



ISO 22301:2019

GUÍA DE IMPLEMENTACIÓN DE SISTEMAS DE GESTIÓN
DE CONTINUIDAD DE NEGOCIO



53,000
CERTIFICATES
GLOBALLY



100%
TRANSPARENT
— FEES —

1000+
EMPLOYEES
WORLDWIDE

AVERAGE
CUSTOMER
PARTNERSHIP



OVER
100

OPERATING
COUNTRIES





> ISO 22301:2019

GUÍA DE IMPLEMENTACIÓN

Contenido

Introducción a la norma	P04
Ventajas de la implantación	P06
Principios clave y terminología	P08
Ciclo PDCA	P09
Pensamiento basado en el riesgo / auditorías	P10
Pensamiento basado en procesos / auditoría	P11
Anexo SLc	P12
CLÁUSULA 1: Alcance	P13
CLÁUSULA 2: Referencias normativas	P14
CLÁUSULA 3: Términos y definiciones	P15
CLÁUSULA 4: Contexto de la organización	P16
CLÁUSULA 5: Liderazgo	P18
CLÁUSULA 6: Planificación	P20
CLÁUSULA 7: Apoyo	P22
CLÁUSULA 8: Operación	P24
CLÁUSULA 9: Evaluación del rendimiento	P26
CLÁUSULA 10: Mejora	P27
Saque el máximo partido a su gestión	P28
Próximos pasos una vez implantado	P29





INTRODUCCIÓN A LA NORMA

ISO 22301:2019 es la última versión de la norma internacional para la Continuidad del Negocio. Esta norma proporciona un marco de mejores prácticas para apoyar a las organizaciones a gestionar eficazmente el impacto de una interrupción de su funcionamiento normal.

El propósito de la norma no es necesariamente lograr una mitigación total del impacto de la interrupción. Se trata de ayudar a una organización a comprender la cantidad y el tipo de impacto que está dispuesta a aceptar tras una interrupción. A continuación, la organización desarrolla un sistema de continuidad de negocio dimensionado correctamente para las necesidades de la organización.

Muchas organizaciones experimentarán en algún momento una interrupción de su actividad. Las causas y la naturaleza de las perturbaciones cambian constantemente. Las organizaciones deben ser capaces de pensar de forma dinámica sobre este panorama cambiante de amenazas y poner en marcha planes adecuados para mitigar los impactos.

La familia ISO 22300

El origen de la norma ISO 22301 se remonta al comité técnico ISO/TC 23, que se centró en abordar las preocupaciones relacionadas con la seguridad de la sociedad. En la actualidad, la norma está gestionada por ISO/TC 292 - Seguridad y resiliencia. La primera iteración de la norma ISO 22301 se publicó en 2012. La segunda edición se publicó en octubre de 2019 y es el tema central de esta guía de implementación.

La serie ISO 22300 consta actualmente de 11 normas. Las demás normas de la serie ofrecen orientaciones y requisitos más detallados sobre cuestiones específicas relacionadas con la continuidad de la actividad empresarial. Abarcan desde la gestión de la respuesta a emergencias hasta las evacuaciones masivas.

Revisiones y actualizaciones periódicas

Las normas ISO se revisan aproximadamente cada cinco años para evaluar si es necesario actualizarlas.

La actualización más reciente de la norma ISO 22301 en 2019 trajo consigo una serie de cambios. Mientras que la edición anterior (2012) fue una de las normas precursoras en adoptar un formato tipo Anexo SL, la nueva edición alinea firmemente la norma con el Anexo SL.

La versión 2019 de la norma refleja el movimiento más amplio de las normas ISO hacia la aplicación del pensamiento basado en el riesgo, la comprensión del contexto organizativo y la satisfacción de las necesidades de las partes interesadas. La versión 2019 contiene menos requisitos prescriptivos y es más flexible en su enfoque de la información documentada. La versión 2019 incluye además el nuevo requisito de planificar eficazmente los cambios en el Sistema de Gestión de la Continuidad del Negocio (BCMS).

Dentro de la serie, las normas más importantes para una organización que pretenda implantar un Sistema de Gestión de la Continuidad del Negocio eficaz son:

- **ISO 22300:2018 - Seguridad y resistencia**
– Vocabulario
- **ISO 22301:2019 - Seguridad y resistencia**
– Sistemas de gest. de la continuidad de negocio.
– Requisitos
- **ISO 22313:2020 - Seguridad y resistencia**
– Sistemas de gestión de la continuidad de las actividades
– Orientaciones. Proporciona orientaciones útiles en apoyo de la aplicación práctica y el funcionamiento de un sistema de continuidad de las actividades.

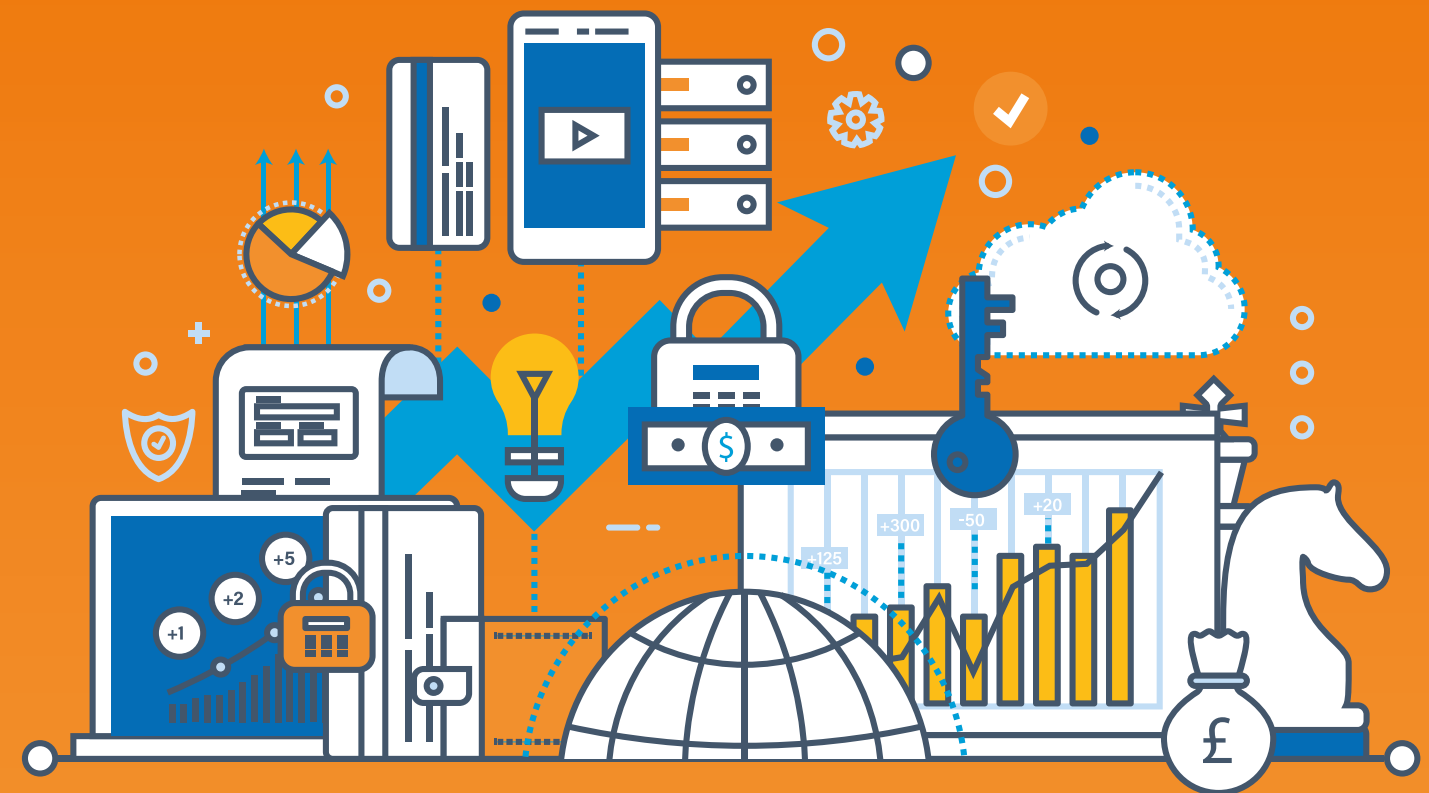


VENTAJAS DE LA APLICACIÓN

En los últimos tiempos se ha demostrado que la capacidad de una empresa para gestionar acontecimientos perturbadores se está convirtiendo en un factor esencial para su supervivencia. La variedad de amenazas que pueden causar perturbación empresarial es cada vez mayor. Desde los ciberataques y las pandemias mundiales hasta las catástrofes naturales; una organización necesita un conjunto de herramientas para gestionarse en tiempos de incertidumbre.

