregir.

Las **auditorías** pueden ser **internas**, que son las que se hacen por encargo de la propia organización para conocer sus fallos y planificar las correcciones necesarias, y las **externas**, que se emplean a modo de examen para conseguir una **certificación** del sistema o bien son encargadas por los clientes para juzgar la solvencia de nuestro sistema. Aún con esa distinción **siguen el mismo patrón**:

Pasos de la auditoría

- La entidad **encarga la auditoría**:
  - Si es **interna,** se encarga a un equipo que tenga experiencia en auditorías, conozca las normas que rigen el sistema a auditar y goce de **independencia** en su trabajo y libertad para formular conclusiones sin represalias que pudieran provenir de los auditados o de la Dirección (**inmunidad**). El responsable de la auditoría puede ser un técnico del equipo, que no haya sido quien ha diseñado el sistema y del que no dependa la operativa en caso de incidente.

    - Si es **externa** se encarga a una organización que tenga suficiente prestigio para servir de testigo fiable del (buen) estado y eficacia del sistema. Por supuesto sus conclusiones estarán sujetas al **secreto** para que no sean empleadas por posibles competidores.
- Hay un **trabajo previo** de preparación:
    - **El auditor** y su equipo se presentan y muestran su ***currículum*** (que avala su experiencia y conocimientos) a la empresa auditada.
    - Se identifica **la norma** que va a servir de patrón en la auditoría. En continuidad de negocio es la **UNE-EN ISO 22301**.
    - Tras determinar el **alcance** de la auditoría preparan la lista con las cuestiones o aspectos a investigar; y presentan su **programa** a los auditados para fijar las sesiones que se tendrán que acordar entre ambos.
    - **Los auditados** preparan la información requerida y las **evidencias** que prueben o avalen sus posteriores respuestas.
- Luego viene la fase de **revisión documental**:
    - El auditor solicita revisar la documentación relevante del sistema, tanto procedimientos como registros.
    - Los auditados entregan la documentación solicitada.
    - El auditor toma nota de las divergencias observadas entre lo prescrito por la norma y los documentos revisados.
- Sigue con la fase de **trabajo de campo**:
    - Se visitan conjuntamente (el auditor y los responsables de los procesos) los espacios donde se desarrollan los trabajos y
    - se determina la adecuación de las operaciones a los documentos que las definen y a la norma de referencia.
    - El auditor entrevista a los operarios para ver su grado de conocimiento y concienciación.
    - El auditor toma nota de las divergencias observadas entre lo prescrito por la norma y las operaciones revisadas.
- Por último, el auditor elabora el **informe de auditoría**:
    - El auditor prepara un **informe con las conclusiones, las no-conformidades, observaciones y los puntos fuertes** observados.
    - El informe se presenta a los auditados en una reunión formal.
- **Acciones correctivas** posteriores al informe de auditoría:
    - La organización prepara una **planificación** para llevar a cabo las **acciones correctivas**, con indicación de responsables, plazos y forma de verificar que se han llevado a cabo.
    - Posteriormente la planificación de las acciones correctivas se integra en los **planes de empresa** para su seguimiento y control, hasta total resolución de las no-conformidades.

A falta de detalles formales y aspectos técnicos acerca de cómo manejar el sistema documental y del uso de ciertas herramientas de gestión, que veremos en las últimas entradas, hemos superado ya el ecuador de este texto y nos vamos acercando progresivamente a nuestro objetivo de montar un sistema sólido de continuidad de negocio. El próximo grupo de entradas estará dedicado a las particularidades de un sistema preparado para gestionar la ciberseguridad y aún nos quedará otra última parte práctica o técnica para mejorar la fluidez de nuestras operaciones de negocio, antes de la recta final, que nos servirá para 'sacar nota'.

PCN 2.3. CIBERATAQUE

El ciberataque es una amenaza que, aunque proceda de la otra parte del mundo, se materializa en nuestras propias instalaciones. En la tabla de escenarios que planteábamos como ejemplo lo calificábamos con el mayor nivel de importancia entre los escenarios mencionados. Emplearemos en este supuesto todas las estructuras que hemos ido creando y otras específicas.

Dado que se trata de la amenaza que nos puede afectar con más probabilidad y con unos resultados potencialmente graves (ver **PCN 1.2.4. Escenarios**), hemos dejado este escenario para después de haber visto los escenarios de epidemia y desabastecimiento, para que nos haya dado tiempo a:

- Preparar nuestro **organigrama** y crear el Gabinete de Crisis _**GC**_;
- Haber definido los Equipos de Respuesta ante Incidentes _**ERI**_ ;
- Tener preparadas las **alarmas** y la lista de **llamadas**,
- Haber preparado nuestros flujos de trabajo de la **gestión de crisis** y recuperación;
- Haber visto **qué sistemas pueden fallar** en caso de ciberataque;
- Tener realizado el **análisis de impacto** para conocer la exigencia de **disponibilidad** de cada sistema;
- Haber planteado las mejores **estrategias** de actuación en caso de incidente;
- Haber comprobado con una **auditoría** que todo ello es correcto.

(Ya hemos ido advirtiendo en varias ocasiones que el sistema de gestión de continuidad de negocio es un sistema recursivo hasta el aburrimiento. Después de haber comprobado algo, lo mejor es volver a comprobarlo más tarde a ver si nos hemos dejado algo).

El ciberataque, nuestro tercer escenario de estudio.

Estrategias para ciberataque

Las **estrategias básicas** para estar preparados contra **ciberataque** son:

- **Copias de seguridad** (también llamadas ***backup***). Con una mayor o menor sofisticación, las copias de seguridad de la documentación de la organización son vitales para recuperarse de un ciberataque. Han de realizarse con suficiente frecuencia para que las pérdidas de datos sean asumibles y no causen ningún trastorno importante. El equipamiento empleado para ello puede variar mucho tanto en *software* como en espacios o mecanismos de almacenamiento. **Un autónomo** tendrá seguramente suficiente con hacer una copia de seguridad diaria y mantener todos los originales o justificantes de la información por si hay que volver a 'picar' los datos desde la última copia buena hasta el momento del incidente; **pero una empresa de tamaño medio** ya necesitará equipos especiales para hacer copias incrementales a ser posible en continuo a fin de no crear un serio problema con la falta de datos. Las copias han de ser **redundantes** por si, para colmo de males, fallara el soporte que las contiene.
- **Virtualización** de sistemas: hace más fácil su mantenimiento y recuperación en caso de incidente y optimiza los recursos centralizados disponibles.
- **CPD de respaldo**. Este es un elemento que se necesita a partir de un volumen importante de datos a mantener y según la exigencia de **disponibilidad** resultante del **Análisis de Impacto** realizado.
- **Almacenamiento en la nube**. Trabajar con la nube como respaldo tiene muchas ventajas, y no sólo el acceso a los datos desde cualquier dispositivo conectado. También permite disfrutar de medidas de seguridad proporcionadas por el proveedor del alojamiento, generalmente superiores y más actualizadas que las disponibles en el lugar de trabajo. En algunos casos, por seguridad, no será posible alojar ciertos datos en la nube.
- **Segmentación** en bloques de los equipos de la red, para evitar que todos se puedan contagiar por estar en la misma red.
- **SOC** siempre vigilante. El _**ERI**_ de seguridad informática se suele conocer como _**SOC**_ (= *Security Operations Center*) y son los primeros que deben detectar que algo va mal con la seguridad de los datos. Sea interno o subcontratado lo normal es que siempre tenga **personal de guardia**. Sus tareas abarcan desde **detección de incidentes** a puesta en práctica de las estrategias aprobadas por la entidad para la **gestión de un ciberataque**.
- **Buenas prácticas** de uso de los sistemas. La difusión de las buenas prácticas y el uso de **accesos restringidos** a la información y los datos que deba manejar cada cual, junto con mantener las actualizaciones al día, son algunas de las estrategias básicas para reducir la exposición al riesgo.

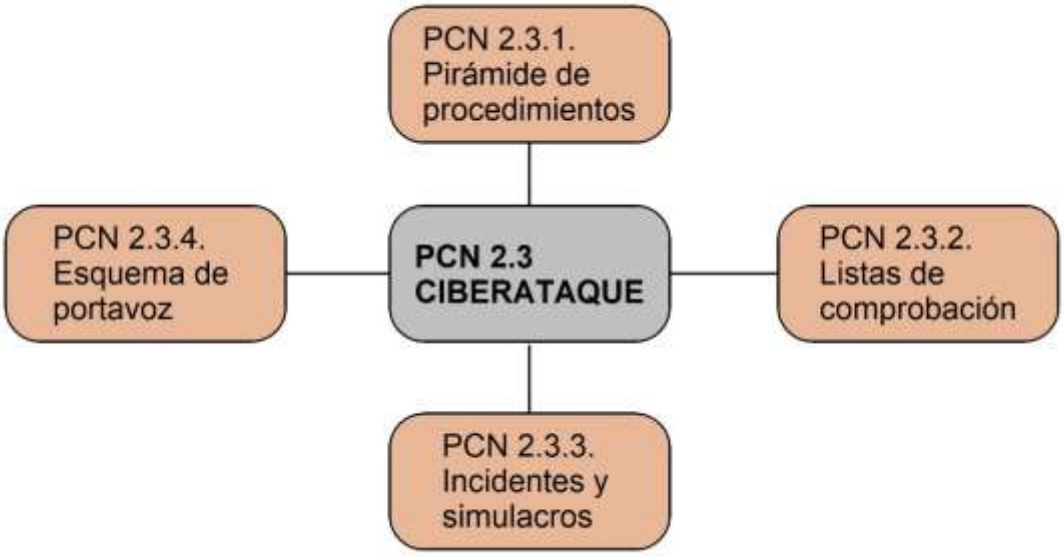
Gestión de Crisis de ciberataque

En caso de que, pese a las estrategias de prevención, se produzca el **ciber incidente** la **secuencia de acontecimientos** puede seguir esta línea de actuaciones, aunque dependerá del tipo de ataque y de las características de nuestros sistemas:

- **Aviso** de un número suficiente de usuarios de comportamiento anómalo de los sistemas que permita concluir que no se trata de un hecho aislado, sino de un ataque intencionado.
- **Primer análisis de la gravedad** del incidente, para conocer su gravedad potencial, de la que dependerán distintas actuaciones posteriores.

    - Si el incidente supera los parámetros fijados para ello, comunicación a las autoridades del **Centro Nacional de Ciberseguridad** (**en España, para las empresas, INCIBE**). Además del importante servicio que presta, podemos contribuir muy positivamente mediante nuestras comunicaciones de un ciberataque (al igual que ocurre con el control de las enfermedades infecciosas y el Centro Nacional de Control de Enfermedades, cuando se comunica la incidencia de un patógeno peligroso). Esto favorece la **acción coordinada** en todo el entorno nacional y previene la infección de muchos más sistemas, por las alertas que se pueden lanzar cuando se detectan ciberataques en masa.
- Medidas de **contención**. Desconexión de la red de los equipos infectados presuntamente (para que no sigan contagiando a otros).
- **Formateo** en caso de que no permita reposición y posterior **reinstalación** del sistema en los ordenadores afectados, o **parcheado** (actualización) de los sistemas con los antídotos adecuados en caso de que sea suficiente.
- **Reposición de los datos** limpios procedentes de las copias de seguridad.
- **Análisis *forense*** final.
- Realización de un **informe completo** como registro.
- **Comunicar los resultados finales** a la Dirección y en su caso al Centro Nacional de Ciberseguridad.
- Dejar constancia de las **lecciones aprendidas** y elaborar en su caso un **plan de actuaciones** de corrección.

El ciberataque nos va a aprovechar para indicar otras líneas de actuación formales, que nos servirán de guía y de preparación.



Oportunidades que nos ofrece el ciberataque para mejorar el sistema de continuidad.

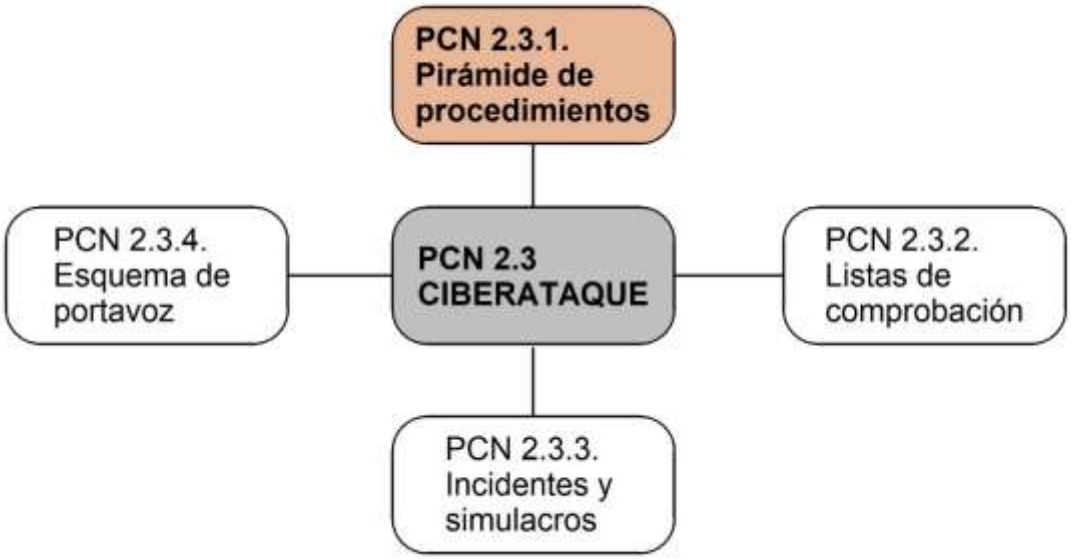
Veremos la estructura que pueden tener los documentos del sistema, que llamaremos '**Pirámide de procedimientos**', porque tendrán varios niveles. Este tipo de incidentes tiene el inconveniente de que se necesita documentar muy bien todos los pasos, pero la ventaja de que muchos de los registros se generan automáticamente en forma de *logs* y detalles de cómo ha funcionado el sistema. Estas **listas de comprobación** y otras que generaremos con fines de asegurar que hacemos lo que tenemos que hacer según los casos, facilitarán el trabajo con muy poco esfuerzo. Emplearemos los **simulacros** para verificar el grado de concienciación del personal y para practicar la

secuencia de las operaciones a realizar en un incidente y, por último, dentro de esta parte, veremos la misión y forma de actuación de un buen **portavoz de crisis**.

PCN 2.3.1. Pirámide de procedimientos

El título 'pirámide' viene al caso porque la documentación de continuidad de negocio, y en particular la de ciberseguridad, suele tener varios niveles: la más general es mantenida por el responsable de continuidad y aprobada por la Alta Dirección, la de cada proceso es mantenida por sus responsables y la de operaciones más técnicas por los responsables de los _ERI_.

Pirámide es un nombre un poco pretencioso, aunque muy descriptivo, ya que generalmente hay un sólo manual, varios procedimientos de procesos y un buen número de documentos técnicos, listas de comprobación, e incluso recordatorios o avisos prácticos que marcan los pasos a seguir en las cuestiones más corrientes.



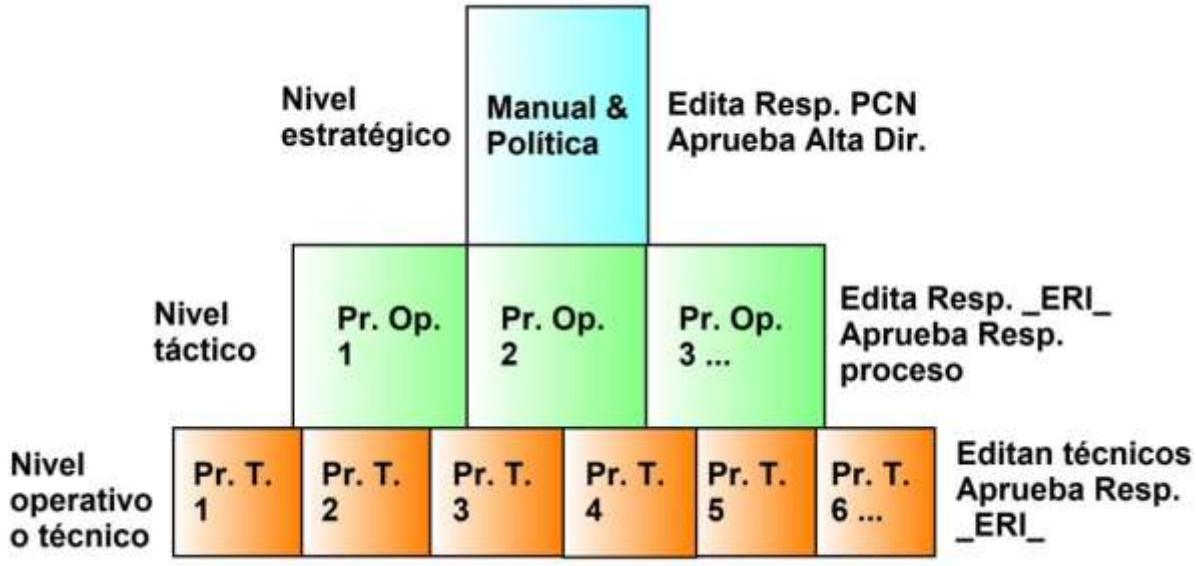
Los procedimientos son parte esencial de la infraestructura de continuidad.

La actividad de continuidad de negocio está organizada en un grado notable basada en **procedimientos** que hacen que estén previstas muchas de las pautas de actuación para evitar improvisaciones y aplicar los recursos lo más eficientemente. Para nuestro fin consideraremos que los niveles de organización empresarial son **nivel estratégico, táctico y operativo o técnico.** Los procedimientos de un nivel se heredan en los niveles inferiores. Por ejemplo, un procedimiento estratégico (el manual) es de aplicación en todos los procesos.

