ISO 22301 – Sistemas de gestión de continuidad del negocio

Mike Henigan
Secretario, ISO/TC 292/GT 2
Continuidad y resiliencia organizacional

Cartagena, Colombia

Viernes 31 de agosto del 2018

Temas a tratar…

- Normas BSI e ISO
- Normas de sistemas de gestión
- ISO/TC 292 y Grupo de trabajo 2
- Continuidad de negocio y BCMS en contexto
- ISO 22301 Sistemas de gestión de continuidad de negocio – requisitos
  - Estructura de Alto Nivel de la ISO
  - Alcance y estructura
  - Requisitos, cláusula por cláusula
  - Estado de la revisión

Mi labor como Secretario de la ISO

Oficialmente

- Conocer los procedimientos y reglas de redacción (Directivas de la ISO)
- Ser un buen organizador, conocer las herramientas y servicios de la ISO
- Ser neutral

Extraoficialmente

- Ser diplomático
- Ser riguroso pero justo
- Saber idiomas (y en especial, el lenguaje corporal)
- Digitar rápidamente

Mi portafolio

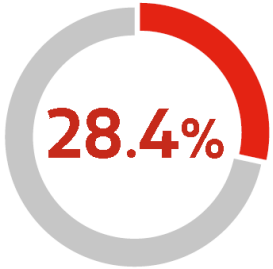
- ISO/TC 292/GT 2 Continuidad y resiliencia organizacional
- ISO/TC 207/SC 1 Sistemas de gestión ambiental
  - ISO 14001, ISO 14004, ISO 14006
- ISO/TC 309 Gobernanza de organizaciones
  - ISO 37000, ISO 37001, ISO 37003

Acerca de BSI

BSI – una organización global de desarrollo de normas

Personal en el ONN, Normas y Publicaciones	300
Miembros suscriptores	14.900
Miembros del comité	>10.000
Comités técnicos y subcomités	1.200
Proyectos vigentes (ISO/IEC/CEN/CLC y normas nacionales)	7.000
Secretariados internacionales/europeos	190
Trabajo de normas internacionales y europeas	93 %

La contribución económica de las normas a la economía del Reino Unido (2015)



del crecimiento anual del PIB del Reino Unido se puede atribuir a las normas, equivalente a **£ 8.200 millones**

37.4 % del crecimiento de la productividad del Reino Unido se puede atribuir a las normas

de las exportaciones adicionales del Reino Unido por año se pueden atribuir a las normas

Las pymes tienen un **41 %** más de probabilidades de exportar si usan normas y las empresas más grandes tienen un **36 %** más de probabilidades de exportar

84% de las empresas afirma que usar normas mejora su reputación

73% de las compañías afirman que las normas permiten tener un mayor control de los problemas ambientales

89% de las empresas afirman que las normas contribuyen a la optimización del cumplimiento de las regulaciones como la ley de salud y seguridad

BSI es pionera en el desarrollo de las normas de S
Gestión líderes en el mundo

Durante más de un siglo, BSI ha trabajado con la industria para crea
consenso y desarrollar normas de excelencia

Año	Norma británica	Norma ISO
1979	BS 5750	ISO 9001 **Gestión de calidad**
1992	BS 7750	ISO 14001 **Gestión ambiental**
1995	BS 7799	ISO/IEC 27001**Seguridad de la información**
1996	BS 8800	ISO 45001 **Salud y seguridad ocupacional**
2000	BS 8600	ISO 10002 **Satisfacción del cliente**
2002	BS 15000	ISO/IEC 20000 **Gestión de servicios de TI**
2004	PAS 55	ISO 55001 **Gestión de activos**
2009	BS 16001	ISO 50001 **Gestión de energía**
2011	BS 10500	ISO 37001 **Antisoborno**
2011	BS 11000	ISO 11000 **Relaciones de colaboración empresarial**
2012	BS 25999	ISO 22301**Continuidad del negocio**
2012	BS 8901	ISO 20121 **Eventos sostenibles**
2013	BS 13500	ISO 37000 **Guía para la gobernanza de organizaciones**

Declaración de políticas de la ISO

Las normas de la ISO ayudan a incrementar los niveles de:

- calidad
- seguridad
- fiabilidad
- eficiencia
- compatibilidad (interoperabilidad)
- intercambiabilidad

y proporciona estos beneficios a un bajo costo.