En el pasado, la planificación de la continuidad de las actividades solía reservarse a las infraestructuras nacionales críticas y a las grandes empresas. Hoy en día, la continuidad de negocio es una cuestión que afecta prácticamente a todas las organizaciones en algún grado. Un Sistema de Gestión de la Continuidad de Negocio correctamente implantado debe adaptarse al tamaño y complejidad de la organización, por lo que es adecuado tanto para PYMES como para grandes corporaciones.

El objetivo principal de un Sistema de Gestión de la Continuidad de Negocio es permitir la mitigación de una interrupción. Dependiendo de la organización, los beneficios que aporte servirán para apoyar sus objetivos, ya sea salvar vidas en un hospital o reducir el impacto financiero en una empresa manufacturera.



RESISTENCIA VISIBLE

Un SGCN eficaz demuestra a los clientes actuales y potenciales que la organización está preparada para afrontar perturbaciones. Esto es especialmente importante en sectores en los que las interrupciones pueden tener repercusiones significativas en la vida de las personas, así como repercusiones financieras, como la administración pública, la sanidad, las finanzas, la defensa y los servicios sociales.



VENTAJA COMPETITIVA

Ser capaz de seguir operando durante o poco después de una perturbación da a una empresa una ventaja competitiva. A corto plazo, puede ser capaz de ganar negocios a competidores que no pueden operar o lo están haciendo con una capacidad reducida. A largo plazo, una empresa puede generar beneficios de reputación que atraerán a los clientes, así como beneficiarse de una mayor capacidad financiera.

Además, un SGCN ayuda a una organización a licitar o presentarse a concursos de forma más eficaz.



PROTEGER EL VALOR DE LA ORGANIZACIÓN

Un SGCN ayuda a mitigar el impacto negativo de un acontecimiento perturbador. En la práctica, esto puede ahorrar a la organización importantes cantidades de dinero, tiempo e impacto en su reputación.



TRANQUILIDAD

El futuro es incierto. Un SGCN implantado eficazmente da confianza a una organización para seguir adelante sabiendo que puede gestionar una interrupción. Esta tranquilidad se extiende a toda la organización, desde los equipos de operaciones de personal hasta los miembros del consejo de administración.



MEJORAR LA CIBERSEGURIDAD Y LA RESISTENCIA ANTE FALLOS

La ciberseguridad y la planificación de en la agenda de muchas organizaciones. Un plan de continuidad de negocio ayuda a una empresa a gestionar el impacto de la interrupción de TI. Puede deberse a una acción malintencionada o a un fallo de la infraestructura. Los criptovirus, los ataques DDoS y los fallos de los centros de datos pueden crear trastornos profundos y duraderos en todas las funciones de una organización.

Las certificaciones de ciberseguridad como ISO 27001 no abordan plenamente los retos de continuidad en caso de interrupción. La ISO 27001 intenta abordar la continuidad dentro de la propia función de TI, pero no se extiende al resto de la organización. La ISO 22301 proporciona un marco para abordar el impacto organizativo más amplio de un fallo de TI. Como resultado, un Sistema de Gestión de Continuidad de Negocio (ISO 22301) está bien adaptado para integrarse con un sistema de gestión de la seguridad de la información ISO 27001.

Vista de alto nivel

Un sistema de gestión de la continuidad de las actividades se basa en principios similares a los de otros sistemas de gestión. El sistema se basa en el modelo Planificar-Hacer-Verificar-Actuar.

• Determinar las necesidades de la organización y comprender la justificación de los planes de continuidad de la actividad:

- Qué es importante continuar en caso de interrupción
- ¿Por qué es importante y para quién?
- ¿Qué nivel de perturbación están dispuestos a aceptar la organización y sus partes interesadas?

• Establecer un marco para mitigar las perturbaciones. Esto puede incluir:

- Procesos
- Capacidades
- Estructuras de respuesta

• Comprobar el rendimiento y la eficacia del sistema mediante la supervisión. En la práctica, esto implicará probar los planes de BC por diversos medios.

• Mejorar el sistema sobre la base de las medidas establecidas, revisar la justificación de los planes de continuidad de la actividad y su adecuación a lo que se ha implantado.

Uno de los retos prácticos de los SGCN es que entran en acción con poca frecuencia. Mientras que los sistemas de gestión de la calidad se implantan en el funcionamiento cotidiano de la empresa, los sistemas de continuidad de la actividad sólo entran plenamente en acción cuando se produce una interrupción. Esto significa que hay que hacer más hincapié en:

- Pruebas o simulacros del plan de continuidad de las actividades (PCN)
- Mantener y actualizar las capacidades organizativas para apoyar la continuidad de las actividades
- Revisiones periódicas del sistema, sus procesos y su justificación para garantizar que sigue estando en consonancia con una organización cambiante.



PRINCIPIOS CLAVE DE LA CONTINUIDAD DE NEGOCIO

La continuidad de la actividad se basa en una serie de principios clave que deben aplicarse sistemáticamente a un sistema de continuidad de la actividad para que sea eficaz.



Responsabilidad

La alta dirección y el consejo de administración de una organización son responsables de la continuidad de la actividad, y esta responsabilidad debe ser comprendida y aceptada. La gestión de la continuidad de la actividad debe ser un componente integral de la gestión global de riesgos. En caso de interrupción, la ausencia de responsabilidades, autoridades y funciones claramente definidas puede hacer ineficaz un plan de continuidad de la actividad.



Objetivos claros

Una organización debe contar con objetivos claros de continuidad de negocio que reflejen la naturaleza de sus actividades y su impacto en las partes interesadas. De este modo se facilita el establecimiento de prioridades y la asignación de recursos al proceso de continuidad de la actividad. Estos objetivos deben definir claramente los niveles de continuidad previstos y los tiempos de continuidad.



Evaluación de impacto y riesgo

La norma de continuidad de la actividad se diferencia de otras en que se centra en el "qué pasaría si". La capacidad de identificar y planificar posibles impactos y riesgos para la empresa es clave para un sistema eficaz de continuidad de la actividad.



Comunicación

Las organizaciones deben incluir en sus planes de continuidad de la actividad cómo y cuándo se comunicarán dentro de sus organizaciones, con los clientes y con las partes interesadas (como reguladores o proveedores).



Pruebas

El sistema de gestión de la continuidad de las actividades debe probarse periódicamente para evaluar su eficacia e introducir los cambios necesarios.

CICLO PDCA

La norma ISO 22031 se basa en el ciclo Planificar-Hacer-Verificar-Actuar (PDCA), también conocido como la rueda de Deming o el ciclo de Shewhart. El ciclo PDCA puede aplicarse no sólo al sistema de gestión en su conjunto, sino también a cada elemento individual, con el fin de centrarse en la mejora continua. En resumen:

Planificar:

Comprender el contexto externo y las necesidades de las partes interesadas. Identificar riesgos y oportunidades. Establecer los objetivos y los recursos necesarios.

Hacer:

Aplicar lo planificado. Desde un nuevo Sistema de Gestión de la Continuidad de Negocio hasta pequeños cambios en los procesos.

Verificar:

Supervisar y medir la eficacia de la continuidad de la actividad. Poner a prueba los planes de continuidad de la actividad y controlar los resultados.

Actuar:

Tomar medidas cuando sea necesario basándose en el seguimiento, la medición y otros factores que impulsen la acción.

Modelo PDCA ISO 22301



Planificar-Hacer-Verificar-Actuar es un ejemplo de sistema de bucle cerrado. Esto garantiza que el aprendizaje de las fases de "hacer" y "comprobar" se utiliza para informar las fases de "actuar" y "planificar" posteriores. En teoría, se trata de un sistema cíclico, pero es más bien una espiral ascendente, ya que el aprendizaje te hace avanzar cada vez que pasas por el proceso.

PENSAMIENTO BASADO EN EL RIESGO/AUDITORÍAS

Las auditorías son un enfoque sistemático, basado en pruebas y en procesos, para evaluar su Sistema de Gestión de la Continuidad de Negocio. Se realizan interna y externamente para verificar la eficacia del SGCN. Las auditorías son un ejemplo brillante de cómo se adopta el pensamiento basado en el riesgo dentro de la Gestión de la Continuidad del Negocio.

Auditorías de 1ª Parte: Auditorías internas

Las auditorías internas son una gran oportunidad para aprender dentro de su organización. Proporcionan tiempo para centrarse en un proceso o departamento concreto con el fin de evaluar realmente su rendimiento. El objetivo de una auditoría interna es garantizar el cumplimiento de las políticas, los procedimientos y los procesos determinados por usted, la organización, y confirmar la conformidad con los requisitos de la norma ISO 22301.

Planificación de auditorías

Elaborar un calendario de auditorías puede parecer un ejercicio complicado. Dependiendo de la escala y complejidad de sus operaciones, puede programar auditorías internas desde cada mes hasta una vez al año. Encontrará más información al respecto en la sección 9: evaluación del rendimiento.