- **Nivel estratégico**. El nivel estratégico de documentación es competencia del responsable de continuidad _**PCN**_ y es aprobado por la Alta Dirección. Este nivel de procedimientos y de registros tiene como finalidad hacer que la Alta Dirección intervenga en los procesos estratégicos de la continuidad, como son:
  - La aprobación del **manual** (o documento de mayor nivel, que regula las cuestiones generales de la organización y contiene la política de la misma);
  - La aprobación de la **revisión por la Dirección** que incluye el conocimiento del desempeño, de los resultados y controles más generales que afectan a toda la empresa, la aprobación de las propuestas y objetivos tácticos anuales;
  - El control de las operaciones de **gestión de crisis** y contacto con los _ERI_ y con los representantes de los trabajadores.

- **Nivel táctico**. Se trata del nivel de **los responsables de los procesos**. Es buena práctica que sean editados por los responsables de los _**ERI**_, ya que luego tendrán que llevarlos a la práctica y serán aprobados por los responsables de los procesos. Este nivel de procedimientos y de registros tiene como finalidad que los procesos se desarrollen conforme a las instrucciones, conocimientos y experiencia de sus jefes responsables, ya que serán los que den cuentas de sus desempeños:
    - Comprenden la **organización del trabajo** con detalle de las dependencias y suministros y sus definiciones y calidades mínimas exigibles, necesidades de infraestructura, contactos de personal, proveedores y clientes clave;
    - Los **procedimientos de recuperación** y las relaciones con otros equipos y otros procesos;
    - Las **comprobaciones** que todo está funcionando con normalidad y de acuerdo a cómo debería.
- **Nivel operativo o técnico**. Este nivel es el de los técnicos a cargo de las distintas operaciones de los procesos. Son documentos de carácter técnico, necesarios para llevar a cabo las tareas y tiene como finalidad que los técnicos trabajen de forma coordinada con los equipos, en particular en situación de incidente. Pueden tomar diversas formas:
    - **Esquemas y diagramas** de los procesos;
    - Listas de **comprobación**;
    - **Registros** de funcionamiento de los sistemas;
    - Conjunto de **buenas prácticas** en el trabajo para mejorar la calidad y la eficiencia;
    - Esquemas de **normas** con indicación de tareas obligatorias, etc.

Esquema de la 'pirámide de procedimientos'



Esquema de la pirámide de procedimientos.

Otras indicaciones normativas. Los procedimientos internos son imprescindibles, pero los responsables de los procesos tienen que tener también acceso a las normas y leyes de aplicación, de forma que no quede ningún aspecto de normalización por considerar.

La documentación como acumulación del conocimiento sobre las mejores formas de actuación. Hay que ir acostumbrando al personal que ha de trabajar en un proceso, que la documentación no solo tiene un objeto formal, sino que debe ser la forma de acumular el mejor conocimiento sobre los procesos.

La documentación como **fuente de aprendizaje**. Como tal acumulación de conocimiento hay que pensar en la documentación como la fuente primaria de aprendizaje más importante, ya que puede consultarse mientras se trabaja, pero también tomar sus textos como un libro, distribuido en múltiples documentos sobre los procesos.

La documentación como **base para la mejora continua**. La organización por procesos tiene la virtud de que permite mejorarlos continuamente. Sólo puede mejorarse un procedimiento que existe, y que está escrito. A base de versiones del mismo se va viendo además cuál es la evolución del pensamiento relacionado con este.

La documentación prueba que se han previsto las **mejores prácticas**. El carácter probatorio de la documentación es el motivo por el que en las auditorías, antes incluso de la visita a los procesos, el trabajo que efectúan los auditores consiste en una revisión a fondo de la documentación. Se conoce mucho del funcionamiento de una empresa estudiando sus procedimientos y revisando sus registros.

En el próximo punto insistiremos en la utilidad de las **listas de comprobación** y la documentación de nivel técnico.

PCN 2.3.2. Listas de comprobación

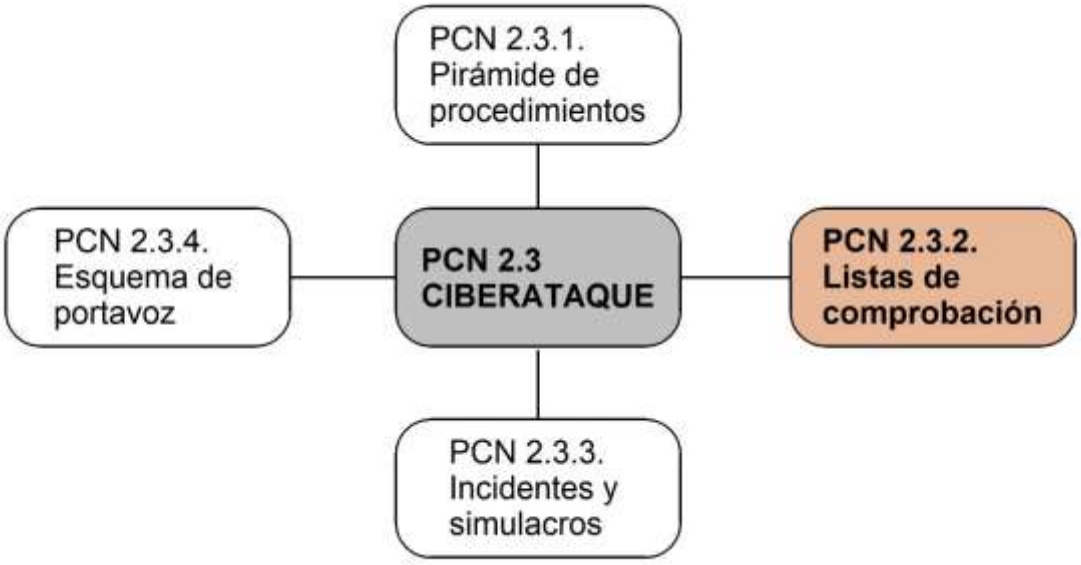
Puede que en una empresa, por su tamaño o por lo simples de sus procesos, no haya demasiados procedimientos que escribir. Incluso en empresas grandes, no siempre hace falta dedicar demasiados esfuerzos, o no siempre hay recursos para ello. Una lista de comprobación es una opción que puede ayudar a documentar los procesos, sobre todo a nivel de operación.

En lo que se refiere a la **ciberseguridad**, las **listas de comprobación** son de aplicación en multitud de ocasiones. Cuando hablamos de las listas de comprobación nos estamos refiriendo a apuntes o anotaciones útiles, que pueden adoptar diversas formas:

- Una **lista simple** es una relación de elementos, acerca de un asunto, que nos resulta útil para un fin atemporal, cuando se dan ciertas circunstancias. Es también conocida como ***check list***. Podemos pensar en las listas que tienen los talleres de coche para asegurarse de que realizan todas las comprobaciones programadas en el mantenimiento periódico.
- Un **flujograma** es muy útil para indicar la marcha de un proceso y de sus opciones y bucles, cuando se trata de conocer los distintos caminos que recorrerá la acción en función de bucles según lo que se decide o se comprueba del estado de la situación.
    - **UML (Lenguaje unificado de modelado)** es un método normalizado muy interesante para aplicarlo a este tipo de diagramas, porque pretende seguir unas reglas sencillas que todo el mundo puede entender y utilizar para identificar un hito, una operación, una condición o un camino lógico.
    - La ventaja de una lista de comprobación gráfica o diagrama es que lo gráfico se asimila mejor y cuesta menos que describir conceptos redactando 'sujeto – verbo y predicado'.
    - Los gráficos son un lenguaje universal (ver los carteles sobre cómo actuar en caso de emergencia).
    - Los **emoticonos** sirven de ejemplo de elementos gráficos, capaces de transmitir información emocional. Esto da una idea de la potencia de los métodos gráficos.
- Un **registro** puede adoptar también el modelo de lista de preguntas-respuestas. Algo muy útil cuando se emplea una lista de comprobación para aprovechar y recoger información estructurada del sistema.
    - **Normalizar los modelos** de registro es una tarea que hará que los datos que vamos tomando de los procesos tengan no solo validez, sino que se puedan emplear en bases de datos relacionales. Se puede ver fácilmente que no hace falta un gran número de modelos. Con un número limitado de registros normalizados puede manejarse una gran cantidad de información sobre la marcha de la empresa.
    - El formato preferente en la toma y registro de datos se ha de elegir con lógica, pero siempre resulta conveniente un formato estructurado como ***CSV (Comma Separated Values***) porque permite abrir el archivo con múltiples programas: Bloc de notas, Excel, **SQlite**, etc.
    - Bases de datos: **SQlite** es una base de datos relacional gratuita que no necesita grandes equipamientos para funcionar, tiene programas gráficos que sirven para editarlas en Windows, Linux, Android, etc., y puede resolver la cuestión de manejar una gran cantidad de información

en una pequeña empresa, alimentada con ficheros **CSV** que se han cumplimentado empleando listas de comprobación o de registro elementales.

- Una forma combinada **mitad lista-mitad registro** es cuando en una pantalla de seguimiento de una operación, por ejemplo, los pasos necesarios para 'levantar' el sistema después de una parada programada o por un incidente, aparecen con un **mapa de calor** aquellas partes que ya se han logrado y las que aún están en marcha y las que quedarían a la espera. Este tipo de comprobaciones hacen de semáforo de las actuaciones y ayudan a visualizar inmediatamente lo terminado y lo que falta. Las hojas de cálculo tienen funciones para lograr este efecto con 'formato condicional' en el que se pueden elegir los colores a representar.



Las listas de comprobación en el contexto de ciberataques.

Listas de comprobación como proto-procedimientos

Otro interesante punto de vista es emplear el recurso de una lista de comprobación como un **proto-procedimiento**. Se empieza reflejando los datos relevantes de cómo ha de ser el trabajo en una lista de comprobación, sin 'literatura', para acabar finalmente añadiendo lo que hace que el documento pueda considerarse un procedimiento formal. Incluso podemos tener una lista de comprobación que nos diga cuáles son los puntos que nos faltan para lograr ese objetivo. Por si alguien no lo tiene claro, un **procedimiento formal** debería tener al menos los siguientes elementos:

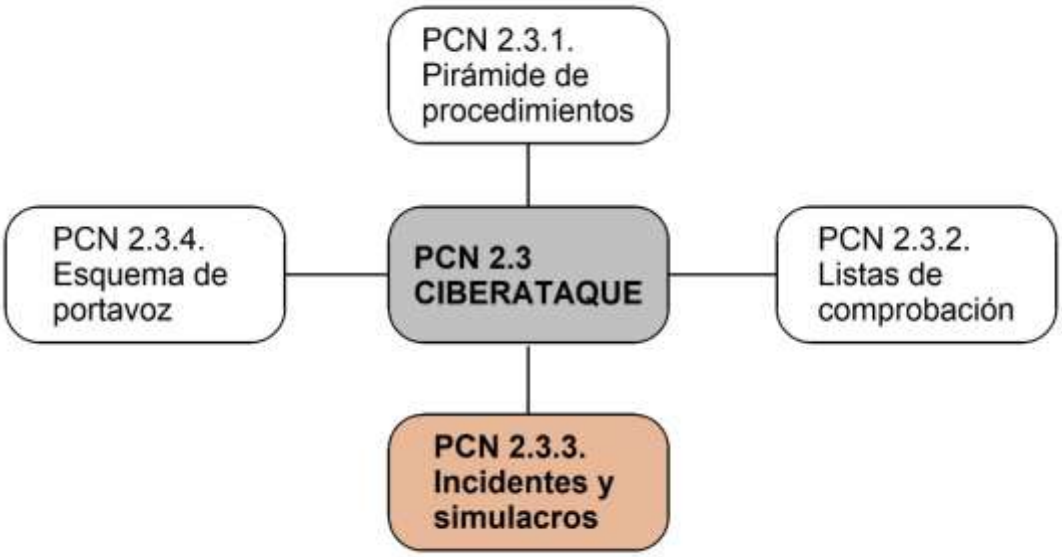
- **Nombre** del objeto del procedimiento visible en la primera página, dejando claro quiénes son los destinatarios del documento.
- **Versión** (un número principal de versión, seguido de otro número de modificaciones de pequeña envergadura o simples revisiones).
- Indicación del **editor, revisor y aprobador** del documento.
- **Fechas** de edición, revisión y aprobación.
- **Control de cambios** para que quede claro porqué se ha llegado a la versión actual.
- **Calificación** de su grado de confidencialidad.

- **Contenido**. Esta parte ocupa la mayor cantidad de espacio en el texto, aunque puede reducirse a una lista de comprobación.
- **Referencias** (por ejemplo, normativa que sigue) y documentos relacionados
- **Caducidad** del documento (puede reflejarse el dato en otro documento general, por ejemplo, indicando que tendrá validez de un año desde la última aprobación).

PCN 2.3.3. Incidentes y simulacros

Dada la velocidad con la que suceden las cosas en los sistemas informáticos, los incidentes y los simulacros que los reproducen, puede que tengan que tratarse con mucha más frecuencia y en un tiempo más breve. La ciberseguridad es por tanto el mejor ambiente para sacar partido de todo lo que puede aportar la resolución de un incidente.

Aunque los incidentes son desagradables, superarlos hace que podamos acumular experiencia en su resolución. En cualquier caso, ya hablábamos en **PCN 1.4.2. Lecciones aprendidas**, sobre la importancia de aprovechar la experiencia y de qué manera reflejar en el informe de lecciones aprendidas los conocimientos que se desprenden del caso.



Los simulacros ligados al estudio de los ciberataques.

Cómo organizar un simulacro

Nunca insistiremos bastante sobre la conveniencia de emplear l**os propios procesos como elementos de experimentación** y de prueba. Cualquier aproximación al proceso, como puede ser un experimento a escala, nos dará información y pistas para completar una investigación y siempre será respetable. Pero lo que más se parecerá al proceso que queremos dominar es el mismo proceso. Esto vale lo mismo para el desarrollo de un nuevo producto o servicio como para ver la forma de proteger los puntos débiles del mismo frente a un incidente. Por eso son importantes los **experimentos mentales**, planteando las preguntas tipo "***¿Y si…?***" y pensando en qué tipo de respuesta nos encontraríamos como consecuencia.

Por lo tanto, para **que un simulacro sea una fuente de conocimiento** ha de ser lo más parecido a la *vida real*. Es típico empezar una programación de simulacros, cuando no se tiene ninguna experiencia, guionizando todo como si de una representación teatral se tratara, incluidas fichas para cada grupo de actores para que sepan cómo deben actuar. El resultado más aproximado de esto será una mayor o menor consecución de que lo representado se parezca a la realidad. Pero tiene el enorme inconveniente de que no obliga a los participantes en el simulacro a revisar los procedimientos y a

pensar por sí mismos, con lo que no se interiorizan las consecuencias y no se aprende nada. Esto está bien para una primera ocasión, pero luego no es lo mejor.

Un simulacro, por tanto, tiene que tener varias fases y ser lo más realista posible (sin tener que parar el proceso necesariamente):

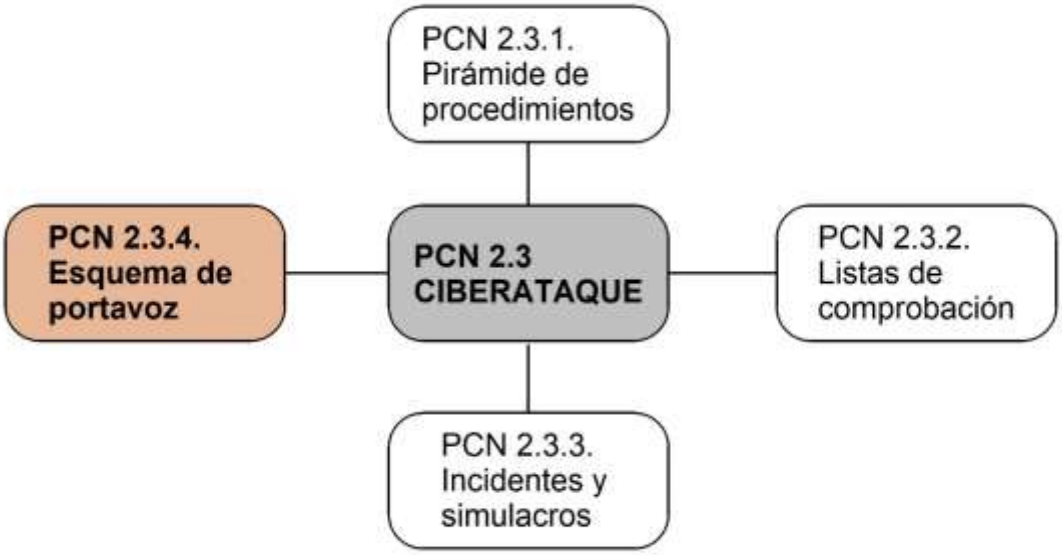
- **Programación** (anual). Las cosas que queramos que se hagan han de programarse, para involucrar a todo el mundo y para estar seguros de que pondremos los medios para lograrlo.
- **Reunión preparatoria**. Con anterioridad al mismo, reunión del responsable de continuidad _**PCN**_ y los equipos de respuesta ante incidentes implicados _**ERI**_ para ver los detalles del simulacro planteado. Confirmar condiciones, fecha, hora, procesos implicados y consecuencias para la producción.
- **Comunicación**. Comunicar y acordar en su caso con los responsables de los procesos los detalles propuestos, sin que haya difusión de los mismos al personal participante.
- **Revisión de los procedimientos**, las alarmas, las listas de contactos y actualización de lo que se detecte incorrecto, antes de la realización del simulacro. Estas revisiones se comunicarán por los canales habituales si hay modificaciones que deba conocer el personal participante. Este es el primer resultado del simulacro, antes incluso de su realización, que aprovecha para revisarlo todo.
- **Designación de testigos** que tomarán notas en el tiempo que duren las pruebas, a fin de aportarlos al informe unificado. Pueden ser responsables o _**ERI**_ de otros procesos, con lo que servirán para que también ellos saquen consecuencias y para tener una visión no mediatizada por las rutinas diarias que a veces impiden detectar comportamientos erróneos porque se asimilan a la normalidad.
- **Realización del simulacro**. En la fecha, hora y localización previstas se realizan las pruebas programadas, comunicando a la mayoría del personal solamente que se trata de un simulacro y cuál es el supuesto que se ejecuta, para que actúen con lo que conocen de los procedimientos hasta ese momento.
- **Alarmas**. Se aprovecha para **probar las alarmas**, informando a la Alta Dirección que se está realizando un simulacro, para que se habitúen a lo que tendrían que hacer en un incidente real. Este es un modo de formar a la Alta Dirección sin que tengan que asistir a seminarios o charlas. Lo mejor es que se realice todo dentro de la jornada normal (e incluso en fin de semana) porque un incidente de verdad no esperará a que todos estén en su sitio y prevenidos.
- **Fin**. Se termina el simulacro y **se recoge información** de los *logs* del sistema, de los testigos, de los participantes, del sistema de alarmas empleado, etc.
- **Informe de lecciones aprendidas**. El responsable de continuidad _**PCN**_ prepara el informe final, dejando constancia de todos los detalles de las pruebas, el grado de cumplimiento de cada supuesto, las observaciones de mejora y la **propuesta de planes de acción** para subsanar las cuestiones no conformes detectadas.
- **Seguimiento de los planes de acción** y proyectos derivados de las lecciones aprendidas del simulacro mediante el sistema que se tenga establecido en la compañía para seguimiento de proyectos.
- **Modificación de los procedimientos**. Cuando se detecte una parte de los procedimientos con carencias o incorrecciones se debe aprovechar para consolidar lo aprendido en el simulacro, modificando los procedimientos afectados.