Contribuyen a que el desarrollo, la fabricación y el suministro de productos y servicios sean **más eficientes, seguros y limpios**.

Hacen que el **comercio** entre países sea más fácil y justo.

También **protegen a los consumidores y usuarios** en general, de productos y servicios – y hacen su vida más simple.

Normas - facilitadoras del comercio

Las normas ayudan a:

- ✓ mejorar el **desempeño** y la **productividad**,
- ✓ propiciar la **innovación**,
- ✓ incrementar la **competitividad**,
- ✓ garantizar la **seguridad del consumidor**,
- ✓ permitir el **acceso al mercado**,
- ✓ cumplir con los **requisitos** del mercado,
- ✓ y estimular el **crecimiento**.

Foro mundial de desarrollo económico 2016:
"Uso efectivo de las normas para facilitar el comercio a nivel nacional e internacional"

Normas – beneficios generales

Las normas ayudan a:

- ✓ apoyar la desregulación
- ✓ permitir que las ideas nacionales sean aceptadas a nivel internacional
- ✓ reflejar todos los intereses, incluyendo los de las pymes, los consumidores y el medio ambiente
- ✓ reducir los costos de desarrollo, producción y transaccionales, tanto para los negocios establecidos como para aquellos que incursionan en el mercado
- ✓ incrementar la diversidad y calidad de los proveedores tanto para los productores como para los consumidores
- ✓ promover la competencia leal y contrarrestar las concentraciones nocivas de poder económico

MSS desempeña un papel clave en la nueva gener de normas

Normas de especificación de productos

- A partir de 1901, las normas iniciales se centraron en las especificaciones del producto para armonizar y facilitar el comercio y reducir la duplicación
  - Ancho de vías férreas
  - Especificaciones del acero
  - Normas de construcción
  - Productos agrícolas
  - Productos de consumo y eléctricos
  - Equipo de protección personal
  - Dispositivos médicos
- Las normas de especificación de productos siguen siendo relevantes en la actualidad, impulsando la interoperabilidad y la innovación en áreas como las ciudades inteligentes y la medicina regenerativa (por ejemplo, las células madre)

Normas de procesos empresariales

- La próxima generación de normas se centró en los procesos empresariales para garantizar una producción de calidad consistente
- La BSI le dio forma a las normas originales para:
  - Gestión de calidad (ISO 9001)
  - Seguridad de la información (ISO/IEC 27001)
  - Gestión del medio ambiente (ISO 14001)
  - Salud y seguridad (OHSAS 18000)
  - Gestión de servicios de TI (ISO/IEC 20000-1)
  - Continuidad de negocio (ISO 22301)
  - Eventos sostenibles (ISO 20121)

Normas de potencial de negocio

- La nueva generación de normas de la BSI se centra en el comportamiento y los valores de las personas para ayudar a las organizaciones a alcanzar su máximo potencial y proteger su reputación corporativa
- Las normas clave incluyen:
  - Antisoborno
  - Responsabilidad Social Corporativa
  - Relaciones empresariales colaborativas/Gestión de cadena de suministro

Normas de especificación de productos

Normas de procesos empresariales

Normas de potencial de negocio

Fundación 1901

1950

2000

Beneficios de las normas de sistemas de gestión

- Las MSS generan rendimientos de **valor financiero** superiores a cualquier inversión o tiempo incurrido
- Mayores tasas de **supervivencia corporativa** frente a quienes no adoptan normas
- **Aumento de ventas**
- **Supera** el promedio del mercado en más del 10 %
- Las **pequeñas empresas** obtienen proporcionalmente más beneficios que las organizaciones más grandes
- **Amplia gama de beneficios** que impacta a los accionistas, empresarios y empleadores

Normas de sistemas de gestión: fundamentos

- Contienen **conceptos básicos** que se pueden aplicar para alcanzar el **logro rentable** de cualquier objetivo deseado.
- Los sistemas de gestión **no arreglarán** una organización mal administrada.
- La implementación y operación exitosas **requieren una buena administración**.
- La organización debe adaptar el sistema de gestión a lo que ya hace, y no tratar de adaptarse a este.
- El sistema de gestión debe diseñarse para que **agregue valor**. Si no agrega valor, la organización debería **reevaluar** su enfoque.
- Los sistemas de gestión se centran en la **prevención de problemas y el valor**, *no* en documentos, procedimientos, registros y papeleo.
- Los sistemas de gestión **promueven la disciplina** donde la disciplina agrega valor; y permite **flexibilidad** donde la flexibilidad agrega valor.

