ISO 22301 (LISTA DE VERIFICACIÓN DE CONTINUIDAD DE NEGOCIO)

1 Cláusula 4 Conozca su organización

Antes de empezar a diseñar planes de continuidad de negocio, tiene que ser capaz de definir su organización. Una organización no sólo se define por lo que produce, sino también por lo que la conforma e influye en ella.

Es posible que haya partes interesadas y normativas que influyan en su organización y su planificación.

Enumere los problemas internos y externos que impulsan la necesidad de planificar la continuidad de negocio:	
Enumere las partes interesadas y sus requisitos:	
Enumere las leyes y reglamentos pertinentes y asegúrese disponer de un proceso para ello:	

2 Cláusula 4 Limite su SGCN a lo que realmente importa

Conociendo su organización y teniendo en cuenta su misión u objetivos empresariales, puede establecer los límites de su Sistema de Gestión de la Continuidad de Negocio (SGCN).

Probablemente no necesite un plan para toda la organización; limite el alcance a lo importante.

Enumere las partes de la organización que deben estar en el ámbito de certificación:	
Enumere los resultados (productos y servicios) que deben figurar en el ámbito de certificación:	
Documente y explique las exclusiones:	

3 Clásula 5 Asegúrese de que la gerencia está comprometida con el SGCN.

Al igual que la gerencia dirige y dota de recursos a una organización para que cumpla su objetivo, debe hacer lo mismo con la gestión de la continuidad del negocio.

Comience con una política, una declaración de intenciones, que a su vez impulse la necesidad, las actividades y los recursos.

Redacte una política de continuidad de negocio:	
Difunda la política a todos las partes interesadas (tanto internas como externas):	
Defina las funciones y responsabilidades para la continuidad de negocio:	
Asegúrese de que alguien de la gerencia es responsable del SGCN y documente cuáles son sus responsabilidades:	

4 Cláusula 6 Establecer objetivos

Una vez que tenga una política de continuidad de negocio, puede empezar a planificar.

La continuidad de negocio no está exenta de riesgos y oportunidades para su organización. Si sabe cuáles son, podrá establecer algunos objetivos.

Averigüe cuáles son los riesgos y las oportunidades a nivel de la organización:

Decida qué tiene que hacer para resolverlos y aplique esas medidas en sus procesos operativos:

Establezca algunos objetivos de continuidad de negocio y lo que necesita para alcanzarlos y defina quién es el responsable:

Decida cómo va a supervisar y medir el rendimiento de los objetivos:

Asegúrese de que dispone de procesos de control de cambios para el SGCN:

5 Cláusula 7 ¿Sus recursos son capaces, competentes y suficientes?

Las personas son un recurso importante en un plan de continuidad de negocio y necesitará equipos y suministros: Quién, Qué, Por qué, Cuándo, Cómo y Dónde.

Decida qué recursos se necesitan (personal, tecnología e infraestructura). En el caso del personal, determine los conocimientos y habilidades necesarios:

Confirme que están presentes en su organización:

Asegúrese tener un plan de comunicación para la organización en general y para las partes interesadas externas:

Documente todo lo que exige la norma (hay una lista al final de este documento) y todo lo que considere necesario. Controle los cambios en sus documentos:

DOCUMENTOS OBLIGATORIOS EN LA ISO 22301:2019

Cláusula	Documento	Cláusula	Documento
4.2.2	Requisitos legales, reglamentos o leyes aplicables, y cualquier otro requisito identificado	8.4.2.4	Procedimientos documentados para cada respuesta
4.3.1	Alcance del SGCN	8.4.3.1	Procedimientos de aviso y comunicación
4.3.2	Exclusiones del alcance del SGCN	8.4.4.1	Planes de continuidad de negocio
5.2.2	Política de continuidad de negocio	8.4.5	Procesos de recuperación y restauración
6.2.1	Objetivos de continuidad de negocio	8.5	Informes posteriores al ejercicio
7.2	Pruebas de la competencia del personal	9.1	Resultados del seguimiento, la medición, el análisis y la evaluación del rendimiento del SGCN
7.5.1	Documentación requerida por la norma y cualquier otra que se considere necesaria para la eficacia del SGCN.	9.2.2	Pruebas de la aplicación del programa de auditoría y de los resultados de la misma
8.1	Información necesaria para confiar en que los procesos de planificación y control operativo se están llevando a cabo según lo previsto	9.3.3.2	Resultado de las revisión por la dirección
8.4.1	Planes y procedimientos de continuidad de negocio	10.1.3	Naturaleza de las no conformidades y lo que se hizo al respecto, así como los resultados de la acción correctiva

6 Cláusula 8 Realice un análisis de impacto empresarial (BIA)

Cuando ocurren perturbaciones, pueden ser temporales o alargarse en el tiempo. Las consecuencias pueden alargarse más aún.