Ligado a cualquier incidente está la función del **portavoz**. Será lo que vamos a ver en el siguiente punto.

PCN 2.3.4. Esquema de portavoz

Las empresas, organizaciones, entidades de todo tipo tienen sus vías de comunicación habituales, que son típicamente los responsables o Alta Dirección de la propia entidad con la propiedad, la Dirección Comercial con los clientes y la Dirección de Personal con los empleados. Pero en caso de crisis se hace necesario un portavoz de cara a los medios.

En esta última entrega dedicada a los incidentes de ciberataques trataremos sobre la figura del **portavoz**, que destaca rápidamente como la imagen de la empresa frente a los medios y redes sociales. Porque la empresa no tiene cara y ojos, el público la personaliza con la figura del portavoz, que se presenta a entrevistas, da la cara, informa, recoge propuestas y se encarga de darles forma y plazo para lograr una conjunción de intereses dentro de lo que es razonable.



El portavoz se convierte en la imagen de la empresa en un ciberataque o en cualquier otra crisis.

Misión y función del portavoz

Vamos a distinguir tres cosas: el espacio de actuación del portavoz, lo que interesa a los medios y lo que debe decir el portavoz.

- **El espacio del portavoz.** Cada empresa, en los 'tiempos de paz' tiene establecido perfectamente su 'tablero de juego' y asignadas funciones normales que realizan distintas responsables, que cambian radicalmente cuando la empresa entra en una crisis:
    - **Tiempo de paz**. Distintas instancias de la organización tienen misiones de comunicación habitual encomendadas, por ejemplo, la **Alta Dirección** es la que suele tener la comunicación tanto con la propiedad como con los representantes de los trabajadores; la **Dirección Comercial** es la que trata con los clientes; la **Dirección de Compras** con los proveedores; la **Dirección de Personal** con los integrantes de la plantilla a efectos laborales. Puede haber también personal dedicado a comunicación y a marketing, en trabajos técnicos de soporte a la imagen de la empresa.

    - **Tiempos de crisis. Portavoz**. Cuando sucede una crisis es preciso que se pueda distinguir un **portavoz** que concentra y personaliza la imagen de la empresa, porque la gente exige que alguien dé la cara. Esta figura se podrá apoyar en toda la estructura para poder ofrecer la imagen correcta, pero es la que está al frente de todos y tiene que resistir la presión de una entrevista en la que se suelen preguntar los asuntos problemáticos, informar de forma controlada sobre lo que pueda dar explicaciones, recibir críticas casi en primera persona y al mismo tiempo debe ser capaz de transmitir soluciones y comprometerse a que se cumplirán. Para ello **debe ser un directivo, con conocimiento del negocio, capacidad de decisión y amplio respaldo** de la Alta Dirección para asegurarse de que el resto de la organización realizará lo que proponga.
- **Qué interesa a los medios**. A los medios, en general, **no** les interesan los detalles técnicos del asunto. Más bien han de preguntar acerca de cuestiones que afectan a la gente. Por lo que es inútil insistir en dar demasiados detalles de tipo tecnológico o específico de la empresa o entidad afectada si no va a influir en **lo que de verdad le va a suponer noticia** para el público. Además, en los medios se tiende a exagerar lo que va mal, las desgracias son noticia, pero que todo funcione bien no es noticia. Por eso interesa:
    - **La salud y bienestar** de la gente. Será noticia algo que suponga un peligro público para la salud porque produzca enfermedades o molestias, o que haga más difícil disponer de bienes o productos que proporcionen bienestar.
    - **Cuestiones económicas**. Todo lo que vaya a suponer aumento de precios es un punto sensible, que será objeto de especulaciones o de protestas.
    - **Cuestiones emocionales** y que afectan a las relaciones entre personas. Cualquier cosa que dificulte las relaciones entre personas, que haga más difícil hablar, comunicar o reunirse con otras personas, será considerado una amenaza y tendrá el máximo interés.
- **Qué debe decir el portavoz**. Ante todo, **la verdad**. Es inútil intentar dar información equivocada porque al final todo se sabe y regresa para castigar a quien no haya tenido la actitud de informar verazmente. Es más: si se reconocen los errores, se gana la confianza del público porque percibe que se ponen los datos a su disposición. Como la empresa u organización habrá seguido los principios que hemos estado tratando en este texto y tendrá los elementos necesarios y los sistemas adecuados para haber obtenido información, haberla evaluado y haber previsto cumplir el **Objetivo de Tiempo de Recuperación (RTO)**, el portavoz podrá dar su discurso basado en tres puntos clave:
    - **La empresa conoce la repercusión del incidente y lamenta las molestias y daños causados**. Este punto es muy importante porque más allá del coste de la crisis para la empresa, se antepone como prioridad evitar el malestar creado por las molestias y daños para la gente.
    - **Se han iniciado las tareas de recuperación** basadas en los planes previstos para estos casos. Si hubiera que dar **indemnizaciones** a los afectados, conviene incluir el mensaje en este punto, para que lo que le corresponda a los afectados no acabe como demandas, que pueden hacer más daño a ambas partes (a la demandante por las molestias añadidas y a la empresa por los costes económicos y de reputación de una sentencia desfavorable) que los costes de una solución pactada y prevista.

- **La previsión es que podremos haber restablecido el servicio en tal tiempo** fijado en nuestros planes de recuperación. Los problemas de continuidad son asimilables a problemas de **disponibilidad**. El tiempo es fundamental en este punto y da una idea de control, respaldando al portavoz como persona que da soluciones. Pero conviene no equivocarse y prometer que todo se va a arreglar antes de que de verdad se pueda, para no crear falsas expectativas.

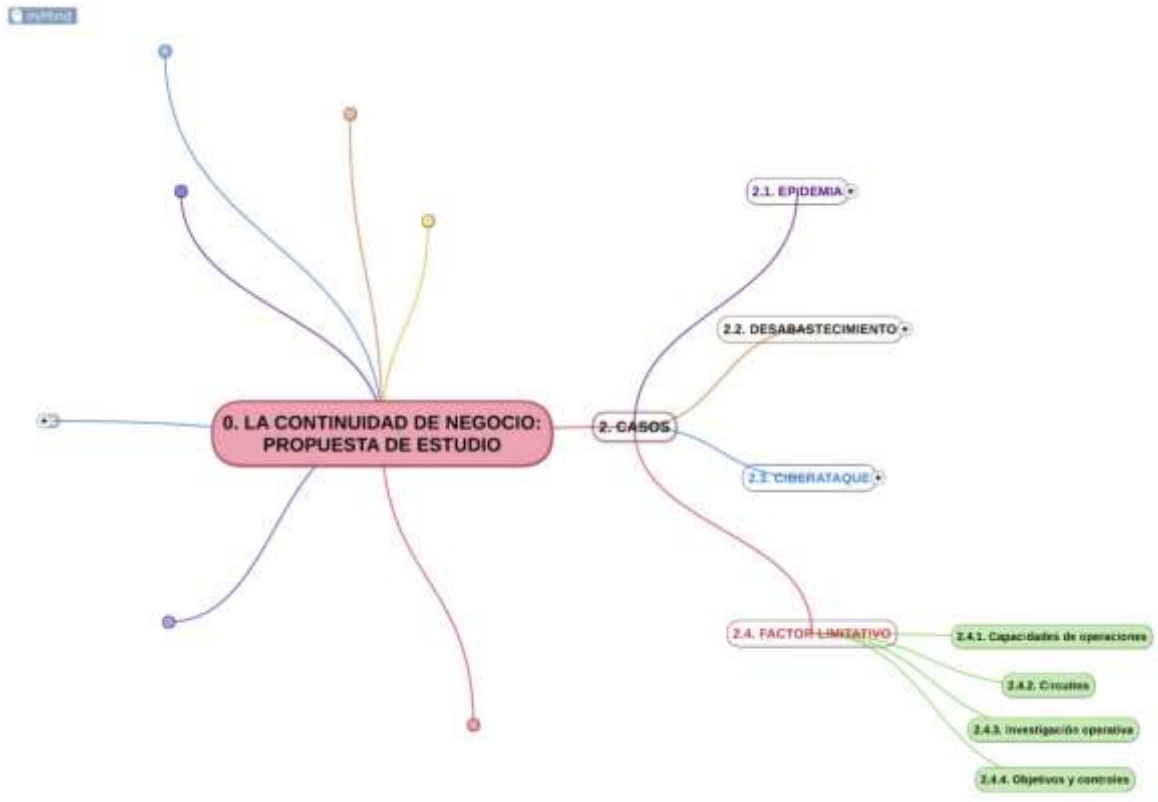
La verdad es que **para cualquier persona *'normal'*, en una primera impresión da pánico asumir el papel de portavoz** si no se tienen las cosas claras o no se conocen bastante los procesos. Pero teniendo en cuenta lo que de verdad interesa, hay mucho adelantado para ponerse delante de una cámara y responder a las preguntas. La naturalidad y buena fe de quien ha de hacer este papel, juegan a favor para ganarse al público.

Ver al final del libro la referencia bibliográfica al libro de **Andy** Osborne que explica este y otros muchos aspectos de la continuidad de forma muy asequible.

PCN 2.4 FACTOR LIMITATIVO

Vamos a terminar la parte dedicada a casos con un tipo de incidente que normalmente no se contempla como incidente de continuidad, pero que es capaz de interrumpir la marcha normal de la empresa y afectar gravemente a sus beneficios. Sería como una muerte a cámara lenta. Está relacionado con los cuellos de botella.

A lo largo de esta parte describiremos el fenómeno y veremos de qué forma podemos contribuir a evitarlo. Al contrario de lo que ocurre con otros incidentes, este, en el que hay **uno o más factores limitativos**, no se percibe como tal, porque no parece que falle nada, no hay una amenaza externa que venga a complicarnos la vida, no hay una queja o molestia porque haya variado (aparentemente) el proceso, pero todo se vuelve más difícil, no se alcanzan las cifras necesarias de facturación y no nos quitamos de en medio las **existencias de productos semielaborados o de servicios a medio preparar**. Lo consideraremos como un caso de continuidad porque produce **los mismos efectos** en el funcionamiento de la empresa que un incidente típico, agravado porque **perdura en el tiempo** y porque no parece haber una causa a la que echarle la culpa. Es más: resulta difícil de abordar por la falta de un diagnóstico válido.



El caso que nos ocupa no es de personas, suministros ni sistemas, sino de diseño de los procesos.

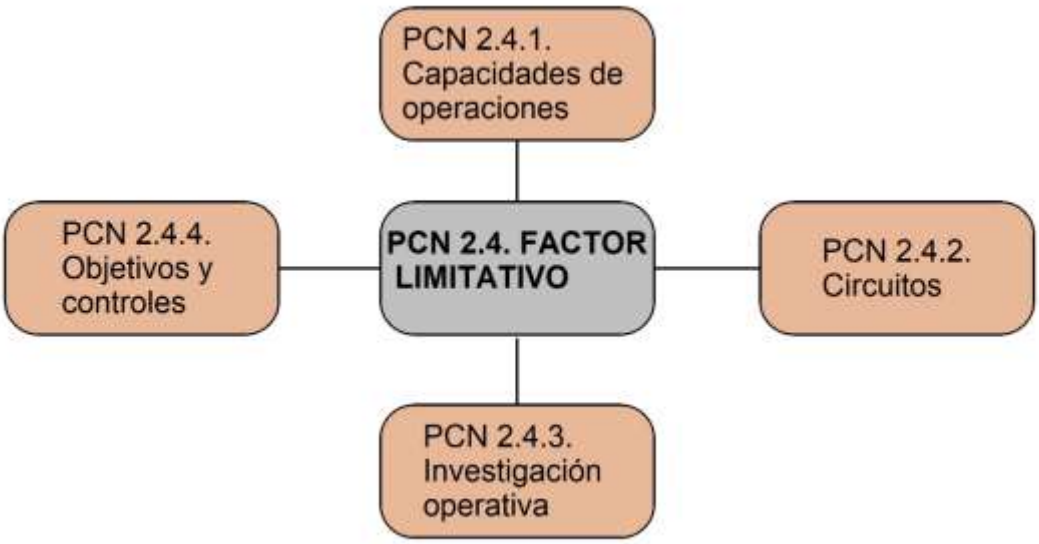
El caos se apodera de nuestro proceso

Los **factores limitativos** son un problema que puede ocurrir aleatoriamente, es decir: imprevisible y caóticamente, y por ello su solución es aún más complicada. El tipo de trabajo es determinante, ya que sucede en procesos con etapas sucesivas. La descripción es que, en determinadas circunstancias, entre unas tareas y otras, se acumulan productos a medio elaborar o se acumulan los expedientes a mitad de

resolver. Es el mismo fenómeno que ocurre en las procesiones de Semana Santa, que transcurren con arranques y paradas sucesivos y aleatorios, que se van transmitiendo a lo largo de todo el recorrido, aunque no siempre haya un obstáculo que impidiera la marcha uniforme. Otro caso más 'laico' es el de los atascos de tráfico. También, apurando un poco más el modelo, es lo que ocurre periódicamente con la marcha de la economía.

Podremos decir sin temor a equivocarnos que siempre que haya un proceso que sigue unos **pasos sucesivos**, salvo que todo esté muy bien calculado y transcurra como está previsto, cualquier perturbación se transmitirá como una onda a lo largo de todo el 'circuito' afectando progresivamente a más etapas, hasta que llegue a paralizar el funcionamiento de todo. Se trata de un **fenómeno caótico** que tiene sus propias reglas. Podemos enumerar algunas, como que:

- El proceso transcurrirá como máximo a la velocidad de la operación más lenta (este principio es elemental y todo el mundo lo asume).
- Si la perturbación se produce porque una etapa posterior va más rápido que una etapa anterior a ella, es decir, hay un *exceso de velocidad*, se puede producir paradójicamente un rendimiento menor del proceso (ninguna operación que adelante a la anterior podrá continuar a ese ritmo y tendrá que parar de vez en cuando; esto si se tiene previsto no es un problema, ya que en este caso disminuye el *stock* intermedio).
- Si la perturbación está en puntos del proceso más cerca del final, se transmite hacia los puntos más lejanos del final, es decir, en sentido contrario a la marcha global (si las operaciones finales no dan salida, se acumulan las paradas al principio).
- Como corolario la perturbación se mueve (hacia atrás) más aprisa que lo que se mueven los elementos del proceso (hacia delante).
- Otro corolario es que para que no se produzca un atasco el factor limitativo debe estar al principio del proceso (las operaciones al final del proceso mejor que estén sobredimensionadas).
- Otro corolario es que un proceso que tiene varias ramas al principio que convergen en una sola fila al final, sufrirán con más facilidad un atasco y este afectará más a los puntos alejados del final del proceso (caso de varias líneas de producción con una sola unidad de empaquetado o finalizado).



Problemas y soluciones de los factores limitativos.

La buena noticia es que se puede someter a estudio y averiguar **en qué punto** el sistema se va a volver caótico e impredecible, cuando alguna de sus variables pasa un determinado **umbral**. Las **capacidades** de las operaciones están en la causa de este tipo de incidentes. Sobre todo si son variables en función de alguna característica del producto que afecte de forma distinta a distintas operaciones del mismo. Los **circuitos** se deben diseñar de forma que no haya factores limitativos hacia el final, a ser posible lo suficientemente flexibles para poderlos adaptar a distintas situaciones y asegurándose que las operaciones son progresivamente de igual o mejor más capacidad que las iniciales. La **Investigación Operativa** es una disciplina de la Ingeniería que puede dar soluciones, matemáticas y por tanto programables, al problema. La **fijación de objetivos y de controles** permiten identificar circunstancias en las que se va a superar el umbral del caos y evitarlo en consecuencia. Todo esto es lo que veremos en los puntos sucesivos.