Proceso de desarrollo de normas

Cualquiera puede sugerir una idea para una nueva norma

Se evalúan todas las ideas para las nuevas normas

Si se aprueban, se crea un proyecto

El comité hace un borrador de la norma

Se expide el borrador para consulta pública abierta

El comité revisa los comentarios

Se entrega el borrador actualizado para su aprobación final

Los documentos se publican en línea en BSOL

Cualquiera puede hacer comentarios sobre una norma existente

Las normas nacionales, europeas y de la ISO se revisan por lo menos cada 5 años

ISO/TC 292
Seguridad y resiliencia

GT 2
Continuidad y resiliencia organizacional

ISO/TC 292 Seguridad y resiliencia

http://www.isotc292online.org/

46 miembros participantes, incluidos Colombia, Panamá, México, Trinidad y Tobago, Haití, Argentina y Brasil

15 miembros observadores

- Grupo de Trabajo 1 - Terminología
- **GT 2 - Continuidad y resiliencia organizacional**
- GT 3 - Gestión de emergencias
- GT 4 - Autenticidad, integridad y confianza para productos y documentos
- GT 5 - Resiliencia de la comunidad
- GT 6 - Seguridad protectora

ISO/TC 292/GT 2 Continuidad y resiliencia organizacional

140 expertos registrados de 29 organismos nacionales miembros

El GT 2 es responsable de:

- ISO 22301:2014 Sistemas de gestión de continuidad del negocio – requisitos > en revisión
- ISO 22313:2014 BCMS – Guía > en revisión
- ISO/TS 22317 BCMS – Directrices para la evaluación de impacto en el negocio
- ISO/TS 22318 BCMS – Directrices para la continuidad de la cadena de suministro

y…

La familia de continuidad del negocio

... El GT 2 es responsable de...

- ISO/TS 22330:2018 BCMS – Directrices para aspectos de las personas
- ISO/TS 22331:2018 BCMS – Directrices para la estrategia de continuidad del negocio
- ISO/TS 22332:20xx BCMS – Guía para el desarrollo de procedimientos de continuidad de negocio >>> borrador en redacción

El GT 2 alimenta la terminología de la ISO/TC 292/GT 1 en

- ISO 22300 Seguridad y resiliencia – Vocabulario

y de la ISO/CASCO para

- ISO/IEC/TS 17021-6 Requisitos de competencias para la auditoría y certificación de BCMS

Continuidad del negocio y gestión de la continuidad del negocio (BCM) en contexto

Definiendo resiliencia y continuidad

ISO 22300:2018

- resiliencia: *capacidad de absorber y adaptarse en un entorno cambiante*
- continuidad del negocio: *capacidad de una organización para continuar entregando sus productos o prestando sus servicios a niveles aceptables predefinidos luego de una perturbación**

*La revisión de la ISO 22301 propone el uso de “incidente perturbador” en lugar de perturbación: *evento que impacta la habilidad de la organización para realizar sus operaciones empresariales de forma normal*

¿Qué es la resiliencia organizacional?

Consciente: Las actividades planificadas, a menudo basadas en funciones, dirigidas a mejorar la resiliencia:

Inconsciente: Los elementos no planificados de la resiliencia que ocurren en:

- Estrategia y planificación de negocio
- Cultura
- Enfoques a la innovación
- Cómo funciona el liderazgo
- Redes y alianzas empresariales, etc…

¿Qué es la continuidad del negocio?

La **Continuidad del negocio (BC)** es la capacidad de una organización para continuar entregando sus productos o prestando sus servicios a niveles aceptables predefinidos luego de un incidente perturbador (ISO 22300:2018)

La **Gestión de continuidad del negocio (BCM)** es el proceso de implementar y mantener la continuidad del negocio para preparar a la organización para hacer frente a incidentes perturbadores que de otra manera podrían impedirle cumplir con sus obligaciones

Un **sistema de gestión de la continuidad del negocio (BCMS)** le permite a la organización controlar, evaluar y mejorar de manera continua su continuidad de negocio.