Pensamiento basado en el riesgo

La mejor manera de considerar la frecuencia de las auditorías es examinar los riesgos que entraña el proceso o área de negocio que se va a auditar. Cualquier proceso de alto riesgo, ya sea porque tiene un alto potencial de salir mal o porque las consecuencias serían graves si saliera mal, debe auditarse con más frecuencia que un proceso de bajo riesgo.

La forma de evaluar los riesgos depende exclusivamente de usted. La norma ISO 22301 no dicta ningún método concreto de evaluación o gestión de riesgos.

2ª Parte - Auditorías externas

Las auditorías de segunda parte suelen llevarlas a cabo los clientes o terceros en su nombre, o usted puede realizarlas a sus proveedores externos. Las auditorías de segunda parte también pueden realizarlas los reguladores o cualquier otra parte externa que tenga un interés formal en una organización.

Puede que tenga poco control sobre el calendario y la frecuencia de estas auditorías, pero si establece su propio SGCN se asegurará de estar bien preparado para su llegada.

3ª Parte - Auditorías de certificación

Las auditorías de terceros corren a cargo de organismos externos, normalmente organismos de certificación acreditados por UKAS, como NQA. El organismo de certificación evaluará la conformidad con la norma ISO 22301:2019. Para ello, un representante del organismo de certificación visitará la organización y evaluará el sistema pertinente y sus procesos. El mantenimiento de la certificación también implica reevaluaciones periódicas.

La certificación demuestra a los clientes su compromiso con la calidad.

LA CERTIFICACIÓN ASEGURA:

- Evaluación periódica para supervisar y mejorar continuamente los procesos.
- Credibilidad de que el sistema puede lograr los resultados previstos
- Reducción del riesgo y la incertidumbre y aumento de las oportunidades de mercado
- Coherencia en los resultados diseñados para satisfacer las expectativas de las partes interesadas.

PENSAMIENTO BASADO EN PROCESOS/AUDITORÍAS

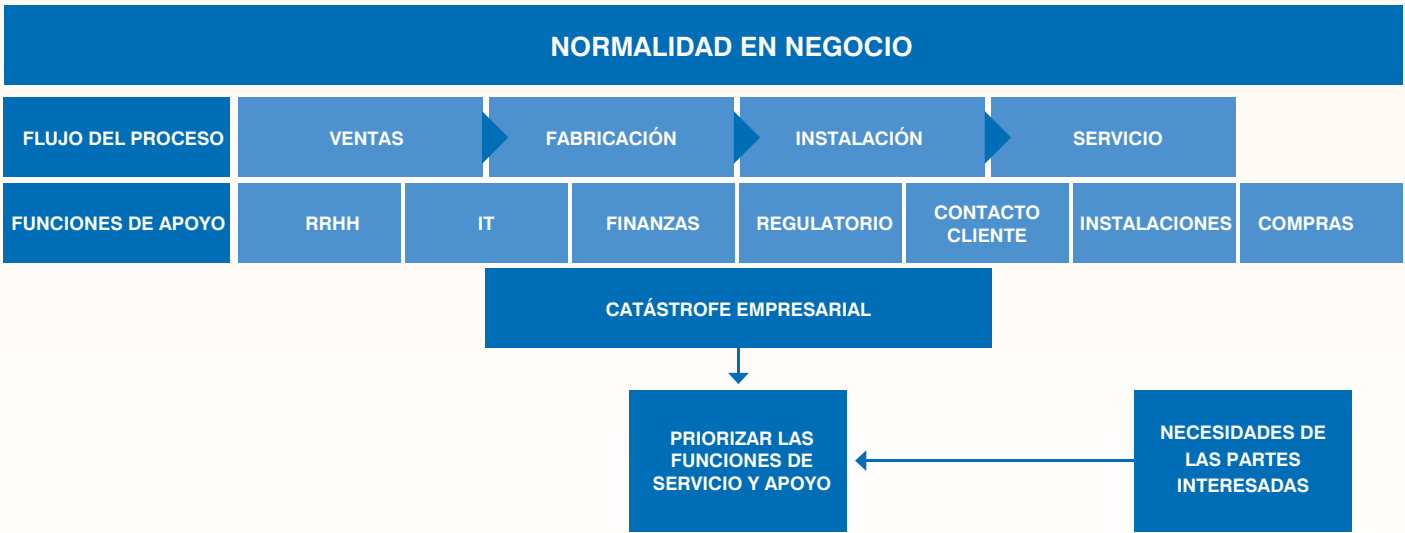
Un proceso es la transformación de entradas en salidas, que tiene lugar como una serie de pasos o actividades que dan lugar al objetivo u objetivos previstos. A menudo, la salida de un proceso se convierte en una entrada para otro proceso posterior. Muy pocos procesos funcionan de forma aislada.

El pensamiento basado en procesos es fundamental para la planificación de la continuidad de las actividades. Para alcanzar los objetivos de continuidad de la actividad, una organización tiene que crear planes de continuidad de la actividad basados en procesos. Abarcan múltiples procesos y funciones organizativas.

En la práctica, esto significa que un sistema de continuidad de la actividad debe considerar el proceso de principio a fin a través de la organización e incorporar las funciones de apoyo pertinentes para alcanzar sus objetivos.

Un sistema de continuidad de la actividad aplicable sólo a un departamento no tiene probabilidades de alcanzar objetivos de continuidad válidos.

El siguiente diagrama ilustra cómo una organización podría considerar la priorización de sus objetivos de continuidad de negocio a través de su estrategia de continuidad de negocio. En el ejemplo siguiente, una organización que suministra equipos sanitarios críticos prioriza su actividad de mantenimiento y sus funciones de apoyo clave tras un acontecimiento perturbador importante.

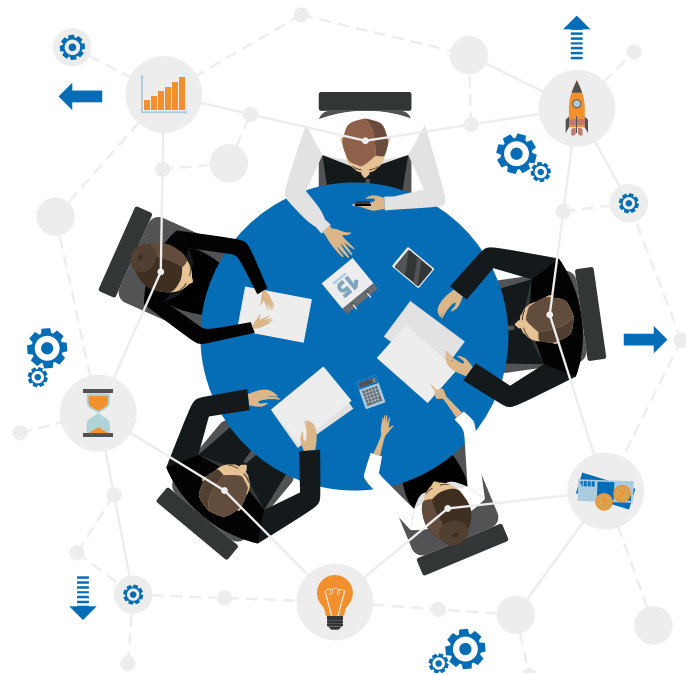


ANEXO SL

Uno de los principales cambios introducidos en la revisión de 2019 de la norma ISO 22301 fue la adopción del Anexo SL para la estructura de las cláusulas de la norma revisada. El Anexo SL (anteriormente conocido como Guía ISO 83) fue utilizado dentro de ISO por los redactores de normas para proporcionar una estructura básica común para las normas de sistemas de gestión.

ISO 22301 (Sistemas de Gestión de Continuidad de Negocio) adoptó esta estructura durante su revisión de 2019. La ISO 27001 (Norma de Sistemas de Gestión de la Seguridad de la Información) también adoptó esta estructura durante su revisión de 2013, así como la ISO 14001 (Norma de Sistemas de Gestión Medioambiental), que adoptó esta estructura durante su revisión de 2015. La recién publicada ISO 45001 (Norma de Sistemas de Gestión de Seguridad y Salud) también sigue esta misma estructura común.

Antes de la adopción del anexo SL había muchas diferencias entre las estructuras de las cláusulas, los requisitos y los términos y definiciones utilizados en las distintas normas de sistemas de gestión. Esto dificultaba a las organizaciones la integración de la aplicación y gestión de varias normas, entre las que se encontraban las más comunes sobre medio ambiente, calidad, salud y seguridad y seguridad de la información.