PCN 2.4.1. Capacidades de las operaciones

En un incidente de factor limitativo, el valor comparativo de la capacidad de las operaciones sucesivas determina la situación del proceso. Esto puede quedar fijado desde el origen si no hay variaciones o variar por según la calidad del producto o por otra causa que afecte a las operaciones con distintas intensidades.

Resulta difícil de visualizar el caso de que se **va a colapsar el proceso** si todo está funcionando aparentemente con normalidad. Pero es lo mismo que cuando vamos por la autopista y nos encontramos con una retención que acaba en atasco, nos impide el movimiento normal, salimos poco a poco, en una especie de baile de parar y arrancar y cuando llegamos al punto álgido no hay nada anormal ni nada que impida la marcha de los vehículos. Todo lo que sucede se debe a **diferencias de velocidad** entre los coches que están circulando. Pues en los procesos de producción pasa lo mismo.

Las diferentes capacidades entran en conflicto en un proceso con operaciones sucesivas.

¿Qué hace que cambien las capacidades?

Cuando se diseña un proceso se procura **equilibrar todas las operaciones**, para que todo funcione al unísono. Tampoco cuando se inicia una procesión hay voluntad de hacer parar a los procesionarios aleatoriamente en el momento menos pensado. El problema se plantea porque en general es imposible asegurar que todo funcionará al mismo ritmo y que el proceso será siempre fluido si partimos del supuesto de que **las operaciones son independientes** y cada una ocurre en máquinas distintas o, si el proceso es manual, las realizan distintas personas en secuencia, **cada una con su distinta capacidad** de producción.

Para evitar esto se hacen varias cosas: la más elemental es **montar el mayor número de operaciones en la misma máquina**, que al funcionar de forma solidaria hace que las operaciones acaben al ritmo que empiezan. Otra decisión normal es que la máquina más valiosa, por su precio o por su más costoso mantenimiento, que llamaremos ***máquina principal***, sea **la que limite la producción**, porque así, con un menor coste, puede hacerse que todas las demás tengan más capacidad que la principal y no limiten la producción del sistema completo. Estas operaciones no principales, si fuera preciso, se pueden realizar en más turnos para que no limiten la

producción de la principal. También podría darse el caso contrario, en que la limitación fuera muy notable y estuviera localizada en la parte principal, que entonces se haría trabajar a más turnos, con lo que se conseguiría amortizarla más pronto, que podría ser en algún caso el criterio que prevaleciera.

Pensemos ahora un proceso no del todo industrial, sino más bien manual o de servicios, en términos de capacidad. No todas las personas tienen la misma capacidad de trabajo. **Las más eficientes han de situarse en las etapas finales** para que las menos capaces no limiten la velocidad a la que se procesan los productos manufacturados o los servicios. También en este caso se puede jugar con los cambios en los turnos de los distintos equipos para adaptar las producciones relativas.

La conclusión hasta ahora es que **la capacidad nominal** de una instalación de etapas sucesivas **se puede adaptar** mediante cambios temporales en el diseño del propio proceso, modificando las máquinas o instalaciones y modificando los turnos de trabajo. Nos vendrá bien recordar esta conclusión porque también podremos emplearla cuando la variación de las capacidades relativas se produce por causas intrínsecas al propio producto.

El ejemplo más importante de variación de las capacidades relativas en un proceso por etapas sucesivas por causa intrínseca del propio producto es el de **cambios en la calidad del producto** que hacen que en algunos pasos del proceso se modifiquen las relaciones entre velocidades de producción de las etapas sucesivas. Estas variaciones de calidad pueden darse por motivo de **requerir una selección** de las unidades producidas en un paso de una a otra etapa de producción, con reducción de la capacidad y eventualmente **reproceso** de los productos que puede producir temporalmente exceso de flujo de entrada en la etapa en que se reintegran los productos reprocesados.

De nuevo, comparando los conceptos de procesos industriales a una producción manufacturera o de servicios, un cambio en la **calidad de los servicios prestados** por distintos equipos debería poderse compensar con cambios en la disposición del personal o de sus turnos en los distintos equipos.

Naturalmente, si los cambios del personal suponen cambios de turno de trabajo o de jornada, esto debe **tratarse primero con los representantes de los trabajadores** para **llegar a acuerdos** operativos y probablemente supondrán **incrementos de coste**s para indemnizar los cambios pactados. Tanto si se puede como si no se puede llegar a acuerdos, el resultado de un incidente de factor limitativo será una menor producción o un mayor coste de producto o de servicio. Al igual que cualquier interrupción por un tiempo superior al Máximo Periodo Permisible de Disrupción (MTPD), va a resultar en un coste económico, añadido al de las multas, indemnizaciones, penalizaciones, etc. ocasionadas por la propia interrupción.

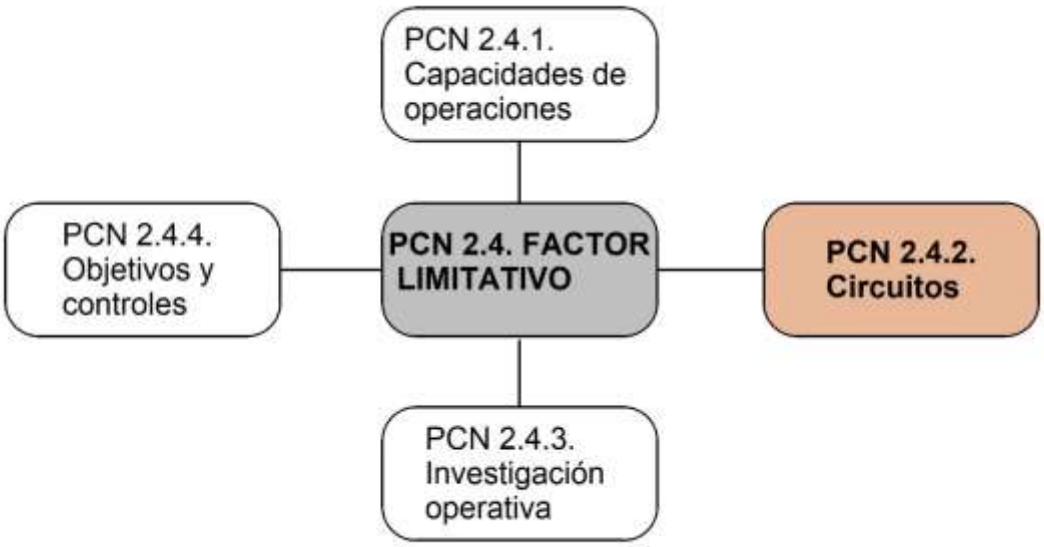
Si tuviéramos **un algoritmo** que permitiera minimizar los tiempos muertos y nos calculara qué modificación de los turnos del personal o de las instalaciones fuera la más favorable en función del parámetro 'calidad' o 'proporción de producto reprocesado' en distintas fases del proceso, tendríamos el dato que necesitamos para **aplicar temporalmente los cambios** en la composición de los equipos de trabajo o en el funcionamiento de las distintas fases, para conseguir que el conjunto maximizara los resultados. Pero la mejora efectiva y el ahorro se producirá si logramos evitar la oportunidad de que el proceso funcione en la medida de lo posible, por etapas

sucesivas. Pero no es el único factor: están también los '**circuitos**' que veremos en el siguiente punto.

PCN 2.4.2. Circuitos

En el punto anterior vimos cómo un factor intrínseco, la calidad, podría ser causante de diferencias de funcionamiento entre partes del proceso de etapas sucesivas, provocando descompensaciones en las velocidades de las partes y con ello atascos de productos o servicios a medio terminar. Ahora veremos que el circuito que sigan las etapas es también determinante.

Una forma de conseguir evitar situaciones de atasco producidas por distintas velocidades de procesamiento de los productos o de la información es **diseñar circuitos de trabajo** más efectivos contra situaciones de atasco. Los circuitos pueden ser como el aparato digestivo de la mayoría de los animales: un tubo en el que tras una etapa sigue otra. Esta sería la forma 'canónica' si se trata de aplicar distintas etapas a los productos y tenemos maquinaria de gran tamaño que hay que manejar de forma especial, distinta del resto del proceso. Pero hay otras opciones que allá donde se pueden aplicar son muy efectivas.



Manejar los circuitos evita bucles y atascos si tenemos la suerte de poderlos modificar.

¿Cómo hacer que el circuito no sea determinante?

El sentido común nos llevaría a reproducir el **aparato digestivo** como paradigma de circuito ideal de producción. ¡Y generalmente funciona!

- Se pueden **juntar cuantas operaciones se puedan hacer a máquina** en una misma pasada para evitar la mayor parte posible de pasos entre etapas sucesivas.
- Se pueden estudiar el plano de las instalaciones **evitando retrocesos** en los casos en que no sea estrictamente necesario.
- Se puede **jugar con la programación** para que las fabricaciones sean más largas o más uniformes, mejorando de paso la calidad y la productividad (sólo que entonces, en general, hay que adelantar más capital circulante para soportar producciones mayores).
- Incluso se puede **modificar el producto** para que necesite menos vueltas atrás y menos manipulaciones.

Pero la modificación maestra del circuito es **cambiar el modelo** del aparato digestivo por el modelo ¡del **aparato respiratorio**! Ello conlleva cambios organizativos y de formación notables. Veamos cómo se puede llevar a la práctica.

En la respiración el aire limpio con alto contenido de oxígeno entra por el mismo conducto que luego sale el aire usado con alto contenido de CO2. Ello significa que **las operaciones que hay que hacer se hacen en lotes** (inspiración-espiración y vuelta a empezar), no en continuo como la digestión. De acuerdo que la química involucrada en la digestión es más compleja y además participa en ella el microbiota y estas dos condiciones no suceden en la respiración. Pero esto es solo una idea primera.

¿Cómo lo hacen en algunas empresas? La respuesta es cambiando las habilidades de sus empleados. El ejemplo que viene al caso es el de las **tiendas** de una conocida cadena de alimentación en las que el **personal** va desempeñando **distintas funciones** de forma que **es capaz de realizarlas todas**, en lugar de especializarse en alguna de ellas. Esto tiene la ventaja de que, sin modificar el circuito, no hay empleados permanentemente en las funciones de almacén, o reponedores, o limpieza, o en la verdulería, o en la droguería o en las cajas, sino que la plantilla se adapta instantáneamente a la disposición más efectiva, y se evitan los cuellos de botella de las distintas funciones y de personal clave para desempeñar determinados trabajos, instantáneamente en cada momento. Todos hacen todo.

Podría parecer que este ejemplo no serviría para la **producción industrial**, donde dominan las cadenas de producción. En alguna empresa automovilística, en lugar de la cadena de montaje, hace ya unos cuantos años trabajaban con **equipos autónomos autosuficientes**: grupos de operarios capaces de montar un coche entero a partir de las piezas, de forma que cada equipo era una minifábrica completamente capaz, quitando las funciones logísticas y administrativas. Con ello se modificaba drásticamente el circuito y se conseguía tener tanta capacidad como equipos se pudieran formar, sin que ninguna especialidad o punto de la cadena fuera determinante de la producción.

También se están popularizando estos métodos de organización para el desarrollo de *software*, como los grupos de **Desarrollo Ágil**. O de **Equipos Autosuficientes Agile**. Hay bastantes referencias en internet. El concepto es el mismo: **superar el circuito en cadena** de etapas sucesivas.

En ambos casos, hacer esto requiere un **plan de formación efectivo** y acostumbrarse a **trabajar en equipo**. Pero elimina del todo ciertos cuellos de botella y fomenta un trabajo más soportable y menos aburrido que hacer siempre la misma operación durante años.

Naturalmente, no todos los procesos pueden adaptarse a voluntad tan fácilmente como daría a entender lo que decimos en éste y en el anterior punto. No hay que hacerse falsas ilusiones. Pero si una cosa no funciona, siempre tenemos otra y **puede que la solución sea mixta**: una mezcla de varias iniciativas. Si todo ello falla, **aún nos quedan las matemáticas** de la **investigación operativa**, que nos puede mejorar un poco más la situación. El caso es que con esas tres iniciativas que formuladas en resumen serían:

- **Equilibrar las etapas**,
- **Cambiar los recorridos** de los productos o servicios durante la producción y

- **Calcular la mejor solución** con los datos disponibles, adaptándola a las necesidades reales, tendremos **recursos suficientes para evitar el colapso** por factor limitativo.

PCN 2.4.3. Investigación operativa

Este es un capítulo interesante para quien pretenda hacer experimentos 'con gaseosa', esto es: sin riesgo. Usar el ordenador para someter a pruebas un modelo de producción que hemos diseñado es siempre gratificante y cuesta sólo el tiempo que se ha empleado en ello, ya que está al alcance de cualquiera con un ordenador corriente.

Hace años era más difícil investigar las consecuencias de cambios aplicados en los procesos de producción por la carencia de herramientas adecuadas. Las matemáticas que podían servir de ayuda requieren hacer cálculos repetitivos que se hacen tediosos y los gráficos para representar procesos costaban más de realizar dado que se tenían que hacer casi en exclusiva manualmente. La situación ha cambiado en los últimos años con el desarrollo fulgurante de los ordenadores personales y del software disponible. La **investigación operativa**, que emplea un conjunto de técnicas que se pueden realizar mediante ordenador, se ha visto beneficiada por este desarrollo.

La investigación operativa dentro del conjunto de ayudas para superar factores limitativos.

Como complemento a los principios de organización industrial que hemos mencionado en los puntos anteriores, está la posibilidad de hacer experimentos creando y poniendo en juego modelos de procesos y viendo cómo evoluciona su estado modificando ciertas condiciones del entorno, como por ejemplo modificaciones de los procesos en sí, de la dedicación de los equipos de trabajo o de los circuitos que definen la producción. Hay mucha bibliografía en internet, aparte de libros especializados. Como ejemplo pongo el **enlace a este artículo**: "¿Qué es la investigación operativa?".

La investigación operativa de procesos de etapas sucesivas con hojas de cálculo.

Un medio ideal para realizar experimentos fácilmente es hacerlo con **hojas de cálculo**. Las ventajas que tiene son evidentes: la hoja de cálculo no solo puede hacer unas determinaciones, sino hacerlo de forma recursiva. Se puede emplear el método de programar macros, o el más sencillo de emplear una fila para cada instancia, de forma que cada fila tome como punto de partida el resultado de la fila anterior. De esa forma,

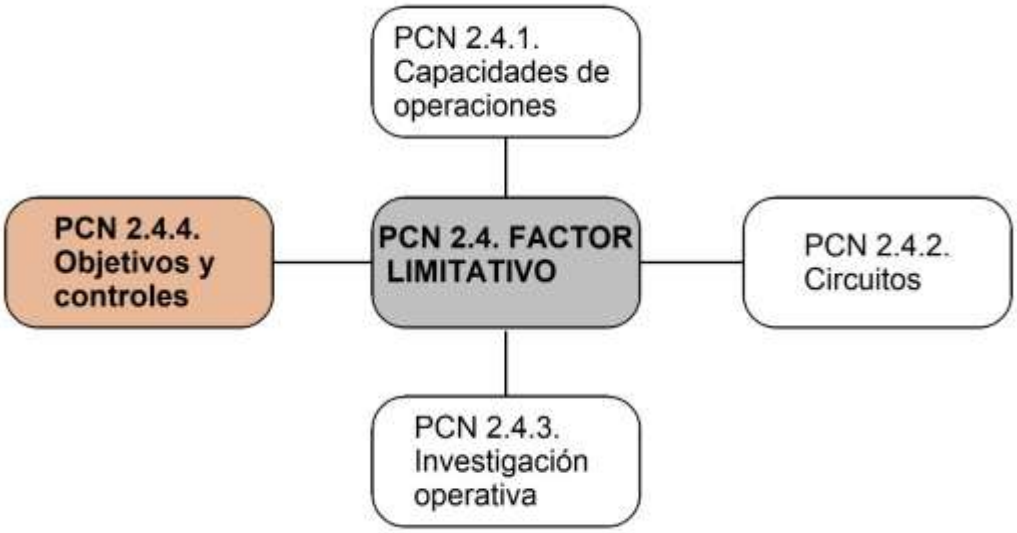
con un número suficiente de filas, que se programan simplemente copiando la fila anterior, se pueden realizar un buen número de etapas sucesivas de forma recursiva, obteniendo en el proceso los datos de cada ciclo, que pueden luego analizarse gráficamente o emplearse para otras determinaciones.

Para no extender demasiado el tema, me remito a la publicación en la página "**unoydostres.com**" sobre **Bases experimentales para una teoría del atasco**. En particular se puede profundizar un poco más en dos de los artículos que componen el trabajo: **Modelización del atasco**, y a este otro **Fórmulas y programas para el estudio del atasco**, que pueden orientar o servir de ejemplo de lo que se puede hacer con una simple hoja de cálculo y un modelo sencillo de la producción (o de la circulación de vehículos si se desea).

PCN 2.4.4. Objetivos y controles

Para terminar con los casos de estudio que hemos abordado en la segunda mitad del texto hasta ahora, vamos a tratar la cuestión de la planificación de objetivos y los controles. Ninguna tarea empresarial puede resistir largo plazo y tener éxito (que requiere definir lo que se pretende lograr) si no se hace el esfuerzo de plantear objetivos y verificar periódicamente su grado de cumplimiento.