Impulsores de la BCM

La BC se enfoca en el **impacto de la perturbación**, no en la causa

Como resultado, *antes* de que ocurra un incidente perturbador, la organización puede proteger:

- **Recursos** (por ejemplo, personas, instalaciones, tecnología e información)
- **Cadena de suministros**
- **Partes interesadas**, y
- **Reputación.**

Puede determinar las **respuestas** que posiblemente se necesiten para poder

- **manejar las consecuencias** y
- **evitar impactos inaceptables.**

Elementos clave de la BCM

La BCM implica:

- **Identificar** los productos y servicios de la organización y las actividades necesarias para proporcionarlos
- Conocer las **prioridades** para reanudar las entregas y actividades, y los **recursos** que requieren
- Comprender claramente las **amenazas** y conocer los **impactos** de no reanudar las actividades
- Contar con mecanismos **sólidos** para **reanudar las actividades** dentro de los **plazos requeridos** después de un incidente perturbador
- Garantizar que estos mecanismos se **revisen y actualicen** de manera rutinaria para que sigan siendo **efectivos** en todas las circunstancias

¿Qué es un evento perturbador?

Perturbación repentina

- Terremoto/huracán/tornado/inundación
- Problemas de TI – apagón/ciberataque/filtración de datos
- Terrorismo
- Calidad del producto