Estructura de alto nivel

El anexo SL consta de 10 cláusulas:

1. Alcance
2. Referencias normativas
3. Términos y definiciones
4. Contexto de la Organización
5. Liderazgo
6. Planificación
7. Ayuda
8. Operación
9. Evaluación del rendimiento
10. Mejora

De estas cláusulas, los términos comunes y las definiciones básicas no pueden modificarse. Los requisitos no pueden suprimirse ni modificarse, pero sí pueden añadirse requisitos y recomendaciones específicos de una disciplina.

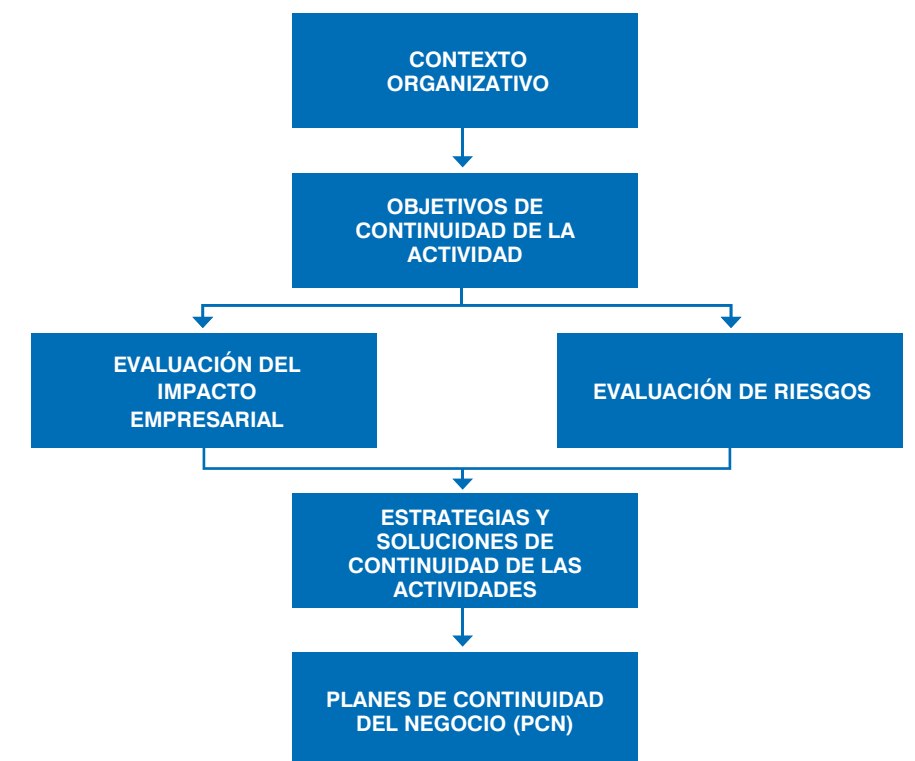
Todos los sistemas de gestión requieren tener en cuenta el contexto de la organización (más información al respecto en la sección 4); un conjunto de objetivos pertinentes para la disciplina, en este caso la calidad, y alineados con la dirección estratégica de la organización; una política documentada que respalde el sistema de gestión y sus objetivos; auditorías internas y revisión por la dirección. Cuando existen varios sistemas de gestión, muchos de estos elementos pueden combinarse para abordar más de una norma.

10 CLÁUSULAS DE ISO 22301:2019

La norma ISO 22301 consta de 10 secciones, denominadas cláusulas.

Al igual que con la mayoría de las demás normas ISO de sistemas de gestión, los requisitos de la norma ISO 22301 que deben cumplirse se especifican en las cláusulas 4.0 - 10.0. Al igual que en la norma ISO 27001, la organización debe cumplir todos los requisitos de las cláusulas 4.0 a 10.0; no puede declarar que una o varias cláusulas no le son aplicables.

El diagrama de la derecha ofrece un flujo ilustrativo de los conceptos de la norma:



CLÁUSULA 1: ALCANCE

La sección de alcance de la norma ISO 22301 establece:

- La finalidad de la norma
- El tipo de organizaciones a las que se aplica
- Las secciones de la norma (denominadas cláusulas) que contienen los requisitos que debe cumplir una organización para que se certifique su "conformidad" con la norma (es decir, que es conforme).

La norma ISO 22301 está diseñada para ser aplicable a cualquier tipo de organización. Independientemente de su tamaño, complejidad, sector industrial, propósito o madurez, cualquier organización puede implantar y mantener un SGCN que cumpla con la norma ISO 22301.

CLÁUSULA 2: REFERENCIAS NORMATIVAS

En las normas ISO, la sección de referencias normativas enumera cualquier otra norma que contenga información adicional relevante para determinar si una organización cumple o no la norma en cuestión. En ISO 22301 sólo se enumera un documento - ISO 22300, Seguridad y resiliencia - Vocabulario.

Algunos de los términos utilizados o de los requisitos detallados en la norma ISO 22301 se explican con más detalle en la norma ISO 22300. La referencia a la norma ISO 22300 resulta muy útil para comprender mejor un requisito o identificar la mejor forma de cumplirlo.

CONSEJO - Los auditores externos esperarán que haya tenido en cuenta la información contenida en la norma ISO 22300 en el desarrollo e implantación de su SGCN.



CLÁUSULA 3: TÉRMINOS Y DEFINICIONES

En la norma ISO 22301 se recogen 31 términos y definiciones y se hace referencia a la versión más actual de la norma ISO 22300 Security and Resilience -Vocabulary. La versión actual de este documento contiene 277 definiciones de términos que se utilizan en la norma ISO 22301.

Además de los términos explicados en la sección "Principios clave y terminología", los términos más importantes de ISO 22301 son:

Continuidad de negocio

- Capacidad de una organización para continuar con la entrega de productos o servicios a niveles predefinidos aceptables tras una interrupción.

Gestión de la continuidad de negocio

- Proceso holístico de gestión que identifica las amenazas potenciales para una organización y el impacto que esas amenazas, de materializarse, pueden causar en las operaciones empresariales, y proporciona un marco para crear resiliencia organizativa con capacidad de respuesta eficaz que salvaguarde los intereses de las principales partes interesadas, la reputación, la marca y las actividades.

Plan de continuidad de negocio

- Procedimientos documentados que guían a una organización para responder, recuperarse, reanudar y restablecerse a un nivel de funcionamiento tras una interrupción.

Análisis del impacto empresarial

- Proceso de análisis de las actividades y del efecto que puede tener en ellas una perturbación de la actividad.

Equipo de gestión de crisis

- Grupo de funcionalidad individual responsable de dirigir el desarrollo y la ejecución del plan de respuesta y continuidad operativa, declarar y la interrupción operativa o situación de crisis de emergencia, y proporcionar dirección durante el proceso de recuperación, tanto antes como después del incidente perturbador.

Disrupción

- Acontecimiento, ya sea previsto (por ejemplo, una huelga laboral o un huracán) o imprevisto (por ejemplo, un apagón o un terremoto), que causa una desviación negativa no planificada de la entrega prevista de productos o servicios de acuerdo con los objetivos de una organización.

Invocación

- Acto por el que se declara la necesidad de aplicar medidas de continuidad de la actividad de una organización para seguir suministrando productos o servicios clave.

Periodo máximo de interrupción tolerable (PMPT)

- Tiempo que tardaría en ser inaceptable el impacto adverso que puede surgir como consecuencia de no suministrar un producto/servicio o no realizar una actividad.

Objetivo Mínimo de Continuidad de Negocio (MBCO)

- Nivel mínimo de servicios y/o productos que una organización considera aceptable para alcanzar sus objetivos empresariales durante una interrupción.

Objetivo de Punto de Recuperación

- Punto hasta el que se restablece la información utilizada por una actividad para que ésta pueda funcionar al reanudarse.

Objetivo de tiempo de recuperación

- Periodo de tiempo tras un incidente en el que se reanuda un producto o servicio o una actividad o se recuperan los recursos.

Cuando redacte la documentación de su Sistema de Gestión de la Continuidad de Negocio, no tiene por qué utilizar estos términos exactos. Sin embargo, puede ayudar a aclarar el significado y la intención si puede definir los términos que ha utilizado. Puede ser útil incluir un glosario en la documentación del sistema.

CLÁUSULA 4: CONTEXTO DE LA ORGANIZACIÓN

El objetivo de un SGCN es permitir que una organización responda eficazmente a un incidente perturbador y continúe suministrando productos y servicios clave a un nivel predefinido, hasta la reanudación de las operaciones normales.