Lo primero es tener una **lista de tareas** a realizar a lo largo del año, algo que nos diga si estamos en disposición de ir cumpliendo todas las tareas (que son muchas) que componen la gestión de continuidad. Por ejemplo, durante el primer trimestre actualizar los datos variables de los procesos, como son los Análisis de Impacto y actualizar los procedimientos, en el segundo semestre realizar simulacros, en el tercero pasar las auditorías y en el cuarto preparar la documentación de la revisión por la Dirección y los planes de acción y objetivos para el año siguiente.



Los objetivos y controles desde distintas facetas, para ver si estamos en el camino correcto.

Naturalmente hay grupos en la organización que tienen más facilidad para adelantar en trabajos que a otros les cuestan más. Entonces los controles de seguimiento se han de hacer para los distintos grupos de la organización a menos que ésta sea muy pequeña y no se necesite tanto detalle. Lo que se haya programado como proyectos, como por ejemplo pueden ser los planes de acción derivados de las auditorías o de los simulacros, se pueden seguir con una herramienta informática de **seguimiento de *tickets*** o de **seguimiento de incidentes** o bien construirse una (pequeña) base de datos propia con tal fin. Si son suficientemente complejos deberían además seguirse con las herramientas típicas de gestión de proyectos, incluido un **Diagrama de Gantt**.

Sugerencia de panel de control

Es muy práctico unir en un sólo documento tipo hoja de cálculo todo lo necesario para llevar al día los asuntos planificados. Por ejemplo, el libro de la hoja de cálculo puede tener diversas páginas y contener información como la siguiente:

- Estado de las acciones derivadas de la última revisión por la Dirección.
- Resultados de las auditorías.

- Evaluación del sistema de PCN respecto de lo recomendado por la norma.
- Listado de cambios relevantes en el sistema realizados y otros, convenientes, pero no realizados.
- Control de tareas por periodo anual detallado por procesos, incluidos los Análisis de Impacto.
- Lista de planes de acción con indicación de responsables, fechas, acciones previstas y estado de cumplimentación.
- Seguimiento de objetivos tácticos (anuales) y proyectos.

Asignando valores a la evolución y al grado de cumplimentación en el tiempo, se puede tener la sensación de que se tiene un mínimo control de la situación.

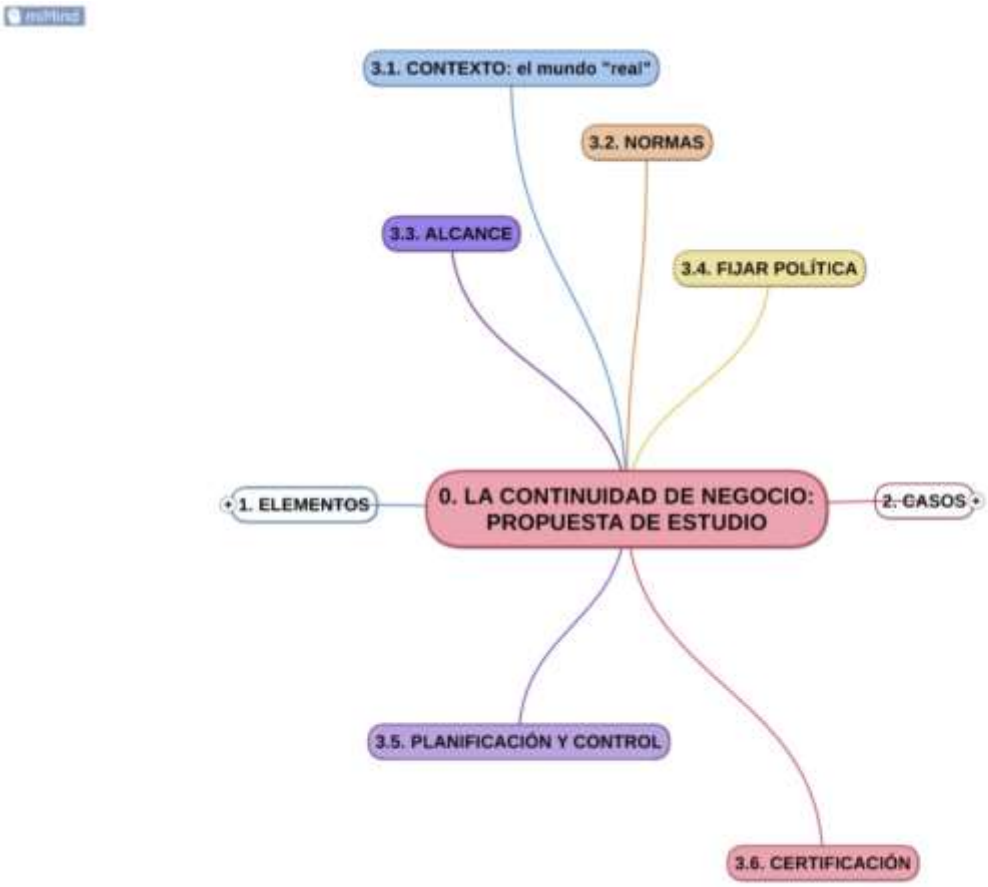
Este panel de control será muy útil en el momento de preparar el documento de revisión por la dirección ya que parte de la información que solicita la norma se tendrá al día en este panel y será inmediato copiar la parte correspondiente. Cada empresa debe preparar su propio panel de control para que tenga algún significado y se puede hacer un seguimiento.

Una vez tratados los cuatro casos que hemos desarrollado para estudio, empezaremos ahora un ciclo de las cuestiones administrativas o formales que completarán nuestro sistema de continuidad de negocio y nos facultarán para lograr el objetivo de la **certificación del sistema**.

PCN 3.0. COMPLEMENTOS FORMALES

Hemos estado tratando elementos de conocimiento que teníamos que conseguir para desarrollar un sistema de planes de continuidad y cuatro casos de incidentes tipo, y hemos dejado para el final dar un repaso a los aspectos formales y administrativos que nos harán falta como infraestructura para concretarlo todo y estar preparados para una certificación, que vamos a ver a continuación.

Esta parte es una ***superestructura*** de lo que hemos visto hasta ahora, Si estuviéramos tratando de *una cebolla*, muy cerca del centro estarían los '**elementos'**, después basándose en los elementos estarían los '**casos'** y en la capa más externa estarían estos **'complementos'** que nos van a ocupar las próximas sesiones. En algunos textos se presentan al principio, pero como hemos empezado sin tener conocimientos del asunto, es más apropiado que la parte que depende de otras más primarias se presente al final.



Los complementos del Sistema de Planes de Continuidad en su contexto.

Cuando se ha de presentar el sistema que hemos creado para mejorar nuestra capacidad de mantener la **disponibilidad** de la empresa, o lo que es lo mismo, cuando se presentan los planes de continuidad es como si mostráramos nuestra casa. Se suele empezar por 'el recibidor'. Este elemento que vemos primero suele dar una idea de cómo será luego la 'casa', o sea: el conjunto. Pues vamos a tratar de despejar las dudas y dar una imagen apropiada, para que los demás elementos se juzguen con ecuanimidad.

La visión ampliada y centrada en estos complementos la representamos como un objeto con 6 brazos. Ninguno de ellos aumentará mucho lo que ya hemos hecho intuitivamente para mejorar nuestra capacidad de defensa y de reacción, pero no tenerlos definidos nos incapacitaría para poder defender nuestra posición y trabajos en pos del objetivo de tener un sistema sólido y respetado:

La *envoltura* de los planes tiene este aspecto.

¿Qué nos faltaba por desarrollar?

Una **descripción somera** de estos complementos es la siguiente:

- **Contexto**: En este elemento se trata de mostrar cuál es el entorno en el que se desenvuelve la actividad de la organización, entidad o empresa. No sólo geográficamente, sino en qué ambiente social, a qué personas da servicio, cuáles son sus estatutos fundacionales y a qué leyes obedece, quiénes son los socios, los proveedores, los clientes y en resumen para qué existe la organización.
- **Normas**: Estas normas en sentido amplio serían todas las que debe cumplir la empresa, pero en sentido estricto y desde el punto de vista de la continuidad, la norma de referencia es la **UNE-EN ISO 22301 Sistema de Gestión de la Continuidad de Negocio**.
- **Alcance**: Este elemento sirve para definir qué es lo que pretende el sistema en términos de qué parte de la empresa va a regular y qué no va a tratar. Fija las fronteras de la competencia en continuidad. Muy importante para quien necesite sentir que está pisando tierra firme. Evita discusiones inútiles sobre si una función la debe desarrollar el equipo de continuidad o deben hacerlo otros.
- **Política**: La política es una declaración de intenciones de la Alta Dirección respecto a lo que va a hacer con el sistema. Va junto con los objetivos estratégicos pertinentes, ya que debe estar orientada a la acción y a la mejora continua, y si no hay objetivos, no se mejora.

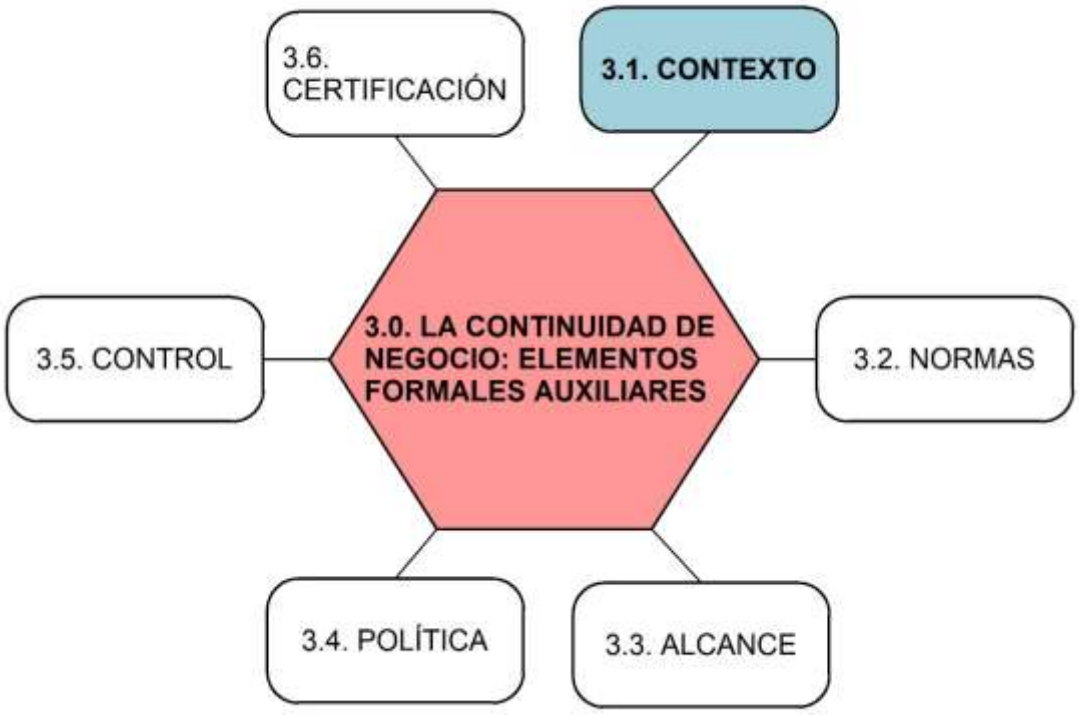
- **Control**: Este capítulo va dedicado al **responsable de continuidad _PCN_**, ya que vamos a ver y hacer una relación sobre de qué cosas tiene que tener todos los datos e información para estar seguro de que domina el sistema. No sólo lo que mostrará a la Alta Dirección cuando presente el **informe de revisión**, sino lo que hace que sepa **asignar prioridades** a los asuntos.
- **Certificación**: Este es el colofón de todo lo que hemos estado preparando. Tiene que haber una entidad independiente que le cuente a la Alta Dirección, propiedad, clientes y proveedores, además de a todos los directivos, mandos y personal de la compañía, que el sistema está probado y encontrado conforme a la norma de referencia. Se trata de un plus de autoestima y de prestigio para poder exigir a los demás que hagan lo que se necesita para mantener este estatus.

Veremos todos estos puntos en las próximas 6 entradas.

PCN 3.1. CONTEXTO

Entendemos contexto en un sentido amplio como el entorno en el que se desenvuelve la actividad de la organización. Nos interesan las condiciones de su fundación y desarrollo, que vendrán marcadas por la geopolítica, es decir: por la sociedad en la que está radicada y su situación mundial, por tanto, cuáles son sus leyes y quiénes son sus partes interesadas y el papel que representa en este entorno su actividad.

Dentro de las varias maneras que hay de considerar el **contexto**, tenemos que pensar en el mundo empresarial, en que no es lo mismo fundar la empresa en un país en el que haya **seguridad jurídica** e imperen las leyes del mercado que en un lugar donde todo esté a expensas de decisiones políticas arbitrarias. De la misma forma que el ciudadano nacional de un país, por el hecho de haber nacido en él tiene condicionada toda su vida personal y laboral, y sería distinta si hubiera nacido al otro lado de la frontera, hay que considerar el lugar donde está implantada la empresa como lo es la tierra para un árbol plantado en ella.



El contexto como circunstancia auxiliar.

Uno de los documentos que constituirán el manual, por lo tanto, el procedimiento de mayor nivel en la '*pirámide de procedimientos*' del sistema de gestión de la continuidad es la definición de su entorno.

¿Qué entra en el concepto de entorno?

Lo que siempre funciona es empezar por el principio. Veamos cuál es el país, su región, el sector económico o social en el que se integra la empresa y sigamos adelante:

- **País '*de nacimiento*'** y condiciones sociales políticas y de comercio:

    - **Lugar donde se constituye la sociedad**. Por ejemplo sólo con decir "**España**", estamos refiriéndonos a: "Un país del suroeste de Europa; miembro de la Unión Europea, del Eurogrupo, de la ONU y de la OTAN; monarquía parlamentaria con alto grado de descentralización y autonomía regional; de 48 millones de habitantes con aproximadamente un 90% de población autóctona; con un nivel económico, definido por la renta *per cápita*, medio; cuyo idioma oficial es el español, junto con lenguas cooficiales en varias comunidades autónomas; líder en producción agrícola, turismo e industria; con un enorme patrimonio cultural y artístico; etc.". En este caso **la comunidad autónoma** en la que se radica la sociedad tiene también sus particularidades, porque condiciona muchas de las relaciones.
- **Aspectos legales y normativos**:
    - **Estatutos fundacionales**: la razón por la que se ha registrado como entidad distinguible de su entorno. De esta forma queda claro a qué se va a dedicar en su funcionamiento. Los estatutos los registra la propiedad e indica cómo será su relación con el mundo, con lo que con ellos conocemos algo más de la empresa: la procedencia de su capital y las relaciones con el resto de las entidades.
    - **Leyes y normativas aplicables**: Además de las propias de su país de localización que afectan a todo el mundo, cuáles son específicas de su sector y de los territorios y municipios en los que desarrolla su actividad.
    - **Norma** del sector en que se va a basar el sistema de gestión en cuestión. En el caso de continuidad de negocio será la **UNE-EN ISO 22301 Sistema de Gestión de la Continuidad de Negocio**.
- **Partes interesadas**, con especial énfasis en sus **necesidades y expectativas**, las marcadas por las leyes aplicables y por la **relación comercial**:
    - **Empleados y colaboradores** de la entidad: cuáles son las condiciones por las que se rigen, cuáles son los beneficios que obtienen de su relación con la entidad.
    - **Clientes**: son el grupo destinatario de la actividad de la empresa o entidad. Si algún grupo tiene un carácter de destinatario preferente de dicha actividad, debe figurar expresamente en este apartado, incluyendo en la descripción qué tipos de necesidad cubre la entidad y qué esperan de la misma sus clientes.
    - **Proveedores**, si son significativos para la marcha de la entidad, también deben reflejarse en este apartado, por ejemplo, las condiciones sociales de los países de los que provienen los suministros.
    - **Intereses sociales**: la **Responsabilidad Social Corporativa** es un factor de afianzamiento de la empresa en su entorno y debe dedicarse un esfuerzo a potenciarla, contando cuáles son las iniciativas de acciones sociales y su repercusión.

Definiendo el entorno, se consigue tener una idea bastante exacta de la situación de partida de la empresa y se aclaran las ideas de su contribución social.

PCN 3.2. NORMAS

La normalización es un concepto general que sirve básicamente para que nos entendamos con relación a un determinado aspecto de la comunicación, de la producción y de la actividad en general. En el caso de los sectores industriales las normas han permitido que la producción de distintos orígenes sea intercambiable y que los niveles de exigencia de determinadas condiciones sean comparables.

Decimos **normalización** y estandarización de forma equivalente. Por ejemplo, de normalización podemos mencionar la denominación de los tamaños de papel para uso en oficinas. Cuando decimos "*tamaño A4*", sabemos que el papel encajará perfectamente en la máquina de fotocopiar y de imprimir sin más atascos de los necesarios y luego lo podremos archivar o doblar y meter en un sobre, también normalizado, sin tener que hacer ninguna otra modificación posterior. Antes de que se generalizara esta denominación teníamos el nombre 'folio' que se usaba para lo mismo pero que era ligeramente distinto (mayor que el A4) y ahora no encajaría en las impresoras. 'Folio' es un concepto sociológico, mientras que 'A4' es un concepto técnico.

Las normas como otro complemento más.

¿Qué dicen las normas?

Resulta interesante ver cuál es el contenido de las normas ISO como es la de referencia para la continuidad, la **UNE-EN ISO 22301 Sistema de Gestión de la Continuidad del Negocio**.