Perturbación gradual

- Pandemia/enfermedad humana
- Nuevas leyes/regulaciones
- Corrupción

657 participantes

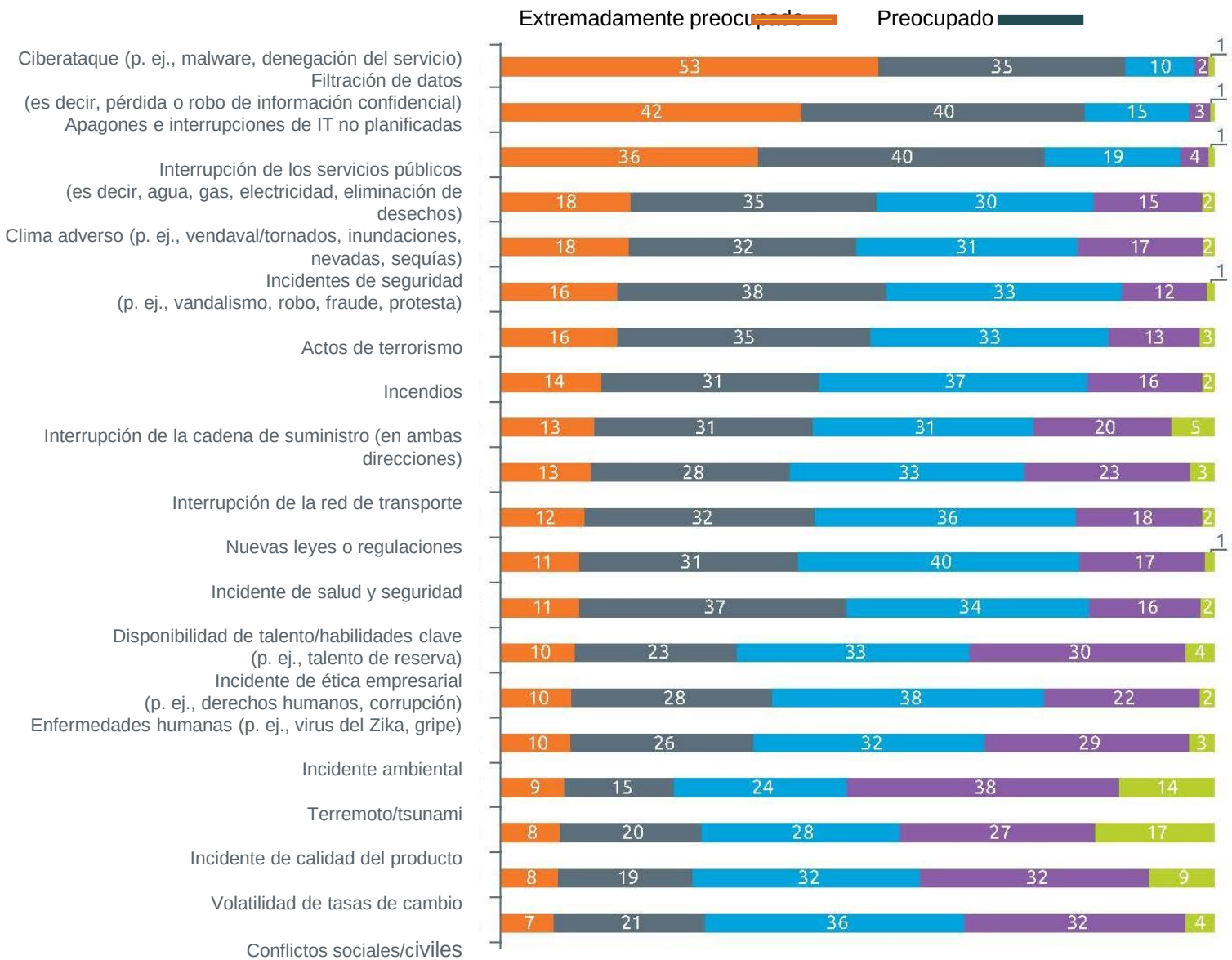
76 países

Las 10 amenazas más comunes

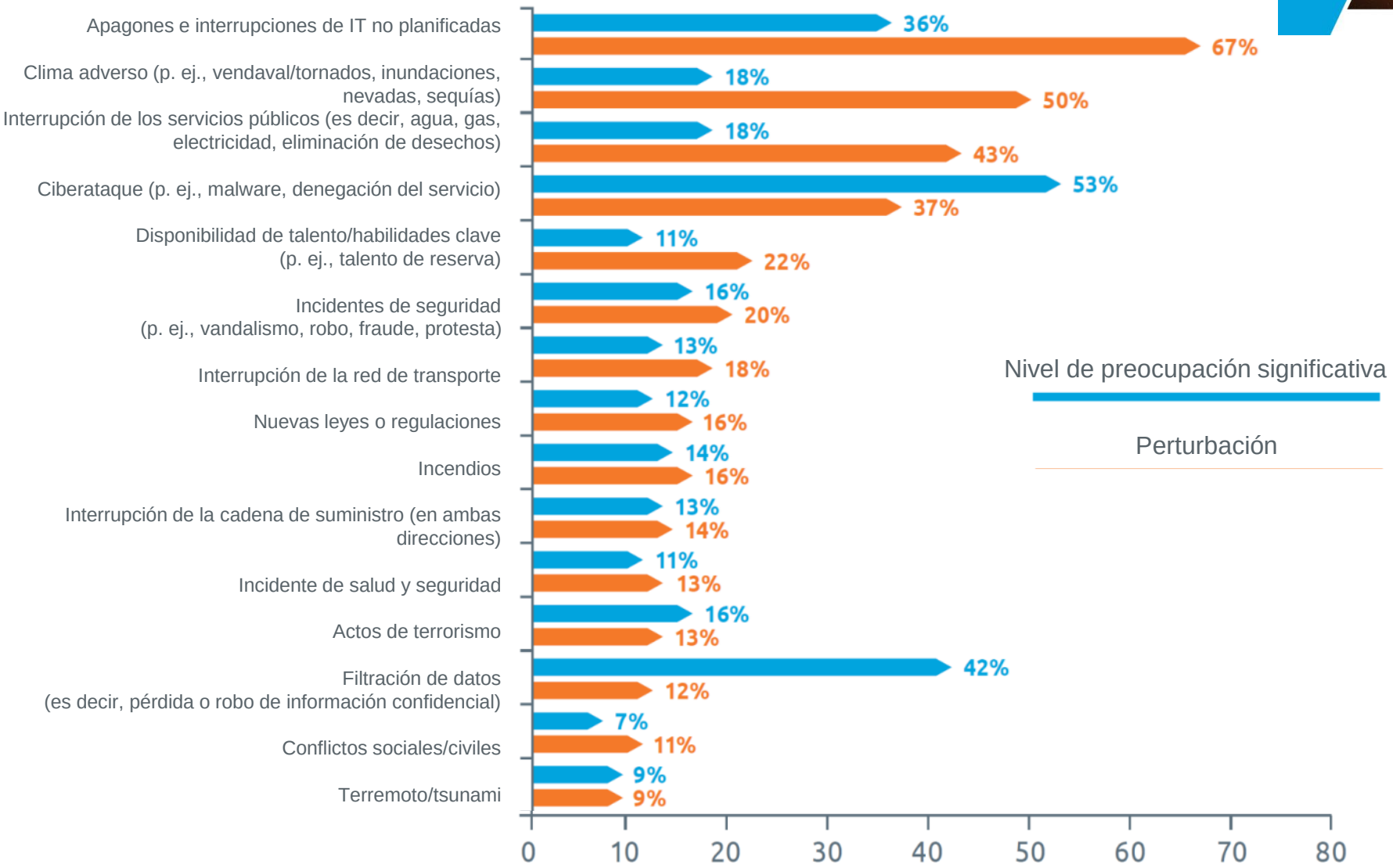
1. Ciberataques
2. Filtraciones de datos
3. Apagones e interrupciones de IT no planificadas
4. Interrupción de los servicios públicos
5. Clima adverso
6. Actos de terrorismo
7. Incidentes de seguridad
8. Incendios
9. Interrupción de la cadena de suministro
10. Interrupción de la red de transporte