Contexto interno

Los siguientes son ejemplos de las áreas que deben tenerse en cuenta a la hora de evaluar las cuestiones internas que pueden influir en el SGCN:

- **Madurez:** ¿es usted una start-up ágil con un lienzo sobre el que trabajar, o una institución de más de 30 años con procesos y planes de contingencia bien establecidos?
- **Cultura organizativa:** ¿es su organización relajada en cuanto a cómo, cuándo y dónde trabaja la gente, o extremadamente reglamentada?
- **Dependencias:** ¿cuáles son las dependencias internas que necesita para responder eficazmente al incidente perturbador (servicios informáticos, energía, equipos)?
- **Gestión:** ¿existen canales y procesos de comunicación claros desde los principales responsables de la toma de decisiones hasta el resto de la organización?
- **Tamaño de los recursos:** ¿trabaja con una cantidad limitada de recursos, personal y equipos?
- **Madurez de los recursos:** ¿los recursos disponibles están informados, plenamente formados, son fiables, o el personal carece de experiencia y cambia constantemente?
- **Coherencia:** ¿tiene procesos uniformes en toda la organización, o una multitud de prácticas operativas diferentes con poca coherencia?
- **Equipamiento:** necesita equipamiento especializado.

Contexto exterior

Los siguientes son ejemplos de las áreas que pueden tenerse en cuenta a la hora de evaluar las cuestiones externas que pueden influir en el SGCN:

- **Propietario:** ¿necesita autorización para mejorar la seguridad física?
- **Proveedores:** ¿son capaces sus proveedores de suministrarle a tiempo?

- **Organismos reguladores:** ¿existen requisitos reglamentarios o legales que deba tener en cuenta a la hora de desarrollar su SGCN? ¿Necesita informarles de que ha recurrido a su PCN?
- **Económico/político:** ¿las fluctuaciones monetarias afectan a su organización?
- **Dependencias:** ¿cuáles son las dependencias externas que necesita para responder eficazmente al incidente perturbador (servicios informáticos, suministros, energía, equipos)?
- **Consideraciones medioambientales:** ¿hay algún problema medioambiental que pueda afectar a su SGCN?
- **Clientes:** ¿qué impacto tendrá la invocación de su SGCN en sus clientes? ¿Necesita informarles de que ha invocado su PCN?
- **Accionistas:** ¿están preocupados por la capacidad de su organización para responder a un incidente perturbador?

Partes interesadas

Una parte interesada es cualquier persona que pueda verse afectada por la invocación de su PCN. Las partes interesadas se irán aclarando a lo largo del proceso de análisis exhaustivo de los problemas internos y externos. Es probable que incluya a accionistas, propietarios, reguladores, clientes, empleados, proveedores y puede extenderse al público en general y al medio ambiente, dependiendo de la naturaleza de su negocio. No tiene por qué intentar comprender o satisfacer todas sus necesidades, pero sí determinar cuáles de sus necesidades y expectativas son relevantes para su SGCN.

Legal y reglamentario

Identifique y manténgase al día de cualquier requisito legal y reglamentario relacionado con la continuidad de sus productos y servicios, actividades y recursos al implantar y mantener su SGCN.

- **Documentación:** documente sus requisitos legales, reglamentarios y de otro tipo, así como su planteamiento para cumplirlos.

Alcance del sistema de gestión

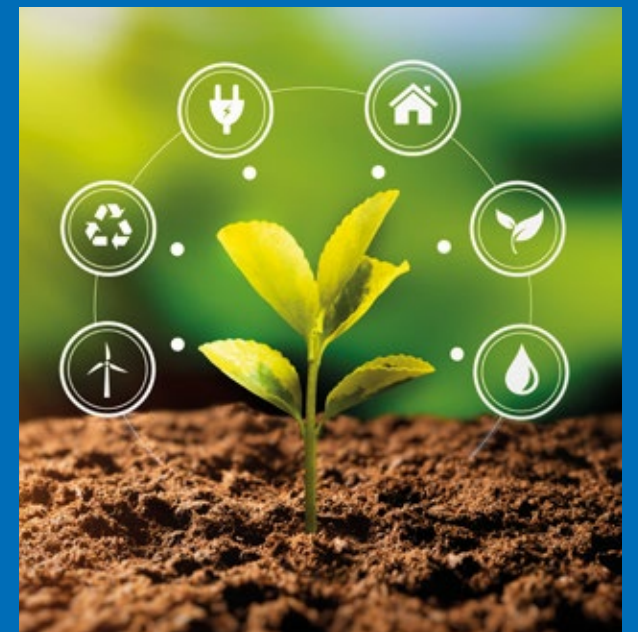
Para cumplir la norma ISO 22301, debe documentar el alcance de su SGCN. Los alcances documentados suelen describir:

- Los límites del lugar o lugares físicos incluidos (o no incluidos)
- Los grupos de empleados internos y externos incluidos (o no incluidos)
- Los procesos, actividades, productos o servicios internos y externos incluidos (o no incluidos)
- Interfaces clave en los límites del ámbito de aplicación.

Si quiere priorizar recursos creando un SGCN que no cubra toda su organización o sus actividades, seleccionar un ámbito limitado a la gestión de los intereses de las partes interesadas clave es un enfoque pragmático. Para ello, puede incluir únicamente centros, activos, procesos, productos o departamentos específicos.

CONSEJO - Documente la información recopilada en el análisis del contexto de su organización y de las partes interesadas, como:

- Conversaciones con un alto representante de la organización.
- Actas de reuniones o planes de empresa.
- Un documento específico que identifica los problemas internos/externos y las partes interesadas, así como sus necesidades y expectativas; por ejemplo, un análisis DAFO, un estudio PESTLE o una evaluación de riesgos empresariales de alto nivel.



Nueva consideración para el cambio climático

ISO ha introducido cambios en la norma ISO 22301 para subrayar la importancia de abordar los efectos del cambio climático en el marco de los sistemas de gestión de las organizaciones.

Para mejorar la concienciación y la respuesta de las organizaciones al cambio climático, ISO ha introducido dos cambios fundamentales en la cláusula 4:

Cláusula original 4.1:

"Comprensión de la organización y su contexto. La organización debe determinar las cuestiones externas e internas que son relevantes para su propósito y que afectan a su capacidad para lograr el resultado o resultados previstos de su sistema de gestión de XXX."

Esta cláusula incluye ahora explícitamente la afirmación "La organización determinará si el cambio climático es una cuestión relevante".

Cláusula original 4.2:

"Comprender las necesidades y expectativas de las partes interesadas. La organización debe determinar:

- Las partes interesadas que son relevantes para el sistema de gestión XXX.
- Los requisitos pertinentes de estas partes interesadas.
- Cuáles de estos requisitos se abordarán a través del sistema de gestión XXX".

La cláusula ahora también dice: "Nota: Las partes interesadas pertinentes pueden tener requisitos relacionados con el cambio climático".

CLÁUSULA 5: LIDERAZGO

Compromiso de liderazgo

En este contexto, liderazgo significa participación activa en el establecimiento de la dirección del SGCN, promoviendo su aplicación, destacando su importancia y garantizando la disponibilidad de los recursos adecuados.

- Garantizar que la política y los objetivos de continuidad de la actividad se establecen y se alinean con la dirección estratégica de la organización.
- Garantizar la integración de los requisitos del SGCN en las prácticas empresariales de la organización.
- Garantizar que el BCMS cuenta con los recursos adecuados.
- Comunicar la importancia de la continuidad de las actividades y de cumplir los requisitos del SGCN.

- Garantizar que el BCMS logre los resultados previstos.
- Dirigir y apoyar a las personas para que contribuyan a la eficacia del SGCN.
- Promover la mejora continua.
- Apoyar otras funciones directivas para demostrar su liderazgo y compromiso.

La norma ISO 22301 concede gran importancia al compromiso activo de la alta dirección en el SGCN, partiendo de la base de que el compromiso de la alta dirección es crucial para garantizar la implantación efectiva, el mantenimiento y la mejora continua de un SGCN eficaz por parte del grupo más amplio de empleados.

Política: continuidad de negocio

Una responsabilidad vital de la dirección es establecer y documentar una Política de Continuidad de Negocio que esté alineada con la dirección estratégica de la organización. Los requisitos del SGCN deben integrarse en los procesos empresariales y contar con los recursos adecuados.

La política deberá:

- Ser apropiada para el propósito de la organización.
- Proporcionar un marco para establecer objetivos al SGCN.
- Incluir el compromiso de cumplir los requisitos aplicables
- Incluir un compromiso de mejora continua del SGCN.
- Ser comunicada con la organización.
- Estar a disposición de las partes interesadas.

La Política de Continuidad de Negocio puede referirse a, o incluir subpolíticas que cubran, procesos y actividades clave que son importantes para la provisión continuada de productos y servicios clave en caso de un incidente perturbador y la recuperación de las operaciones. Para demostrar la importancia de la Política de Continuidad de Negocio, ésta debe ser autorizada por la Dirección.

CONSEJO - Para asegurarse de que su Política de Continuidad de Negocio está bien comunicada y a disposición de las partes interesadas, es una buena idea:

- Incluirlo en los paquetes de iniciación y en las presentaciones para nuevos empleados y contratistas.
- Colocar la declaración clave en los tableros de anuncios internos, las intranets y el sitio web de su organización
- Hacer de su cumplimiento y/o apoyo un requisito contractual para empleados, contratistas y proveedores críticos.