Primero viene una introducción que explica las razones de esta norma. Lo más interesante de esta parte es que cuenta el famoso **ciclo de Deming para la mejora**

continua, que lo llama "Modelo planificar-hacer-verificar-actuar (PDCA)". Lo cual es toda una declaración de intenciones. Los apartados que nos encontramos luego son los siguientes (no los menciono literalmente):

1. **Objeto y campo de aplicación**. Habla de que la norma fija los requisitos para implantar un sistema de gestión de la continuidad.
2. **Normas para consulta**. Aquí sólo se menciona una norma, la ISO 22300, seguridad y resiliencia. Vocabulario.
3. **Definiciones**. Este capítulo es muy interesante para que *todos hablemos la misma lengua*. Muchos de los términos empleados en estos textos que vamos publicando reciben una definición escueta y comprensible. Disrupción, análisis de impacto, incidente, riesgo y otros muchos más términos tienen cabida aquí.
4. **Contexto** y alcance explicados en detalle en esta parte, en concreto el asunto de las necesidades y expectativas de las partes interesadas.
5. **Liderazgo**. Me encanta este punto porque liga el liderazgo al compromiso. Brillante. También viene explicada la política y la definición de roles. El mundo real debería aprender de estos conceptos y todo sería más fácil.
6. **Planificación**. La forma de abordar riesgos y oportunidades mediante la planificación, los cambios en el sistema de continuidad.
7. **Apoyo**. Como si hubiese sido escrito por un club de ajedrecistas, que saben que sin apoyo no se puede abordar ninguna acción de envergadura en el tablero. Recursos, competencia, concienciación, comunicación e información documentada son los apartados de esta parte.
8. **Operación**. En la puesta en práctica general de *todo*, que es este capítulo de la norma, vienen los apartados de Planificación, Análisis de Impacto, Evaluación de riesgo, Fijación de Estrategias y soluciones, Planes y procedimientos, Programa de entrenamiento, Valoración de la documentación
9. **Evaluación del desempeño**. Aquí tenemos la cuestión de la medición y análisis, la auditoría interna, la revisión por la dirección,
10. **Mejora**. Viene detallada la gestión de no-conformidades y la mejora continua.

No oculto el **entusiasmo** que me transmite la norma, lo cual tiene bastante mérito para un documento que generalmente resultaría de aburrida lectura y demasiado centrado en las expresiones del sector. Tiene algo de todo ello, pero resulta ser el mejor apoyo para quien pretenda embarcarse en una ventura como esta de montar un sistema de gestión completo, partiendo de la nada. Por tanto, mi recomendación es comprar un ejemplar de la norma a AENOR y aprenderla *como si fuera* ***el Catecismo***. Es lo único que nos libra de todo mal cuando no estamos seguros de si lo estamos haciendo bien.

PCN 3.3. ALCANCE

El alcance define qué será la competencia de continuidad y qué quedará fuera. Esto que parece sencillo se complica por la propia dinámica interna de las organizaciones en las que cada uno tiende a defender lo que considera que son los intereses de su competencia.

La cuestión de fijar el **alcance** está bien plantearla porque hay **dos tendencias nefastas** en las organizaciones relativas al mismo. La que pretende que los responsables de un sistema *sean los responsables* de los resultados de los procesos, por ejemplo, cuando se le pretende 'cargar' al responsable de calidad la culpa de que la calidad del producto fabricado no sea la correcta. La tendencia opuesta es la de que el responsable de calidad *no tiene nada que decir* sobre un proceso que forma parte de la actividad de la empresa.

La solución al conflicto es doble: **el responsable de un proceso es el responsable** no sólo de la producción, sino de la calidad, aunque haya un departamento de calidad que busque la forma de que se cumplan las normas y se realicen los productos según las especificaciones; y el responsable de calidad, *por supuesto* que **debe intervenir con autoridad suficiente** para que el responsable del proceso *acate* la normativa de calidad vigente.

Alcance fija las fronteras de la acción del sistema de gestión. No confundir con contexto.

Cuestiones de fronteras

Las fronteras del **alcance** han de fijarse claramente por escrito y refrendadas por la Alta Dirección. La mejor forma y más natural es que queden claras **en el manual** de PCN que la Dirección ha de aprobar cada año. El alcance del sistema puede empezar

siendo el de un solo proceso, que sirva de piloto al principio del proyecto para implantar un sistema de gestión de continuidad, pero su vocación ha de ser la de expandirse a toda la entidad. Todo empieza siendo pequeño alguna vez. Se trata de que los errores que se cometan en el momento del establecimiento del sistema sean limitados por el alcance inicial y se corrijan en cada ampliación, hasta alcanzar el límite natural de todo sistema de gestión, que es toda la entidad.

Para que el alcance no sea toda la entidad sólo hay dos excusas:

- **Estamos iniciando el proyecto** y el alcance es el primer proceso incluido. Se necesita un tiempo para madurar y pretender ampliar el alcance más allá. Generalmente hacen falta un par de años para dar ese salto, que es cuando los proyectos empiezan a madurar. Aun así, el sistema deberá aplicarse no solo a un proceso de producción sino también a todo lo que gira en torno al mismo, como por ejemplo la gestión de personal, las compras, las ventas, y todos los departamentos que gestionan procesos comunes a toda la organización.
- **Los procesos son tan distintos** en importancia, extensión o estado de desarrollo de sus infraestructuras que es prudente no mezclarlos en un mismo sistema de gestión.

En todo caso es necesario indicar claramente en los documentos pertinentes, cuál es el alcance reivindicado en cada momento, para evitar confusiones o discusiones estériles.

En la siguiente entrada hablaremos de **política**.

PCN 3.4. POLÍTICA

La *política* es una declaración de la dirección acerca de cuáles son las líneas de actuación que se quieren llevar a cabo. No será muy distinta de lo que asigna la norma UNE-EN ISO 22301 a los planes de continuidad: "Implementar, mantener y mejorar un sistema de gestión para proteger y reducir la probabilidad de ocurrencia, prepararse, responder y recuperarse de disrupciones cuando éstas surjan".

Esta declaración formal tiene la misión de que sean asumidos por la Alta Dirección una serie de actuaciones, que a veces comportarán gastos y al principio pueden suponer un mayor coste en recursos que se tendrán que dedicar a una nueva tarea. Como todo lo que es nuevo en una organización, al principio genera resistencias, aunque luego acaba integrándose en la rutina y finalmente se puede comprobar que resulta beneficioso económicamente al reducir el riesgo y aumentar la confianza de los clientes en la empresa.

Una vez definido el contexto y el alcance estamos en disposición de definir la política.

¿Se puede definir la Política en abstracto?

Todo se puede. Sólo que no hay una declaración de cualquier precepto de la norma que sea válido sin importar su destinatario. Si fuera posible así no se editarían normas, sino directamente manuales. Asumir que la política de mi entidad es la misma que la de otra empresa es equivalente a no creer en ninguna. **La política ha de ser específica de la entidad a la que representa**. Por eso es mejor plantearla después de tener claros tanto el **contexto**, que marca la situación de la entidad en el mundo real, como el **alcance**, que indica en cierta forma cuán interesados estamos en este momento en hasta dónde llegar con el sistema, cuán ambicioso es.

La política no se ha de emitir 'sola' sino acompañada de los **objetivos estratégicos** de la continuidad. Los objetivos de las empresas son al menos de tres clases:

- **Objetivos estratégicos** o permanentes: se trata de proyecciones de futuro atemporales que se desea que se cumplan como resultado global de la acción.
- **Objetivos tácticos** o anuales: son los que se plantean tras una apreciación de riesgos (ver la entrada **PCN 1.3.4. Apetencia de riesgo**), la revisión por la dirección (**PCN 1.4.1. Revisión sistemática**) y cada vez que hay un plan de acción o proyecto derivado de una no-conformidad en una auditoría o unas lecciones aprendidas tras un incidente o simulacro (**PCN 1.4.2. Lecciones aprendidas**).
- **Objetivos operativos** dependientes del proceso: se trata de los RTO o tiempos objetivos de recuperación y otro tipo de objetivos puntuales que son dependientes de un proceso concreto (**PCN 2.2.2. Análisis de Impacto I=F(t)**).

En este contexto, la política va acompañada en su formulación de unos **objetivos que no caducan**, porque los va a perseguir la organización permanentemente. Los que habíamos visto hasta ahora eran o tácticos o bien operativos, y ahora ampliamos la oferta.

Aunque la política es una pieza formal del sistema, se vuelve también práctica al asociarle unos objetivos específicos. Entre los objetivos estratégicos que pueden plantearse, estarían:

- En primer lugar, dar prioridad a la **seguridad** de las personas que trabajan en la entidad y a las que tienen relación con ella.
- Prevenir y **evitar daños** de los incidentes que pueda tener la empresa.
- **Mejorar la disponibilidad**, reduciendo los tiempos previstos de las recuperaciones tras un incidente, o **RTO**.

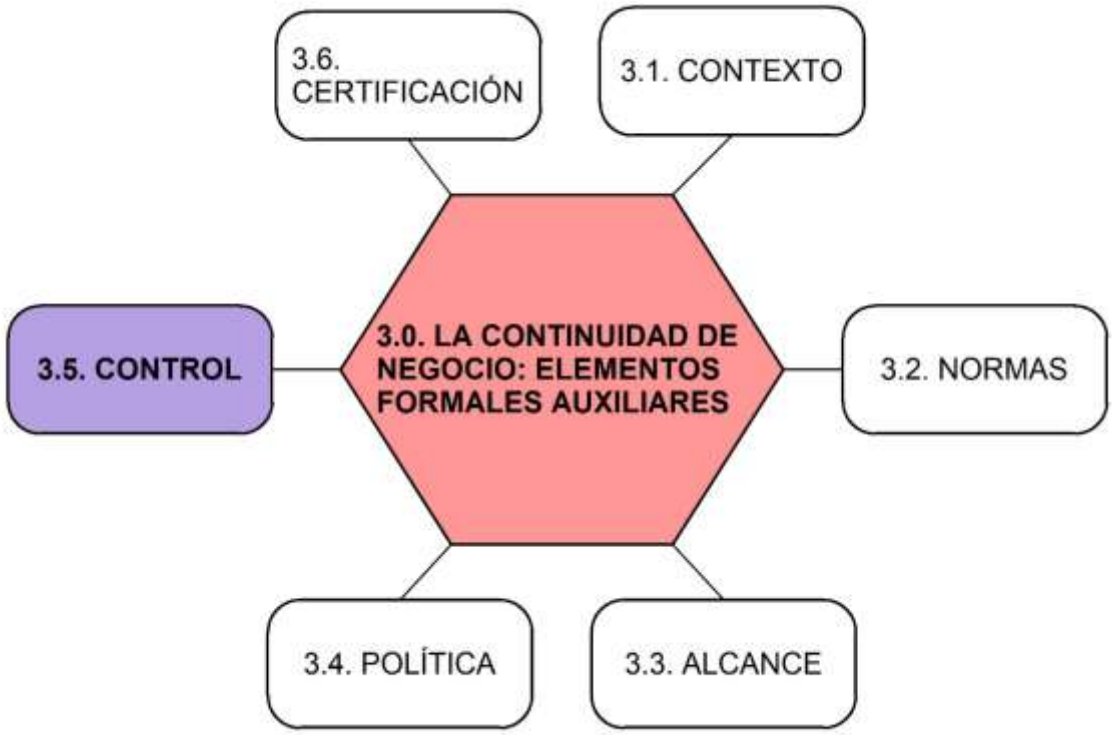
Una vez visto el punto de la política vamos a fijar ciertos **elementos de control**, especialmente de información.

PCN 3.5. CONTROL

La planificación y el control (conceptos ligados completamente en la gestión de proyectos) se emplean en el proyecto de crear, mantener y mejorar un sistema de gestión de continuidad, como herramientas en manos del responsable de continuidad o _PCN_. Son sus 'armas de gestión'.

En la norma **UNE-EN ISO 22301** se mencionan elementos que sirven para caracterizar el sistema y gestionarlo de cara al resultado y mostrarlos en las auditorías. Pero para el manejo del proyecto se necesita manejar documentación que normalmente no trasciende o de la que la organización no se ocupa, pero que es vital para el responsable de continuidad, que hemos representado por el símbolo **_PCN_**.

Para llevar a buen término un sistema tan completo como es el de continuidad de negocio, sobre todo para la gestión de los planes de acción, hemos mencionado más de una vez la conveniencia de emplear herramientas informáticas de **gestión de proyectos**. Cuando haya muchas tareas enlazadas y *multidependientes* no hay nada como un diagrama de Gantt. Hay *software* de pago extraordinario, como puede ser el **MS Project** que no se vende junto con MS Office, aunque puede interactuar con varias de sus aplicaciones. Si queremos hacer algo más modesto tenemos aplicaciones para PC (**Ganttproject**) y también para Android (**Project Schedule**).



Control global del proyecto.

¿No echamos algo más en falta?

El **responsable de continuidad _PCN_** debe tener control sobre un número de informaciones importantes de las que vamos a enumerar algunas:

- **Listas de personal** que constituye el gabinete de crisis _**GC**_ y los distintos _**ERI**_ para poderlos convocar de la manera que se establezca cuando haya un incidente.
- **Lista de las alarmas** codificadas para las llamadas según las emergencias que se planteen.
- **Análisis de Impacto** detallado de los procesos y mapa de procesos incluyendo los resultados generales de dichos análisis a fin de poder discernir en caso de crisis las prioridades de asignación de recursos a los procesos de más exigencia de disponibilidad.
- **Apreciación de riesgos**, escenarios y estrategias, de forma que se tenga un mapa de riesgos que permita en caso de crisis asignar mejor las prioridades de los recursos que puedan abordar los riesgos de más capacidad para producir daños a las instalaciones.
- **Resultados de las auditorías**, para poder comprobar periódicamente el grado de cumplimiento de las correcciones de las no-conformidades sin dejar ninguna por tratar debidamente antes de la siguiente auditoría.
- **Tabla de planes de acción** de las no conformidades y acciones de mejora que permita conocer si se van reduciendo las acciones aún abiertas o se incrementan las solucionadas, a fin de dedicar más recursos a las que demuestran ser más resistentes y poder animar a los responsables de procesos que llevan retraso en sus trabajos.
- Tabla de la previsión del **plan de simulacros**, a fin de que se realicen los que estaban previstos y haya tiempo para programar todas y cada una de las fases de todos ellos (**PCN 2.3.3. Incidentes y simulacros**).
- Tabla de los elementos del **plan de formación** para el personal en sus distintas fases de contacto con el sistema, desde su incorporación a la empresa hasta hacerse cargo de un _**ERI**_ o de un proceso.

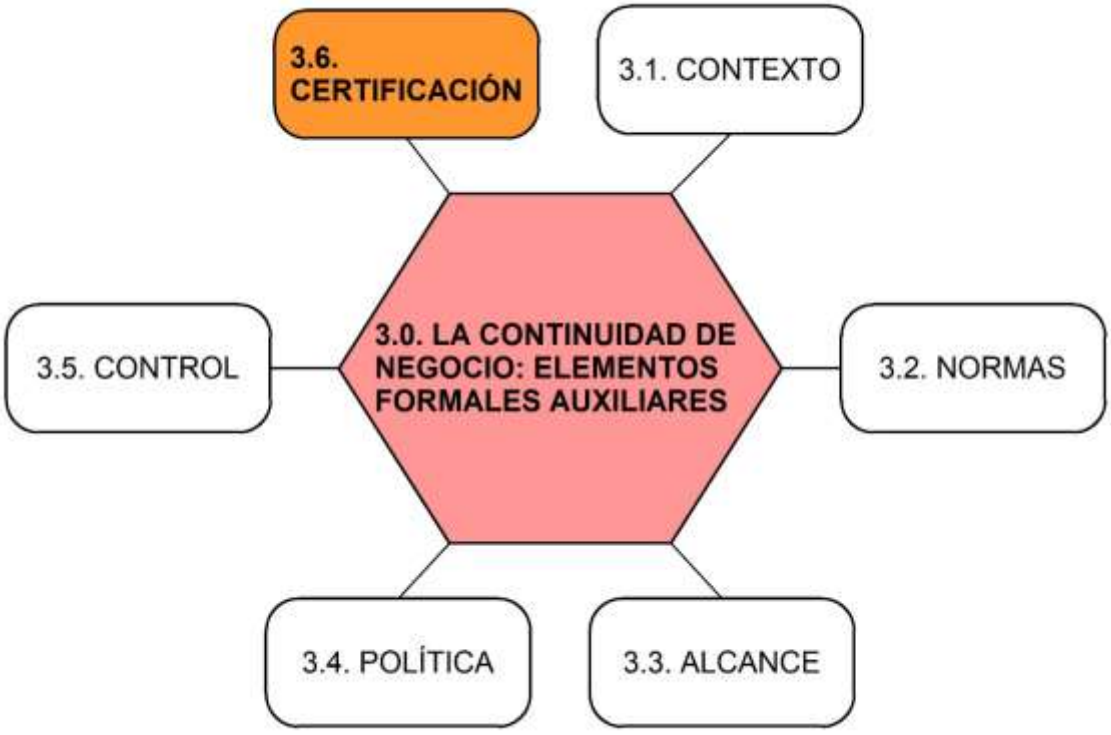
Bueno, esto está mejor. Necesitamos un premio. Una **certificación** nos vendría bien…

PCN 3.6. CERTIFICACIÓN

El justo premio a un trabajo excelente es pasar un examen y que alguien que sabe más que nosotros nos diga que 'hemos logrado el aprobado' y nos ponga una buena nota. Las tareas a realizar para corregir las no-conformidades entonces se hacen con gusto con tal de tener el expediente limpio y demostrar que tenemos capacidad suficiente.

De la misma manera que los estudiantes quieren aprender, progresar en el desempeño de lo que están estudiando, también como condición satisfactoria necesitan tener una nota que suponga el **reconocimiento** de un esfuerzo continuado, el **responsable de continuidad _PCN_** pelea por obtener la certificación del sistema por parte de un organismo independiente.