bsi.

Los 20 motivos de preocupación más comunes



CREENCIA VS. REALIDAD (LAS 15 PRINCIPALES CAUSAS DE PERTURBACIÓN)



Las tres principales

	Europa	Norteamérica	América Central/Latinoamérica
Las tres principales amenazas	1. Ciberataques (55 %) 2. Filtración de datos (42 %) 3. Apagones e interrupciones de telecomunicaciones no planificadas (236 %)	1. Ciberataques (53%) 2. Filtración de datos (44%) 3. Apagones e interrupciones de telecomunicaciones no planificadas (30%)	1. Ciberataques (44%) 2. Filtración de datos (34%) 3. Apagones e interrupciones de telecomunicaciones no planificadas (28%)
Las tres principales perturbaciones	1. Apagones e interrupciones de telecomunicaciones no planificadas (73%) 2. Interrupción de los servicios públicos (45 %) 3. Ciberataques (40%)	1. Clima adverso (81 %) 2. Apagones e interrupciones de telecomunicaciones no planificadas (56%) 3. Interrupción de los servicios públicos (44%)	1. Clima adverso (53%) 2. Interrupción de los servicios públicos (42%) 3. Apagones e interrupciones de telecomunicaciones no planificadas (32 %)
Las tres principales tendencias	1. Uso de la Internet para lanzar ataques maliciosos (80 %) 2. Nuevas regulaciones e incremento del escrutinio regulatorio (52 %) 3. Influencia de las redes	1. Uso de la Internet para lanzar ataques maliciosos (80 %) 2. Influencia de las redes sociales (54%) 3. Prevalencia y alta adopción de servicios	1. Uso de la Internet para lanzar ataques maliciosos (61%) 2. Nuevas regulaciones e incremento del escrutinio regulatorio (56%) 3. Influencia de las redes

Uso de la ISO 22301

54%
Usa la ISO 22301 como marco pero no se certifica.

16%
Usa la ISO 22301 como marco y se certifica.

10%
No usa actualmente la ISO 22301 como marco, pero se tienen intenciones de avanzar en este tema durante 2018.

13%
No usa actualmente la ISO 22301 como marco y no tiene intenciones de avanzar en este tema durante 2018.

7%
N.A.

Comparación por sector de la industria

Minorista y mayorista	Fabricación	Administración pública y defensa	Salud y seguro social	Financiero y seguros	Energía y servicios públicos	Servicios profesionales	TIC
35%	58%	68%	68%	72%	74%	74%	86%

(Mala) gestión de la continuidad del negocio

Perrier, cuando se halló benceno en su agua embotellada

- Perrier Francia inicialmente negó la existencia del problema
- Por el contrario, Perrier EE. UU. retiró todas las existencias de inmediato
- Esta confusión provocó pérdida de confianza en la marca
- Eventualmente, todo el producto tuvo que ser retirado en todo el mundo
- El valor de las acciones de la compañía colapsó
- Perrier fue adquirida por Nestlé

Buena gestión de continuidad del negocio

Ejemplo de una empresa que gestionó la BCM adecuadamente

Morgan Stanley antes de los atentados del 11 de septiembre a las Torres Gemelas

- Más de 3.000 empleados trabajaban en las Torres Gemelas
- En los 3 días posteriores al atentado, todos los empleados sobrevivientes fueron contactados
- En los 3 días posteriores al atentado, se pusieron en marcha instalaciones de emergencia y se restauraron capacidades importantes
- Se pusieron en marcha programas de apoyo para proporcionar apoyo emocional al personal