Funciones y responsabilidades

Se establecerán, asignarán y comunicarán dentro de la organización las funciones y responsabilidades en materia de continuidad de las actividades.

Se asignarán responsabilidades para:

- Garantizar que el SGCN se ajusta a los requisitos de la norma.
- Informar sobre el funcionamiento del SGCN a la alta dirección.

Para que la continuidad de la actividad forme parte de las actividades cotidianas, es necesario definir, comprender y comunicar las responsabilidades y obligaciones de todo el personal en materia de continuidad de la actividad.

Evidenciar el liderazgo ante un auditor

La alta dirección es el grupo de personas que establecen la dirección estratégica de una organización y aprueban la asignación de recursos a la organización o área de negocio dentro del ámbito de su SGCN. Dependiendo del tamaño y de cómo esté estructurada su organización, estas personas pueden ser o no el equipo de gestión diaria.

Un auditor suele comprobar el compromiso de liderazgo entrevistando a uno o más miembros de la alta dirección y evaluando su nivel de implicación y participación en la empresa:

- Evaluación de riesgos y oportunidades
- Establecimiento y comunicación de políticas
- Fijación y comunicación de objetivos
- Revisión y comunicación del rendimiento del sistema
- Asignación de recursos, responsabilidades y obligaciones adecuadas.

CONSEJO - Antes de su auditoría externa, identifique quién de su alta dirección se reunirá con el auditor externo y prepárele para la entrevista con un repaso de las preguntas que probablemente le harán.

CLÁUSULA 6: PLANIFICACIÓN

Al planificar su SGCN, una organización debe tener en cuenta los riesgos y oportunidades identificados al determinar el contexto de la organización y el alcance del SGCN. La organización debe determinar qué riesgos y oportunidades deben abordarse para:

- Garantizar que el SGCN pueda alcanzar los resultados previstos.
- Prevenir o reducir los efectos no deseados.
- Lograr la mejora continua.

Gestionar riesgos y oportunidades

Una organización debe establecer una metodología para evaluar los riesgos y oportunidades que afectan a la capacidad del SGCN para lograr los resultados previstos y determinar las acciones necesarias para abordar el riesgo y las oportunidades.

Una organización deberá:

- Determinar medidas para hacer frente a los riesgos y oportunidades.
- Aplicar las medidas identificadas.
- Evaluar la eficacia de estas acciones.

Objetivos de continuidad de negocio (y planificación para alcanzarlos)

Los objetos de continuidad de negocio deben establecerse en las funciones y niveles pertinentes dentro de una organización; los objetivos pueden ser a nivel organizativo o departamental.

Los objetivos deben ser:

- Acordes con la política de continuidad de las actividades.
- Ser mensurables.
- Tener en cuenta los requisitos aplicables.
- Comunicados.
- Supervisados y actualizados según proceda.

Los objetivos deben comunicarse a las personas pertinentes de la organización; deben supervisarse y actualizarse según sea necesario.

Alcanzar los objetivos

Una organización debe establecer un plan para alcanzar sus objetivos; el plan debe tener en cuenta:

- Lo que hay que hacer
- Los recursos necesarios
- Quién es responsable
- La fecha de finalización; y
- Cómo evaluar los resultados.

Cambios en el SGCN

Es probable que con el tiempo los procesos, actividades, productos y servicios de una organización cambien. Como resultado, tendrá que hacer cambios en su SGCN, los cambios deben llevarse a cabo de una manera planificada y deben tener en cuenta:

- El objetivo del cambio y sus posibles consecuencias.
- La integridad del SGCN.
- Disponibilidad de recursos
- Reasignación de responsabilidades y autoridades.



CLÁUSULA 7: SOPORTE

La cláusula 7 se refiere a los recursos. Se refiere tanto a las personas, la infraestructura y el entorno como a los recursos físicos, materiales, herramientas, etc. También se presta una atención renovada al conocimiento como recurso importante dentro de su organización. A la hora de planificar sus objetivos de continuidad de la actividad, una consideración importante será la capacidad actual de sus recursos, así como los que pueda necesitar de proveedores o socios externos.

Recursos

Para implantar y mantener un SGCN eficaz, una organización debe identificar y proporcionar los recursos de apoyo necesarios para su funcionamiento, mantenimiento y mejora continua.

Los recursos tienen que ser:

- Capaces - si el recurso es equipo o infraestructura; y
- competentes - si son personas; y
- Suficientes - si son suministros.

Competencia

La implantación de un Sistema de Gestión de la Continuidad de Negocio eficaz depende de los conocimientos y capacidades de sus empleados, proveedores y contratistas. Para tener la certeza de contar con una base adecuada de conocimientos y competencias, es necesario:

- Definir los conocimientos y competencias necesarios.
- Determinar quién debe poseer los conocimientos y competencias necesarios.
- Verificar que las personas adecuadas tienen los conocimientos y las competencias adecuadas.

Su auditor esperará que disponga de documentos que detallen sus requisitos en materia de conocimientos y competencias. Cuando considere que se cumplen los requisitos, deberá demostrarlo con documentos como certificados de formación, registros de asistencia a cursos o evaluaciones internas de competencias.

CONSEJO - La mayoría de las organizaciones que ya utilizan herramientas como matrices de formación/habilidades, evaluaciones o valoraciones de proveedores pueden satisfacer el requisito de registros de competencias ampliando las áreas cubiertas para incluir la Continuidad de Negocio.

Concienciación

Además de garantizar la competencia específica del personal en continuidad de negocio, los empleados, proveedores y contratistas deberá conocer los elementos básicos de su SGCN. Esto es fundamental para establecer una cultura de apoyo dentro de la organización.

Todo el personal, proveedores y contratistas deben ser conscientes de lo siguiente:

- Que tiene un SGCN y por qué lo tiene.
- Que dispone de una Política de Continuidad y qué elementos concretos de la misma son relevantes para ellos.
- Cómo pueden contribuir a que su organización responda a una situación adversa y mantenga la continuidad de los productos o servicios en un nivel predefinido.
- Qué políticas y procedimientos les afectan y qué consecuencias tiene su incumplimiento.

SUGERENCIA - La comunicación de esta información puede realizarse a través de los procesos y documentos existentes, como los cursos de iniciación, los contratos de trabajo, las charlas sobre herramientas, los acuerdos con proveedores, las reuniones informativas para empleados y actualizaciones.

Comunicación

Para que su SGCN funcionen eficazmente, deberá asegurarse de que la omunicación están bien gestionada:

Una organización deberá establecer:

- Lo que hay que comunicar.
- Cuándo debe comunicarse.
- A quién debe comunicarse.
- Cuáles son los procesos de comunicación.
- Responsable de la comunicación.

CONSEJO - Si sus requisitos de comunicación están bien definidos en sus procesos, políticas y procedimientos, no necesita hacer nada más para cumplir este requisito. Si no lo están, debería considerar la posibilidad de documentar sus actividades de comunicación clave en forma de tabla o procedimiento que incluya los epígrafes detallados anteriormente. Recuerde que el contenido de estos documentos también debe comunicarse.



Información documentada

Para que sea útil, la información documentada que utilice para implantar, mantener y mejorar su SGCN tiene que:

- ser preciso
- ser clara, inequívoca y comprensible para las personas que la utilizan habitual u ocasionalmente
- Apoyar el cumplimiento de los requisitos legales y gestionar los riesgos y problemas internos y externos que afectan a la capacidad del SGCN para alcanzar los resultados previstos.

Para que su información documentada cumpla estos requisitos, deberá disponer de procesos que garanticen que:

- la información documentada sea revisada por las personas adecuadas antes de su difusión general.
- la información documentada está disponible cuando se necesita y es adecuada para su uso.
- el acceso a la información documentada se controla para que no pueda modificarse, corromperse, borrarse o ser consultada por personas a las que no corresponda.
- iLa información se elimine de forma segura o se devuelva a su propietario cuando sea necesario.
- Puede realizar un seguimiento de los cambios en la información para garantizar el control del proceso.

La fuente de la información documentada puede ser interna o externa, por lo que los procesos de control deben gestionar la información documentada de ambas fuentes.

CONSEJO - Las organizaciones que tienen un buen control de los documentos suelen contar con uno o más de los siguientes elementos:

- Una sola persona o un pequeño equipo responsable de garantizar que los documentos nuevos/modificados se revisan antes de su publicación, se almacenan en el lugar adecuado, se retiran de la circulación cuando son sustituidos y que se mantiene un registro de cambios.
- Un sistema de gestión electrónica de documentos que contiene flujos de trabajo y controles automáticos
- Sólidos procesos de copia de seguridad de datos electrónicos y de archivo/almacenamiento de archivos en papel.
- Gran conocimiento por parte de los empleados de los requisitos de control de documentos, mantenimiento de registros y acceso/conservación de la información.