Hay que saber qué es importante para la organización, cuáles son las consecuencias de la perturbación en el tiempo y cuánto tiempo se puede tolerar. Esto se resuelve con un Análisis de Impacto Empresarial (BIA o "Business Impact Analysis" por sus siglas en inglés).

Defina los impactos y sus criterios para realizar el BIA. Esto garantizará que las evaluaciones sean coherentes y repetibles:

Enumere las actividades clave que componen sus productos y servicios:

Identifique los recursos internos y externos necesarios para ofrecer estos productos y actividades (personal, equipos, tecnología, suministros, infraestructura):

Utilice los criterios para calcular el impacto empresarial a lo largo del tiempo en las actividades clave:

Decida cuánto tiempo pasará antes de que los impactos empresariales sean inaceptables (MTPD o periodo máximo tolerable de disrupción).

Fije plazos para recuperar las actividades hasta los niveles mínimos aceptables (MBCO o objetivos mínimos de continuidad de negocio).

Una vez determinados los impactos, hay que decidir qué actividades deben tener prioridad para la recuperación.

Defina los impactos y sus criterios para realizar el BIA. Esto garantizará que las evaluaciones sean coherentes y repetibles:

Enumere las actividades clave que componen sus productos y servicios:

7 Cláusula 8 Realice una evaluación de riesgos

Ahora que conoce las actividades clave, debe considerar los riesgos que corren. Esto le ayudará a determinar la probabilidad de que se interrumpan y, por tanto, su impacto en la empresa.

Priorice los riesgos para su tratamiento, lo que impulsa las estrategias de continuidad de negocio y luego los planes. La ISO 31000 es un buen recurso para la evaluación de riesgos.

8 Cláusula 8 Cree estrategias y soluciones de continuidad empresarial

Sus estrategias deben tener en cuenta los riesgos y los requisitos del BIA.

Dado que se trata de un enfoque basado en riesgos, habrá que tener en cuenta la relación coste-beneficio. Y deben ser realistas, teniendo en cuenta la disponibilidad de los recursos que se consideren necesarios para lograr el éxito.

9 Cláusula 8 Defina procedimientos y planes para lograr las estrategias

Aquí es donde se define la respuesta a los incidentes. Se trata de la movilización de los recursos identificados en sus estrategias de manera oportuna y controlada.

Procedimientos:

- **Deben ser a la vez específico para abordar las medidas inmediatas, pero también lo suficientemente flexible para hacer frente a un incidente:**
- **Establecer un equipo de gestión de crisis:**
- **Definir las funciones y responsabilidades:**
- **Definir una estructura de respuesta para el equipo responsable:**
- **Deben gestionar las comunicaciones internas y externas:**

Planes:

- **Orientar a equipos sobre cómo responder, incluyendo el orden de actividades:**
- **Especificar los criterios para invocar las actividades:**
- **Proteger el bienestar de las personas:**
- **Qué medidas hay que tomar:**

Recuperación de normalidad

Desarrollar un plan y procesos que garanticen una transición fluida de recuperación a las operaciones normales.

10 Cláusula 8 Probar, probar y volver a probar

Muy pocos planes sobreviven a su primer uso. Es mucho mejor probar los planes antes de que sean necesarios. Un programa de ejercicios es la mejor manera de garantizar que los planes funcionen y evitar perder conocimientos. La evaluación de las capacidades de la organización es una parte esencial del ciclo de mejora continua que exige la norma.

11 Cláusula 9 Supervisión continua del rendimiento de la continuidad de negocio

Teniendo en cuenta todo lo definido en las cláusulas anteriores, aquí es donde se mide el rendimiento de su SGCN. Debe saber qué debe medir, quién, cómo y cuándo. La norma dictamina lo siguiente: "Necesita un programa de auditoría interna permanente y revisiones periódicas por parte de la dirección".

12 Cláusula 10 Mejora continua

A veces las cosas salen mal (no conformidades), por lo que hay que tener un proceso para:

- **Controlarlos:**
- **Arreglarlos:**
- **Averiguar qué sucedió:**
- **Tomar medidas para evitar su repetición:**