Resultados de un programa efectivo de BCM

- Los productos y servicios clave están identificados y **protegidos**
- La **cadena de suministro** de la organización está asegurada
- La **reputación** de la organización está protegida
- Se identifican y siguen las **obligaciones legales y reglamentarias**
- Se habilita una **capacidad de gestión de incidentes** para proporcionar una respuesta efectiva, se brinda apoyo y capacitación al personal, se establece una comunicación adecuada
- La **comprensión** de la organización sobre sí misma y sus relaciones con otras organizaciones, reguladores o departamentos gubernamentales pertinentes, autoridades locales y servicios de emergencia se desarrolla, documenta y comprende adecuadamente
- Los **requisitos de los grupos de interés** se comprenden y pueden ser atendidos

ISO 22301
Sistemas de gestión de continuidad del negocio – Requisitos

ISO 22301:2014 y la próxima revisión

La edición actual fue publicada en 2014.

La gestión de continuidad del negocio es una disciplina relativamente "nueva", por lo que se está revisando la ISO 22301:2014 para

- proporcionar mayor claridad con respecto a los requisitos, y
- reflejar las últimas consideraciones sobre BCM.

Se proponen algunos requisitos adicionales; sin embargo, se necesita una **justificación clara y sustancial** para los cambios propuestos que tienen un impacto significativo en las filosofías de la continuidad del negocio.

Esta presentación se centra en los requisitos de 2014 pero identifica los requisitos/cambios adicionales clave propuestos para la revisión

ISO 22301 y la Estructura de Alto Nivel de la ISO

El “Anexo SL” de las Directivas de la ISO, Parte 1, proporciona definiciones básicas normalizadas y requisitos comunes que:

- garantizan la **consistencia entre MSS**
- apoya la **integración de MSS**.

Proporciona **flexibilidad** para que los comités individuales integren sus temas y requisitos técnicos “específicos de disciplina”

La Estructura de Alto Nivel es utilizada por todas las MSS de la ISO, *incluidas*	
ISO 9001 **Gestión de calidad**	ISO 14001 **Gestión ambiental**
ISO/IEC 27001**Seguridad de la información**	ISO 45001 **Salud y seguridad ocupacional**
ISO/IEC 20000 **Gestión de servicios de TI**	ISO 55001 **Gestión de activos**
ISO 50001 **Gestión de energía**	ISO 37001 **Antisoborno**
ISO 22000 **Seguridad alimentaria**	ISO 22301**Continuidad del negocio**
ISO 39001 **Seguridad vial**	ISO 37101 **Desarrollo sostenible en las comunidades**

ISO 22301 y la Estructura de Alto Nivel de la ISO

- ✓ Comprender el **contexto de la organización**
- ✓ Comprender las **necesidades de las partes interesadas**
- ✓ Identificar **riesgos y oportunidades**
- ✓ Hacer énfasis en **liderazgo**
- ✓ Enlazar a la **dirección estratégica** de la organización
- ✓ **Integrada** a los procesos empresariales
- ✓ **Planificar** para tener en cuenta riesgos y oportunidades, establecer **políticas y objetivos**
- ✓ **Planificar, Hacer, Verificar, Actuar**

Alcance de la ISO 22301

"Especifica los requisitos para planificar, establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar continuamente un sistema de gestión documentado para protegerse, reducir la probabilidad de que ocurra, prepararse, responder y recuperarse de incidentes perturbadores cuando surjan"

- ✓ Aplica a **todas las organizaciones**, independientemente del tipo, tamaño y naturaleza
  - ➢ Organizaciones pequeñas, medianas y grandes
  - ➢ Sectores público, privado, voluntario, sin fines de lucro
- ✓ El alcance de la aplicación depende del entorno operativo y la complejidad de la organización *(revisión: magnitud del impacto)*
- ✓ La organización puede diseñar un BCMS apropiado para sus necesidades y cumple con los requisitos de las partes interesadas.