CLÁUSULA 8: OPERACIÓN

Una vez completadas todas las actividades de planificación y evaluación de riesgos exigidas por la norma, pasamos a la fase de implantación y funcionamiento. Aquí es donde se implantan y controlan los procesos y acciones identificados para abordar los riesgos y oportunidades.

Para implantar procesos eficaces son cruciales las siguientes prácticas:

- 1 Los procesos se crean adaptando o formalizando las actividades habituales de una organización.
- 2 Identificación sistemática de los riesgos de continuidad de la actividad pertinentes para cada producto y servicio.
- 3 Definición y comunicación claras del conjunto de actividades necesarias para gestionar los riesgos asociados a la continuidad de la actividad.
- 4 Asignación clara de las responsabilidades para llevar a cabo las actividades relacionadas .
- 5 Asignación adecuada de recursos para garantizar que las actividades relacionadas puedan llevarse a cabo como y cuando sea necesario.
- 6 Evaluación rutinaria de la coherencia con la que se sigue cada proceso y su eficacia en la gestión de los riesgos de continuidad de la actividad.

CONSEJO - Para cada proceso, designe a una persona responsable de garantizar que se lleven a cabo los pasos 2 a 6. Esta persona suele denominarse propietario del proceso. A esta persona se la suele denominar propietario del proceso.

Análisis de impacto empresarial y evaluación de riesgos

Una organización debe implantar y mantener un proceso para analizar el impacto empresarial y evaluar el riesgo de interrupción de sus actividades clave. Los resultados del análisis del impacto empresarial y de las evaluaciones de riesgos permitirán a una organización determinar la estrategia y la solución adecuadas necesarias para responder a un incidente perturbador.

Análisis del impacto empresarial

El propósito de realizar un análisis de impacto en el negocio es permitir que una organización identifique sus requisitos y prioridades de continuidad del negocio. El proceso para llevar a cabo un análisis de impacto en el negocio deberá:

- Definir los tipos de impacto y los criterios pertinentes para el contexto de la organización
- Identificar y priorizar las actividades clave y los productos y servicios necesarios para llevarlas a cabo.
- Evaluar las repercusiones a lo largo del tiempo de la interrupción de las actividades.
- identify the point in time when the non-resumption of these activities would have a detrimental impact on the organization (MTPD)
- Identificar el momento en que se reanudarán estas actividades a un nivel aceptable (RTO)
- Determinar los recursos necesarios para las actividades.
- Determinar las dependencias internas y externas necesarias para apoyar las actividades prioritarias.

Evaluación de riesgos

El proceso de evaluación de riesgos permitirá a una organización determinar la probabilidad de que se produzca un incidente. A continuación, ayuda a identificar las acciones necesarias para reducir la probabilidad y el impacto en las actividades en caso de que se produzca un incidente perturbador. Las evaluaciones de riesgos deben realizarse a intervalos planificados o cuando se produzcan cambios significativos en la organización o en el contexto:

El proceso de evaluación de riesgos deberá:

- Identificar los riesgos para las actividades prioritarias de la organización y sus recursos necesarios.
- Analizar y evaluar el riesgo identificado.
- Determinar los riesgos que requieren tratamiento.

Estrategia y soluciones de continuidad de negocio

Los resultados del análisis del impacto en la actividad y de la evaluación de riesgos deben utilizarse para determinar la estrategia correcta de continuidad de la actividad e identificar los recursos necesarios para responder y gestionar el incidente de continuidad de la actividad hasta el retorno a la normalidad.

Selección de estrategias y soluciones:

La selección de la estrategia y las soluciones de continuidad de las actividades de una organización se basará en:

- La capacidad de cumplir los requisitos para continuar y recuperar las actividades prioritarias a una capacidad predeterminada y en un plazo acordado.
- rReducir la probabilidad y la duración de las perturbaciones.
- Recursos necesarios.
- La propensión al riesgo de la organización.
- Costes y beneficios.

Recursos necesarios

A la hora de determinar los recursos necesarios para la implantación del SGCN, la organización deberá tener en cuenta los recursos internos y externos necesarios.

Como mínimo, los recursos deben incluir:

- Personal
- Información y datos
- Infraestructuras y servicios de apoyo
- Equipos y consumibles
- Sistemas informáticos y de comunicación
- Transporte y logística
- Finanzas
- Socios y proveedores.

Planes y procedimientos de continuidad de negocio

Basándose en los resultados de las estrategias y soluciones de continuidad de negocio, una organización debe establecer una estructura de respuesta e implementar planes y procedimientos para gestionar la organización durante un incidente perturbador que requiera de sus soluciones de continuidad de negocio.

Los procedimientos deberán:

- identificar las medidas adoptadas durante una perturbación.
- Ser capaces de adaptarse a los cambios en las condiciones internas y externas como resultado de una perturbación.
- Centrarse en el impacto de los incidentes y perturbaciones.
- Minimizar el impacto de las perturbaciones
- Asignar funciones y responsabilidades para las tareas.

Estructura de respuesta

La estructura de respuesta constará de uno o varios equipos (equipo(s) de gestión de crisis) responsables de responder a y gestionar las perturbaciones. Las funciones y responsabilidades de cada equipo deben estar definidas, los equipos deben ser competentes para evaluar el impacto de la perturbación y aplicar la respuesta adecuada. La estructura de respuesta debe incluir procedimientos de comunicación con las partes interesadas, las autoridades y medios de comunicación.

Plan de continuidad de negocio

Se elaborarán y mantendrán planes y procedimientos documentados de continuidad de la actividad que proporcionen orientación e información para permitir a los equipos responder a un incidente perturbador y recuperar la normalidad de las operaciones. Los planes deberán estar fácilmente disponibles donde y cuando sea necesario.

Los planes de continuidad de la actividad contendrán:

- Detalles de las medidas que tomará cada equipo para continuar o recuperar las actividades prioritarias, supervisar el impacto de la perturbación y la respuesta de la organización.
- Referencia a los umbrales y procesos predefinidos para activar la respuesta
- Procedimientos para permitir la entrega de productos y servicios a una capacidad acordada
- Detalles para gestionar las consecuencias inmediatas de una perturbación teniendo en cuenta el bienestar de las personas, la prevención de nuevas perturbaciones en las actividades prioritarias y el impacto en el medio ambiente.

Cada plan deberá:

- Indicar la finalidad, el ámbito de aplicación y los objetivos
- Las funciones y responsabilidades del equipo que aplicará el plan
- Identificar acciones para aplicar las soluciones
- Contener la información necesaria para activar, operar, coordinar y comunicar las acciones del equipo
- Identificar las dependencias internas y externas necesarias
- Identificar los recursos necesarios
- Incluir requisitos de información
- Incluir un proceso de dimisión.

Recuperación

Una organización debe tener procesos documentados para volver a la normalidad tras un incidente de continuidad de negocio.

Programa de ejercicios

Para garantizar que sus estrategias, soluciones y planes de continuidad de la actividad siguen siendo válidos, una organización debe establecer un programa de ejercicios para comprobar la eficacia de sus medidas de continuidad . No es necesario que la organización compruebe todas las medidas de continuidad de las actividades en cada ejercicio.

Las pruebas son para:

- Ser coherente con sus objetivos de continuidad de la actividad.
- Basarse en escenarios apropiados con metas y objetivos claramente definidos.
- Desarrollar el trabajo en equipo y la competencia de los equipos de continuidad y de quienes tienen funciones que desempeñar durante una perturbación.
- Validar estrategias, soluciones y planes de continuidad.
- Elaborar informes posteriores al ejercicio que contengan resultados, recomendaciones y acciones de mejora.
- To realizarse a intervalos planificados o cuando se produzcan cambios significativos en la organización o en el contexto en el que opera.

Evaluación de la documentación y las capacidades en materia de continuidad de las actividades

Una organización debe evaluar la adecuación y eficacia de su análisis de impacto en el negocio, evaluación de riesgos, estrategias, soluciones, planes y procedimientos a intervalos planificados, después de un incidente o invocación y cuando se produzcan cambios significativos.



CLÁUSULA 9: EVALUACIÓN DEL RENDIMIENTO

Seguimiento, medición, análisis y evaluación

Una organización necesita evaluar el rendimiento y la eficacia de su SGCN para asegurarse de que puede lograr los resultados previstos. Para ello, debe determinar qué debe ser objeto de seguimiento y medición, los métodos de seguimiento y medición y cómo se evaluarán los resultados. El personal encargado de las actividades de seguimiento y medición debe ser identificado y seleccionado teniendo en cuenta su competencia e imparcialidad. Deben conservarse pruebas adecuadas de las actividades de seguimiento y medición y de los resultados de dichas actividades.