Hasta el momento de conseguirlo, probablemente se encontrará en su organización un cierto grado de **incomprensión**, porque los conceptos de continuidad son nuevos y un tanto abstractos (nosotros nos hemos esforzado durante este recorrido por emplear el menor número de palabras 'extrañas') y porque al principio **los objetivos parecen inalcanzables**. Pero hay un ***cambio de fase*** en el momento en que se consigue por fin superar la fase de auditoría con un resultado favorable. Entonces se observa cómo el equipo se refuerza y la relación entre todos los participantes mejora.



La certificación es un premio que se anuncia con un diploma acreditador de haber logrado el objetivo.

¿Quién puede auditarnos para lograr la certificación?

En España **AENOR** es una buena opción. Es el organismo encargado de editar las normas UNE que traducen y adaptan las ISO para las empresas españolas y tiene además capacidad de auditar no sólo el **sistema de continuidad** sino otros muchos

sistemas de gestión, como, entre otros el **de calidad**, o el **de seguridad de la información**.

EPÍLOGO

Deconstrucción del título y de la frase solemne sobre los negocios.

¿El título no era “LA CONTINUIDAD DE NEGOCIO PASO A PASO, **Análisis de riesgos y gestión de crisis**”?

No hemos visto en el texto ningún capítulo dedicado específicamente a estas dos últimas afirmaciones. La verdad es que haberse olvidado de estos temas hubiera sido imperdonable, porque son dos de los conceptos que más se repiten cuando se habla de continuidad de negocio. El truco está en el método empleado en el libro para la introducción de todos los conceptos, evitando conscientemente emplear el lenguaje de los técnicos, que, a fuerza de utilizar algunas palabras, les quitan el significado que deberían tener en el lenguaje ordinario. Por ejemplo, si empleamos continuamente contaminación (palabra técnica) en lugar de suciedad (palabra ordinaria), aunque definamos así muy bien el concepto, lo alejamos de la experiencia y sensación que produce la palabra ordinaria.

Fijémonos en dos partes concretas del diagrama del curso:

Detalle de dos partes del libro en donde tratamos el análisis de riesgos y la gestión de crisis.

La parte **1.2 AMENAZAS**, tiene cuatro capítulos:

- 1.2.1. Riesgos
- 1.2.2. Gravedad estimada
- 1.2.3. Probabilidad ocurrencia
- 1.2.4. Escenarios

Son los aspectos clásicos que se requieren en un **análisis de riesgos**, para evaluarlos en función de los dos parámetros, el de gravedad y el de probabilidad. Para acabar configurando unos **escenarios** de crisis y ordenarlos según su **evaluación**.

La parte **2.1 EPIDEMIA**, tiene estos cuatro capítulos:

- 2.1.1. Alarmas: guardias y mecanismos de contacto
- 2.1.2. Llamadas: escalonamiento según gravedad
- 2.1.3. Organigrama: roles y responsabilidades
- 2.1.4. Gestión de crisis y recuperación

Esta parte la hemos dedicado a introducir las actuaciones típicas de la **gestión de crisis** que afecta, fundamentalmente en este caso, al personal. Nos ha valido para conocer el **flujograma de actuaciones** en estos casos y para hablar de forma natural de la **organización** que la entidad necesita para llevar a cabo las actuaciones. Las enseñanzas de este caso son extensibles a todos los casos de crisis.

De esta forma hemos conseguido no aburrir al lector con la *gramática* del lenguaje de continuidad, empleando palabras o conceptos corrientes, pero consiguiendo que no quede ningún concepto importante por tratar y habilitándonos de forma natural para la **actuación inmediata**.

Lo mismo ocurre con otros conceptos fundamentales de continuidad de negocio. Solo mencionaré ahora, por ejemplo, el **análisis de impacto en función del tiempo**, que lo introducimos en otro caso, el caso de desabastecimiento, en el capítulo 2.2.2 Análisis de Impacto I=F(t). Y así ocurre con otros aspectos, que se van introduciendo donde más fácil es ver su función.

Y ahora la frase solemne:

> **“Los grupos humanos, las sociedades y los negocios** hacen lo que saben y pueden con el objeto de lograr su supervivencia y bienestar… es una continua sucesión de acciones de **autodefensa** y **continuidad**. Todo ello **economizando** …”

No tiene sentido hacer nada que cueste más que el problema que queremos evitar. Si un seguro costara el doble, habría muchos menos clientes que optaran por contratarlo. De igual forma, las actuaciones de continuidad suelen cumplir la condición de que **se priorizan los recursos para los escenarios que pueden causar más daño** y son más probables. Yo me decanto por la primera condición, la del daño, ya que nunca vamos a estar totalmente exentos de un riesgo inesperado por improbable, que pueda cambiarlo todo, lo que se conoce como un **cisne negro**. En caso de duda intentaría siempre **evitar la exposición a los riesgos** empezando por los que puedan ser más dañinos. En eso consiste acometer acciones de autodefensa pensando en economizar.

Aquí termina esta introducción a la continuidad de negocio. Gracias por la atención.

ANEXO 1.- BIBLIOGRAFÍA

Aunque el texto está pensado como un instrumento de divulgación autocontenido, se incluyen a continuación unas pocas referencias de publicaciones útiles para ampliar conocimientos y continuar con la lectura.

Muchas referencias que hubieran sido objeto de notas al pie (que deliberadamente se han evitado), se acceden mediante **enlaces o hipervínculos incluidos en el texto**, evitando hacer demasiado farragosa la lectura.

Las **publicaciones oficiales** más importantes, de las que citamos algunas a continuación, son las **normas** internacionales, que definen de forma exhaustiva y reglamentada las prescripciones necesarias para establecer sistemas de gestión documentales y certificables. También los **organismos gubernamentales** competentes son fuentes valiosas de información, difundiendo métodos correctos de actuación conforme a las normas, leyes y reglamentos vigentes.

Publicaciones oficiales:

- AEPD. (2018) *Guía análisis de riesgos RGPD*.

- CCN-CERT. (2020). *Gestión de ciber-crisis*.

- INCIBE. *Ciberseguridad Gestión de riesgos*.

- INCIBE. *Plan de contingencia y continuidad de negocio*.

- Ministerio de Defensa. (2018). *Doctrina para el empleo de las FAS.*

- *Norma UNE EN ISO 22301: Sistema de Gestión de Continuidad de Negocio*. (2019). AENOR.

- *Norma UNE EN ISO 27001: Sistema de Gestión de Seguridad de la Información*. (2014). AENOR.

Muchas de las publicaciones que se incluyen a continuación en esta lista sobre continuidad de negocio, análisis de riesgos y gestión de crisis, se publicaron antes de la edición de las normas oficiales sobre continuidad (La UNE EN ISO 22301 en 2014). Por ese motivo pueden estar en algún aspecto desactualizadas, ya que las normas, si se han editado posteriormente, son el resultado del mejor acuerdo entre los distintos actores del asunto cuando ya ha habido un importante consenso sobre contenidos y terminología y son las que servirán de referencia para los procesos de certificación.

Libros sobre continuidad, riesgos y crisis:

- Aven, T. (2003). *Foundations of risk analysis*. Wiley.

- Barnes, J. C. (2001). *A Guide To Business Continuity Planning.* Wiley

- Blyth, M. (2009). *Business Continuity Management*. Wiley.

- Casal, J. & al. (1999). *Análisis del riesgo en instalaciones industriales.* UPC.

- Da Costa, N. (2004). *Operational Risk with Excel and VBA*. Wiley

- Fontenla Ballesta, S. (2002). *Un concepto de Acción conjunta*. ESFAS.

- González, J. R. (2015). *El factor humano en el análisis de riesgos.* UPC.

- Haimes, Y. (2009). *Risk Modeling, Assessment and Management* (3ª edición). Wiley.

- Molak, V. (1997). *Fundamentals of Risk Analysis and Risk Management*. CRC.

- Mun, J. (2006). *Modeling Risk Applying Monte Carlo Simulation.* Wiley

- Olson, D. & Dash Wu, D. (2017) *Enterprise Risk Management Models*. (2ª edición). Springer.

- Osborne. (2021). *Practical Business Continuity Management 2: 101 More tips for effective, Real-World Business Continuity Management (English Edition)*. Amazon (libro electrónico).

- Snedaker, S. (2007). *Business Continuity and Disaster Recovery Planning for IT Professionals*. Syngress.

- Sutton, D. (2018). *Business Continuity in a Cyber World*. BEP.

- Taleb, N. (2017). *Antifrágil: Las cosas que se benefician del desorden* (1ª edición, 4ª reimpresión). Paidós Transiciones.

- Taleb, N. (2008). *El cisne negro. El impacto de lo altamente improbable* (1ª edición, 7ª reimpresión). Paidós Booket.

- Wallace, M. & Webber, L. (2004). *The Disaster Recovery Handbook A Step By Step Plan*. Amacom

- Watters, J. (2014) *Disaster Recovery, Crisis Response, and Business Continuity*. Apress.

Libros sobre organización empresarial e investigación operativa:

- Davim, J. Paulo. (2016). *Design of Experiments in Production Engineering.* Springer.

- Deming, E. (1989). *Calidad, productividad y competitividad. La salida de la crisis*. Díaz de Santos, S.A.

- Taha, Hamdy A. (2004). *Investigación de operaciones* (9ªedición). Pearson.

Libros sobre la aleatoriedad del entorno:

- Gleick, J. (2012). *Caos. La creación de una ciencia*. (1ª edición) Crítica.

- Mandelbrot, B. (2021). *La geometría fractal de la naturaleza*. (1ª edición) Tusquets.

- Smith, L. (2007). *Caos: una breve introducción*, Alianza editorial.

- Stewart, I. (1989). *¿Juega Dios a los dados?* (1ª edición) Grijalbo Mondadori.

Libros clásicos que hay que leer:

- Homero. (1968). *La Ilíada* (8ª edición). [Colección Austral]. Espasa Calpe S.A.

- Tzu, S. (2020). *El arte de la guerra* (8ª edición). EDAF.

Web del autor:

-unoydostres.com. Aquí se puede encontrar mucha información sobre continuidad. Por ejemplo: Cómo prepararnos racionalmente para superar incidentes y crisis.

ANEXO 2.- SOFTWARE ÚTIL PARA CREAR DIAGRAMAS Y ESQUEMAS

Vamos a presentar muy brevemente varios programas gratuitos que pueden facilitar el trabajo, sobre todo en pequeñas organizaciones o autónomos, aliviando los costes de mantenimiento de los sistemas documentales.

Por lo general, las empresas se pueden permitir disponer de ***software* de pago**, que tiene sin duda mejor soporte técnico en caso de problemas y muchas más prestaciones que permiten hacer desarrollos para los que no están pensadas muchas de las **aplicaciones gratuitas**. Por ejemplo, los programas de la *suite* **MS Office** son líderes en todas sus facetas, tanto en la edición de textos como en hojas de cálculo o datos. Pero su *suite* homóloga **Libre Office** es capaz de detalles en los que sorprende su versatilidad y en general es suficiente para la mayoría de necesidades. Ambas tienen una larga experiencia en la informática personal y sus formatos de fichero son mayormente compatibles.

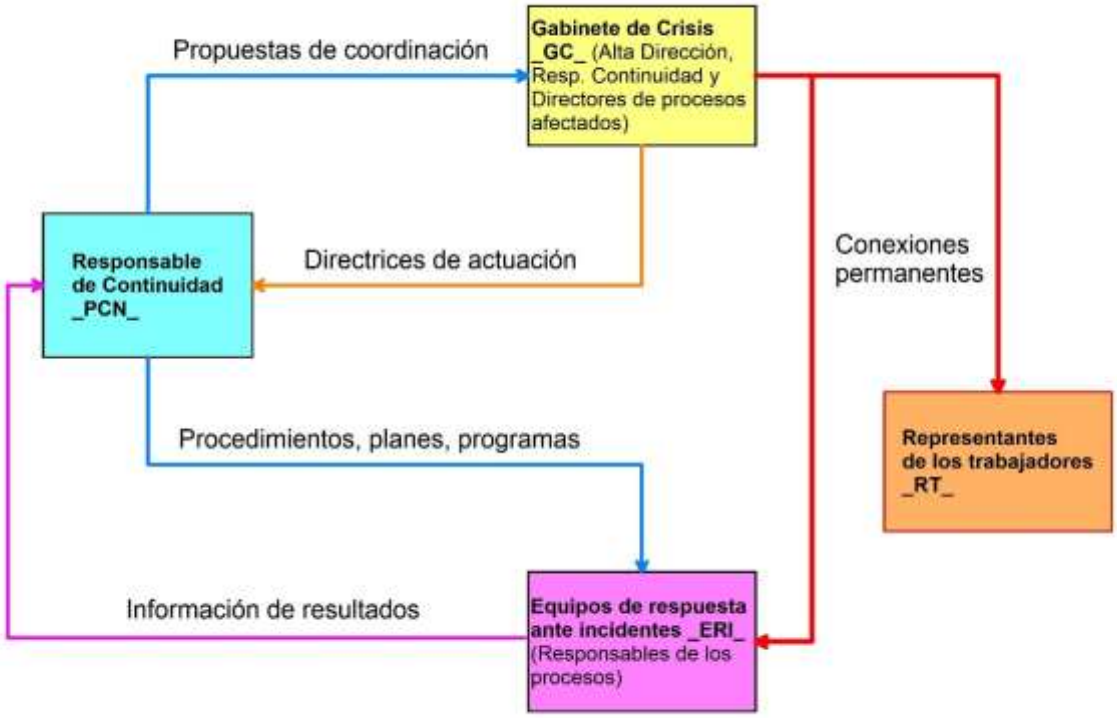
Bien es verdad que **Microsoft ofrece su *suite* como accesorio a la contratación de su almacenamiento en la nube**, lo que la hace muy accesible económicamente, pero tener alternativas nunca es malo, si sirven para conseguir los resultados deseados, ya que no siempre estaremos en el ordenador o red para la que tengamos licencia y **LibreOffice puede ejecutarse en modo portable** desde un disco externo o un *pendrive*, lo que nos da una movilidad y libertad infinita para la edición de nuestros datos.

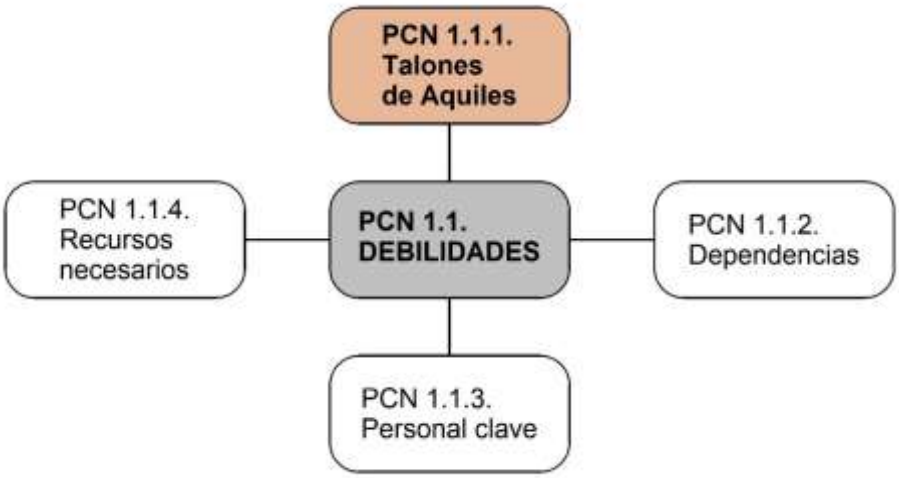
En cuanto a los **programas de generación de gráficos** que presentamos, ambos tienen campos especializados y su uso es muy sencillo, sin requerir periodos previos de aprendizaje. Si solamente van a servir para editar figuras o esquemas que sirvan para textos específicos como nuestros documentos de continuidad, no hace falta pagar por una *suite* gráfica a la que no se le va a sacar partido.

Diagram Designer

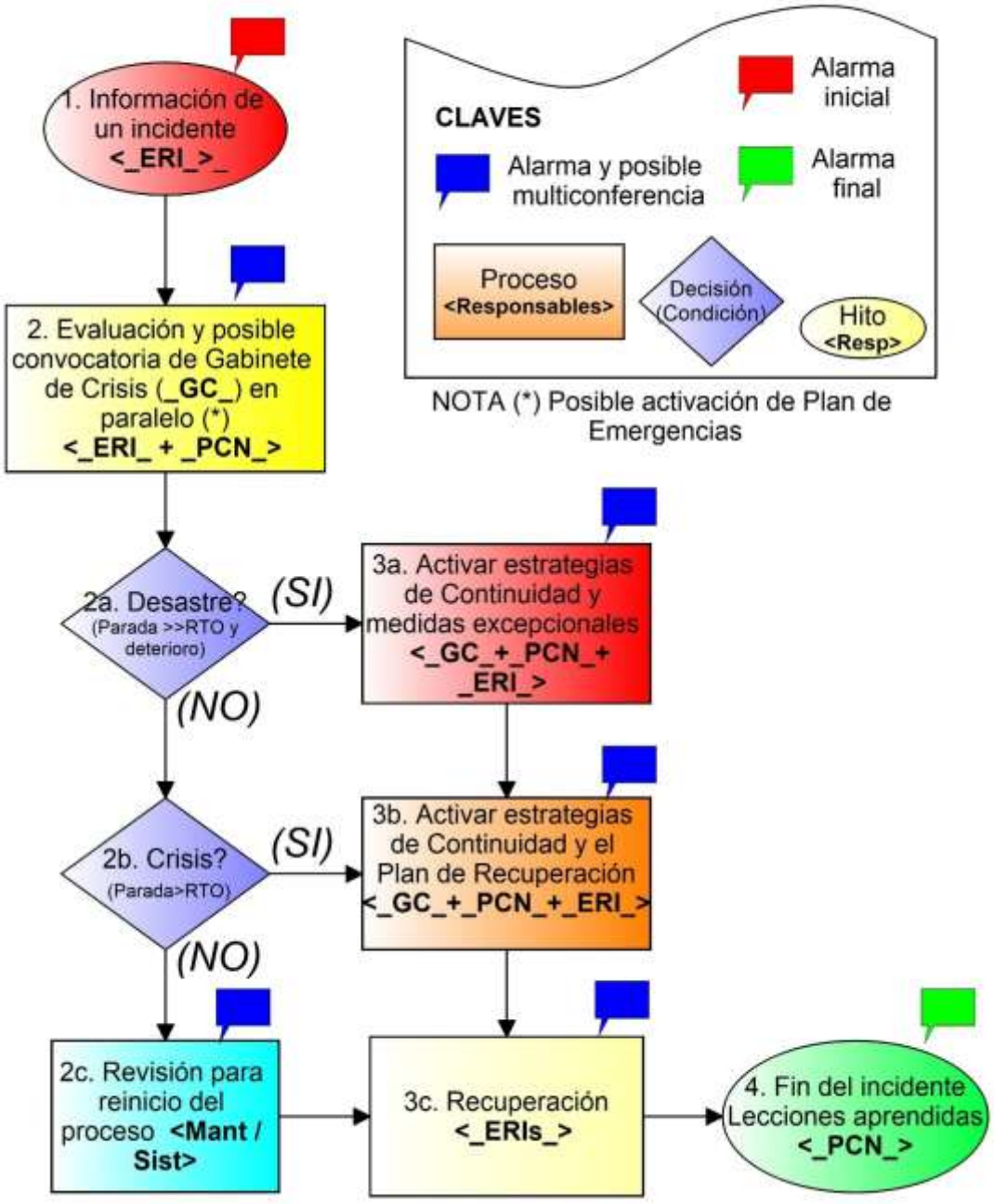
- Diagram Designer: **https://sourceforge.net/projects/diagramdesigner/**

Con este programa, muy adecuado para diagramas de flujo o esquemas organizativos, hemos preparado gráficos más bien 'rígidos' como éstos:



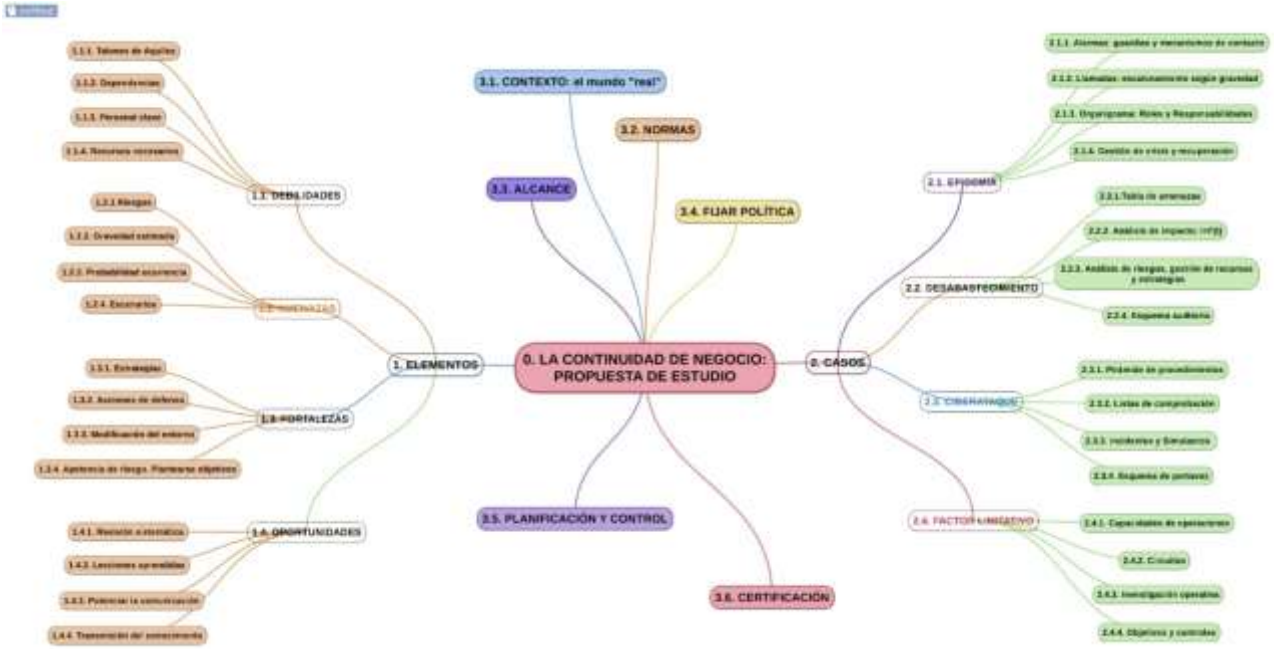


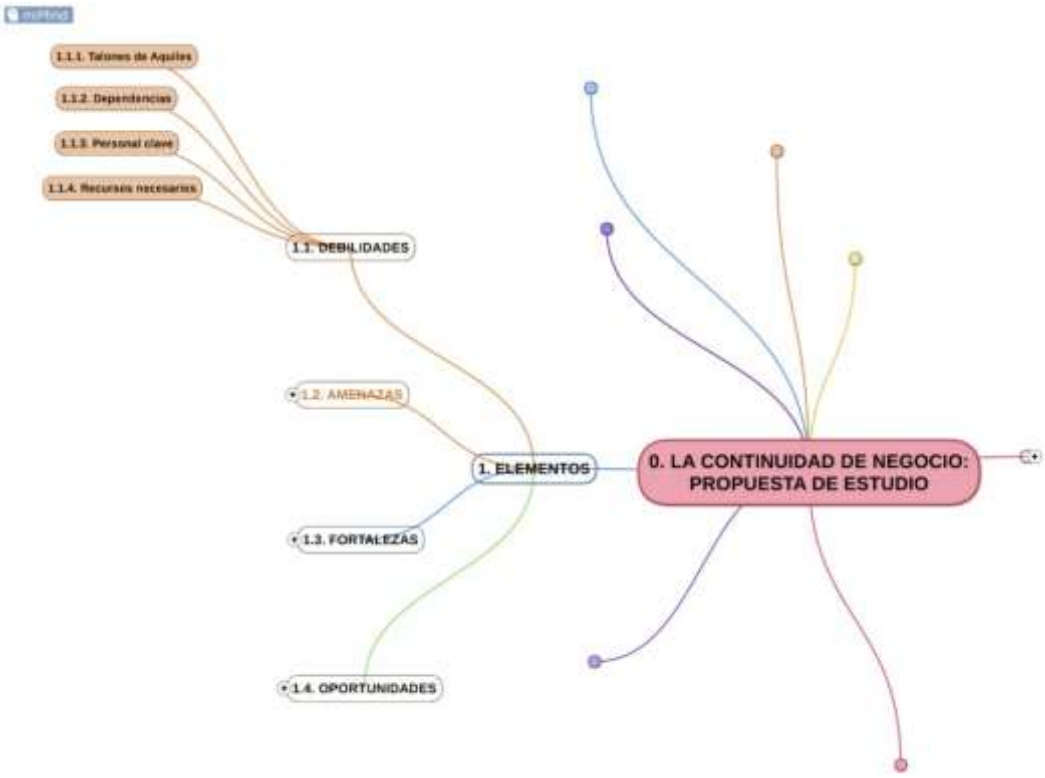
PCN: GESTIÓN DE CRISIS *(v2023 simplificada)*



- miMind: **https://mimind.cryptobees.com/**

Con este programa, absolutamente genial, especializado en realizar mapas mentales o resúmenes de un montón de relaciones hemos realizado los gráficos 'sinuosos' tipo 'pulpo':



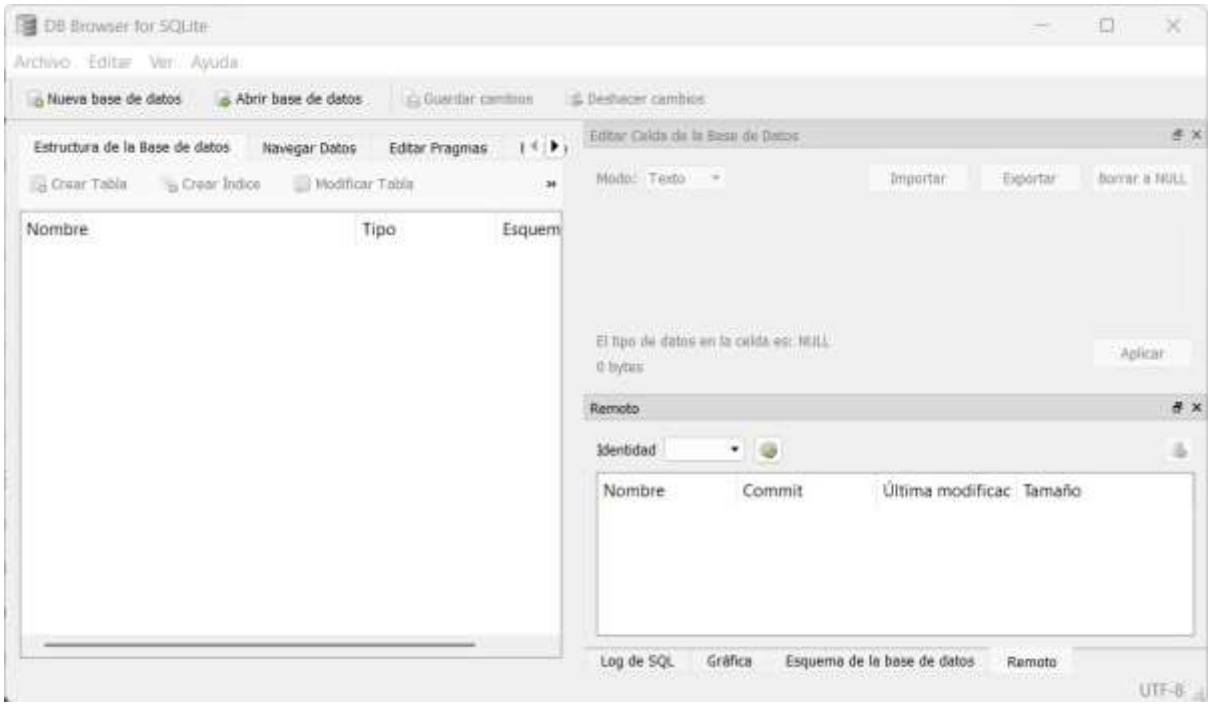


SQLite Browser

- SQLite: **https://sqlitebrowser.org/**

Este programa puede generar bases de datos profesionales partiendo de ficheros de texto conocidos como CSV (Comma Separated Values), que es uno de los formatos que puede guardar una hoja de Excel de forma nativa. Aunque no se ha hecho énfasis sobre este programa en el texto, cualquiera de las tablas de nuestra lista de procesos u otras que hayamos generado en nuestro trabajo en la puesta en marcha del sistema de gestión quedarían perfectamente guardadas en una base de datos. Es, junto con las bases de datos de Oracle y de Microsoft, el motor de bases de datos más empleado en el mundo y está en segundo plano de muchas de las aplicaciones que manejamos diariamente. No hay que ver esta aplicación en modo alguno como una aplicación menor pues, a pesar de su pequeño tamaño y que no necesita ningún servidor para funcionar puede generar bases de datos completamente profesionales.

Hay una **versión portable** de esta *suite* que la recomiendo porque es posible arrancarla desde un *pendrive* en cualquier ordenador, sin necesidad de más protocolo. Se puede encontrar esta versión en la página de **portableapps.com**



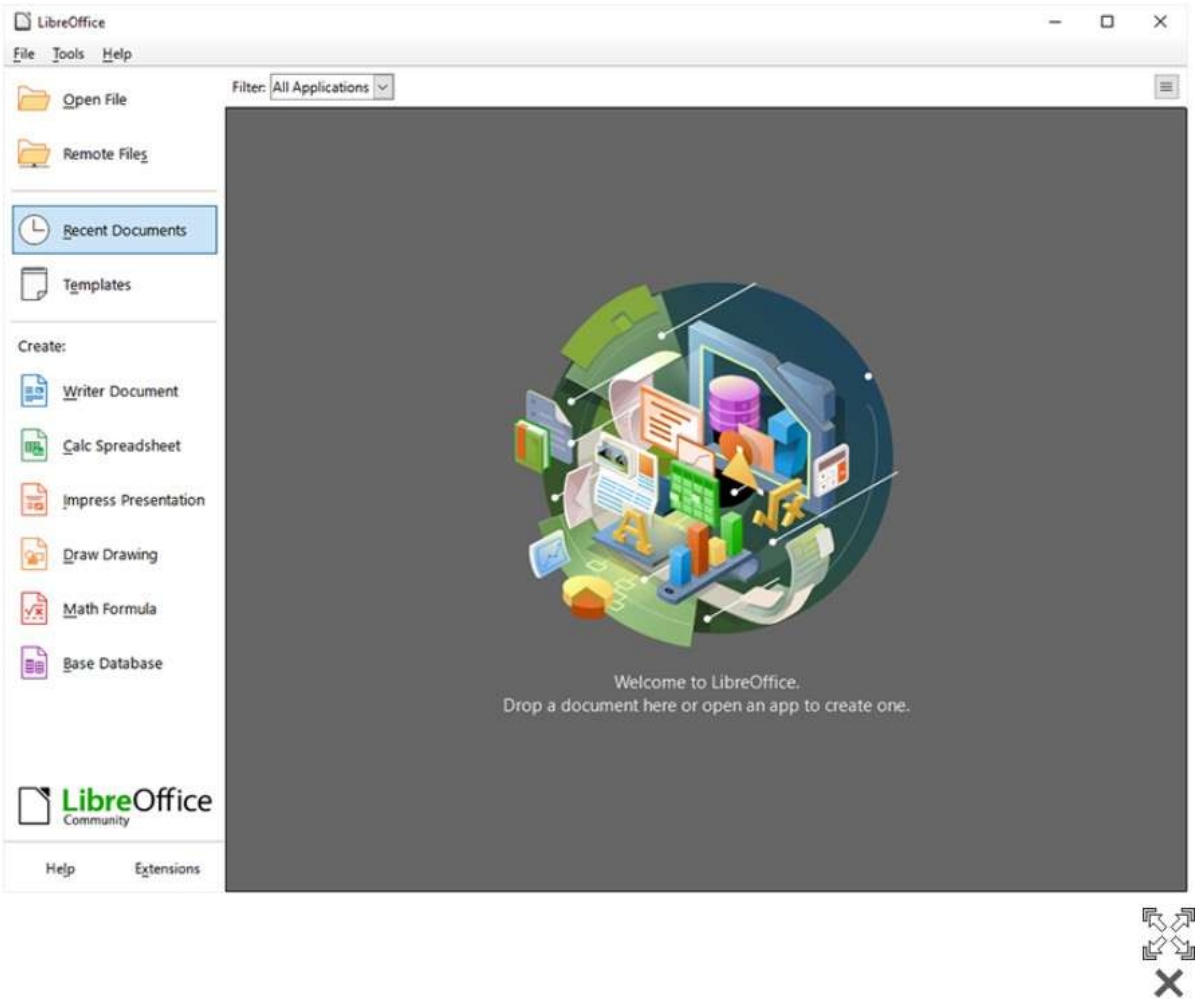
SQLite DB Browser. Impresión de pantalla.

LibreOffice

- LibreOffice: **https://es.libreoffice.org/**

La *suite* Libre Office, se puede emplear para producir directamente los ficheros en formato ePub a partir de textos en formato DOCX, editados con Libre Office o con Word**.** Word de MS Office es una magnífica opción para la edición del texto y para su exportación a PDF. Pero Word no incluye en sus prestaciones la exportación a ePub, como si hace Libre Office, que puede crear directamente, a partir de ficheros en formato DOCX, ficheros ePub con la misma facilidad que los crea en PDF.

Aprecio también la versión portable de esta *suite* porque puedo arrancarla desde un *pendrive* en cualquier ordenador. Se puede encontrar esta versión en la página de **portableapps.com**



LibreOffice. Impresión de pantalla.

Calibre

- Calibre: **https://calibre-ebook.com/es/download**

Aunque la *suite* Libre Office es una solución "todo en uno", **Calibre es la aplicación de referencia para producir ficheros ePub.** Con Calibre tenemos una colección de herramientas diseñadas específicamente para este propósito. **La versión en ePub de este documento que estamos leyendo se ha obtenido con Calibre**. Comparado con Libre Office, Calibre permite un mayor control de todos los detalles de la edición del ePub, como por ejemplo crear una tabla de navegación más rica, que es esencial cuando estamos trabajando con un fichero para ser leído en medios digitales como el ordenador, la tablet o incluso el teléfono.

Calibre en Windows. Impresión de pantalla.

La aplicación **Calibre** no solo sirve para *transformar* cualquier documento DOCX en ePub, sino que permite *editar* el propio ePub en todos sus detalles y además, incluye un estupendo lector de libros electrónicos, así como una base de datos para *mantener la colección* de libros digitales.

Además de la versión para instalar, también se puede optar por la solución portable, que se encuentra en **https://portableapps.com/apps/office/calibre-portable**, que es ideal para un uso más ocasional, y puede arrancarse desde un pendrive en cualquier situación, sin tener que instalarla en ningún ordenador.

ESTO ES TODO ■