Auditoría interna

El objetivo de las auditorías internas es confirmar que el SGCN se ha implantado eficazmente e identificar cualquier debilidad y oportunidad de mejora.

Las auditorías internas deben comprobar:

- Si el SGCN satisface las necesidades de la organización.
- Cumple los requisitos de la norma ISO 22301:2019.
- La coherencia con que se aplican los procesos y procedimientos.
- Si los procesos y procedimientos logran los resultados previstos.

Programa de auditorías

Una organización debe realizar auditorías internas a intervalos planificados. El programa de auditoría deberá:

- Tener en cuenta la importancia de los procesos en cuestión y los resultados de auditorías anteriores.
- Definir los criterios y el alcance de cada auditoría.
- Seleccionar auditores y realizar auditorías para garantizar la objetividad e imparcialidad del proceso de auditoría.
- Garantizar que los resultados de las auditorías se comunican.
- Conservar pruebas documentales de la aplicación del programa de auditoría y de los resultados de las auditorías.
- Garantizar que se adopten sin demora las medidas correctoras para subsanar las no conformidades y sus causas.

Management Review

La alta dirección revisará el SGCN de la organización a intervalos planificados para evaluar si sigue siendo adecuado, apropiado y eficaz para satisfacer las necesidades de la organización.

Las entradas y salidas de las reuniones de revisión por la dirección deben cumplir los requisitos de la cláusula 9.3 de la norma. Los resultados incluirán decisiones relacionadas con las oportunidades de mejora continua y cualquier cambio necesario para mejorar la eficiencia y eficacia del SGCN.

Una organización debe conservar información documentada como prueba de los resultados de las revisiones por la dirección y comunicar los resultados a las partes interesadas pertinentes.



CLÁUSULA 10: MEJORA

El principal objetivo de la implantación de un SGCN es garantizar que una organización pueda responder a tiempo a un incidente perturbador y seguir suministrando sus productos y servicios clave a un nivel predefinido hasta que pueda volver a la normalidad.

No conformidad y acción correctiva

Las organizaciones deben determinar las oportunidades de mejora y aplicar medidas para lograr los resultados previstos de su SGCN. Las organizaciones deben reaccionar ante las no conformidades y tomar medidas para controlar y corregir las no conformidades y hacer frente a las consecuencias.

Análisis de las causas

Las organizaciones deben investigar las no conformidades para:

- Establecer si la disconformidad existe en otro lugar.
- Identificar la causa raíz de la no conformidad.
- Determinar las medidas correctoras necesarias para evitar que vuelva a producirse la no conformidad.
- Identificar los cambios necesarios en el SGCN.

Cualquier acción correctiva identificada para abordar las no conformidades debe aplicarse sin demoras indebidas. Las medidas correctivas aplicadas se revisarán para determinar su eficacia.

SAQUE EL MÁXIMO PARTIDO A SUS SISTEMAS DE GESTIÓN

Consejos para implantar con éxito un SGCN



1. "¿Por qué? Asegúrese de que las razones para implantar un SGCN son claras y están en consonancia con su dirección estratégica; de lo contrario, corre el riesgo de no obtener el apoyo fundamental de la alta dirección.



2. "¿Para qué? Implantar y mantener un SGCN requiere un compromiso significativo, así que asegúrese de que su alcance es lo suficientemente amplio como para cubrir la información crítica que necesita protección, pero no tan amplio que no disponga de recursos suficientes para implantarlo y mantenerlo.



3. Implicar a todas las partes interesadas. La dirección para establecer el contexto, los requisitos, la política y los objetivos; los directivos y empleados con valiosos conocimientos para la evaluación de riesgos, el diseño de procesos y la redacción de procedimientos.



4. Comuníquese ampliamente a lo largo del proceso con todas las partes interesadas. Hágales saber lo que está haciendo, por qué lo está haciendo, cómo piensa hacerlo y cuál será su participación. Actualice periódicamente los avances.



5. Obtenga ayuda externa cuando la necesite. No fracase por falta de conocimientos técnicos. La gestión de los riesgos requiere a menudo conocimientos especializados.



6. Los procesos y la documentación de apoyo deben ser sencillos. Puede ampliarse con el tiempo si es necesario.



7. Diseñar y aplicar normas en la práctica. No cometa el error de documentar una norma demasiado elaborada que nadie pueda cumplir. Es mejor aceptar un riesgo y seguir buscando formas de gestionarlo.



8. Recuerde a sus proveedores. Algunos proveedores le ayudarán a mejorar su SGCN, otros aumentarán su riesgo. Debe asegurarse de que los proveedores de alto riesgo aplican controles al menos tan buenos como los suyos. Si no es así, busque alternativas.



9. Llover, formarse y volver a formarse. Es probable que la Continuidad de Negocio sea un concepto nuevo para muchos o la mayoría de sus empleados. Es posible que tengan que cambiar hábitos arraigados durante muchos años. Es poco probable que baste con una sola sesión informativa de concienciación.



10. Recuerde que debe asignar recursos suficientes para poner a prueba sus controles de forma rutinaria. Las amenazas a las que se enfrenta su organización cambian constantemente y debe comprobar si es capaz de responder a ellas. a esas amenazas.

PASOS TRAS LA IMPLEMENTACIÓN

1 FORMACIÓN DE SENSIBILIZACIÓN

- Su organización debe concienciar sobre las distintas normas incluidas en el SGCN.
- Debe celebrar reuniones de formación separadas para la alta dirección, los mandos intermedios y los directivos de nivel inferior, lo que contribuirá a crear un entorno motivador, listo para la aplicación.

2 POLÍTICA Y OBJETIVOS

- Su organización debe desarrollar una Política Integrada de Calidad/Política Medioambiental/Política de Salud y Seguridad/Política de Seguridad de la Información y los objetivos pertinentes para ayudar a cumplir los requisitos.
- En colaboración con la alta dirección, la empresa debe organizar talleres con todos los niveles del personal directivo para perfilar los objetivos integrados.

3 ANÁLISIS INTERNO DE DEFICIENCIAS

- Su organización debe identificar y comparar el nivel de cumplimiento de los sistemas existentes con los requisitos de las normas de su nuevo SGCN.
- Todo el personal pertinente debe comprender las operaciones de la organización y elaborar un mapa de procesos para las actividades de la empresa.

4 DOCUMENTACIÓN/DISEÑO DE PROCESOS

- La organización debe crear documentación de los procesos de acuerdo con los requisitos de las normas pertinentes.
- Debe redactar y aplicar un manual, un cuaderno de procedimientos funcionales, instrucciones de trabajo, procedimientos del sistema y proporcionar los términos asociados.

5 DOCUMENTACIÓN / APLICACIÓN DE PROCESOS

- Los procesos y documentos elaborados en el paso 4 deben aplicarse en toda la organización, abarcando todos los departamentos y actividades.
- La organización debe organizar un taller sobre la aplicación de los requisitos de la norma ISO.

6 AUDITORÍA INTERNA

- Es esencial que la organización cuente con un sólido sistema de auditoría interna. Se recomienda la formación de auditores internos y NQA puede proporcionar formación de auditores internos para la(s) norma(s) que está implementando.
- Es importante aplicar medidas correctoras de mejora, en cada uno de los documentos auditados, para colmar las lagunas y garantizar la eficacia del SGCN.

7 ORGANIZAR UNA REUNIÓN DE REVISIÓN DEL "SISTEMA" DE GESTIÓN

- La dirección de alto nivel debe revisar varios aspectos oficiales de la organización, que son relevantes para las normas que se están implantando.
- Revisar la política, objetivos, resultados de la auditoría interna, resultados del rendimiento de los procesos, resultados de las quejas, resultados de la evaluación de riesgos/incidentes y desarrollar un plan de acción tras la reunión, del que debe levantarse acta.

8 ANÁLISIS EXHAUSTIVO DE LAS DEFICIENCIAS DE LOS SISTEMAS

- Debe realizarse un análisis formal de las deficiencias previo a la certificación para evaluar la eficacia y el cumplimiento de la implantación del sistema en la organización.
- Este análisis final de deficiencias preparará a su organización para la auditoría final de certificación.

9 MEDIDAS CORRECTORAS

- La organización debe estar preparada para la auditoría de certificación final, siempre que la auditoría de análisis de deficiencias realizada en el último paso y todas las no conformidades (NC) se hayan asignado acciones correctivas.
- Compruebe que todas las NC significativas están cerradas y que la organización está preparada para la auditoría final de certificación.

10 AUDITORÍA FINAL DE CERTIFICACIÓN

- Una vez cumplimentado, es de esperar que se recomiende a su organización que se registre según la norma exigida
- ¡ENHORABUENA!



Authored by: Tony Bevan, NQA UK Auditor



www.nqa.com