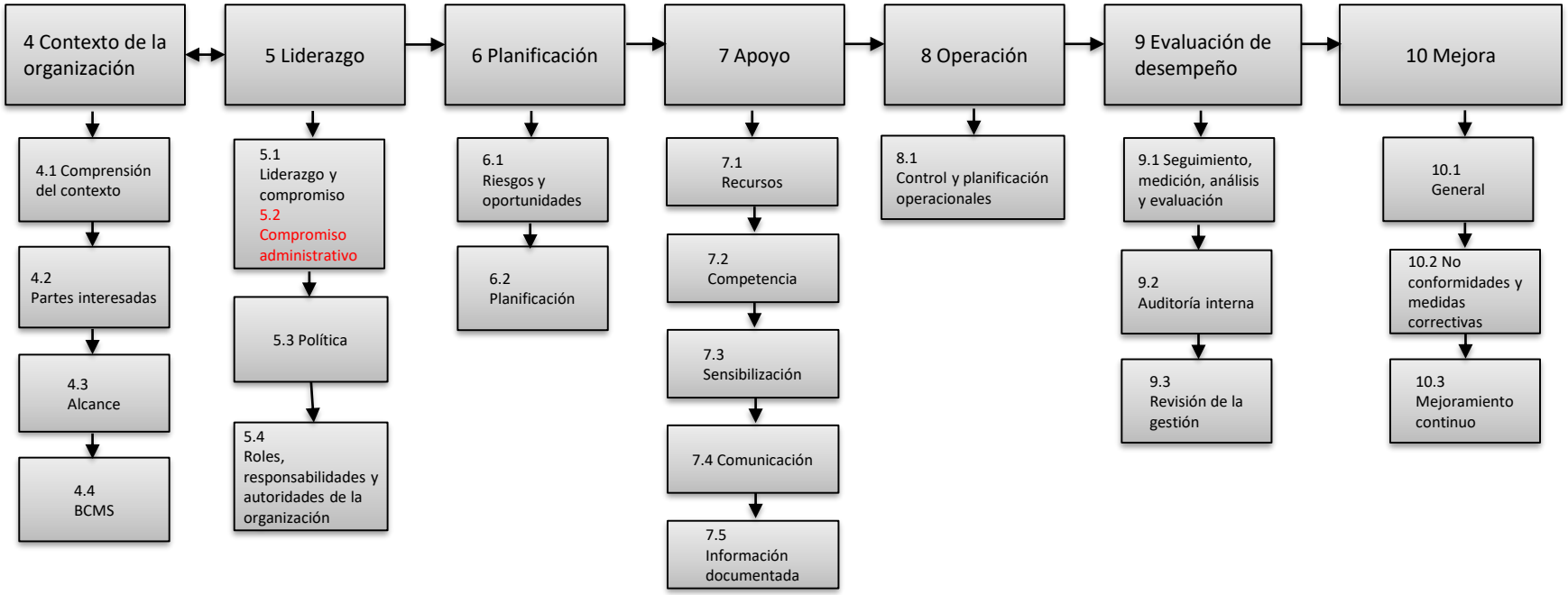
Alcance de la ISO 22301

Recordatorio: **Las normas son voluntarias**. No incluyen requisitos contractuales, legales o reglamentarios y no reemplazan las leyes nacionales, cuyas normas se entiende que los usuarios cumplen y que tienen prioridad; esto significa que no existe un requisito de la ISO para “obedecer la ley”.

El **principio de neutralidad** de la ISO se aplica a la ISO 22301 como un requisito de la norma. La norma ISO 22301 se redactó de manera tal que la conformidad puede evaluarse por:

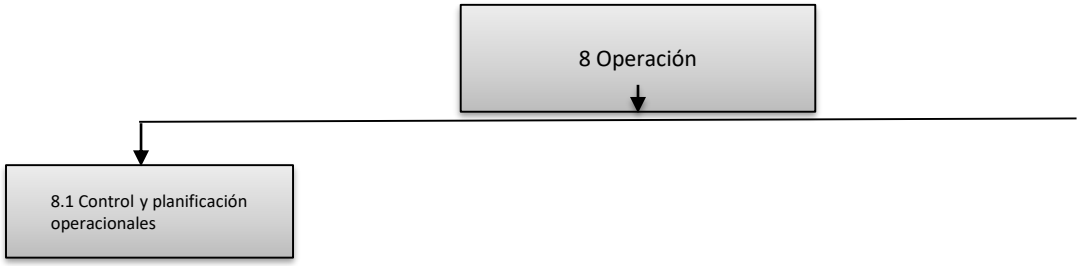
- Primera parte, es decir, el fabricante o el proveedor
- Segunda parte, es decir, un usuario o comprador
- Tercera parte, es decir, un organismo independiente como el organismo de certificación

Estructura y contenido de la ISO 22301

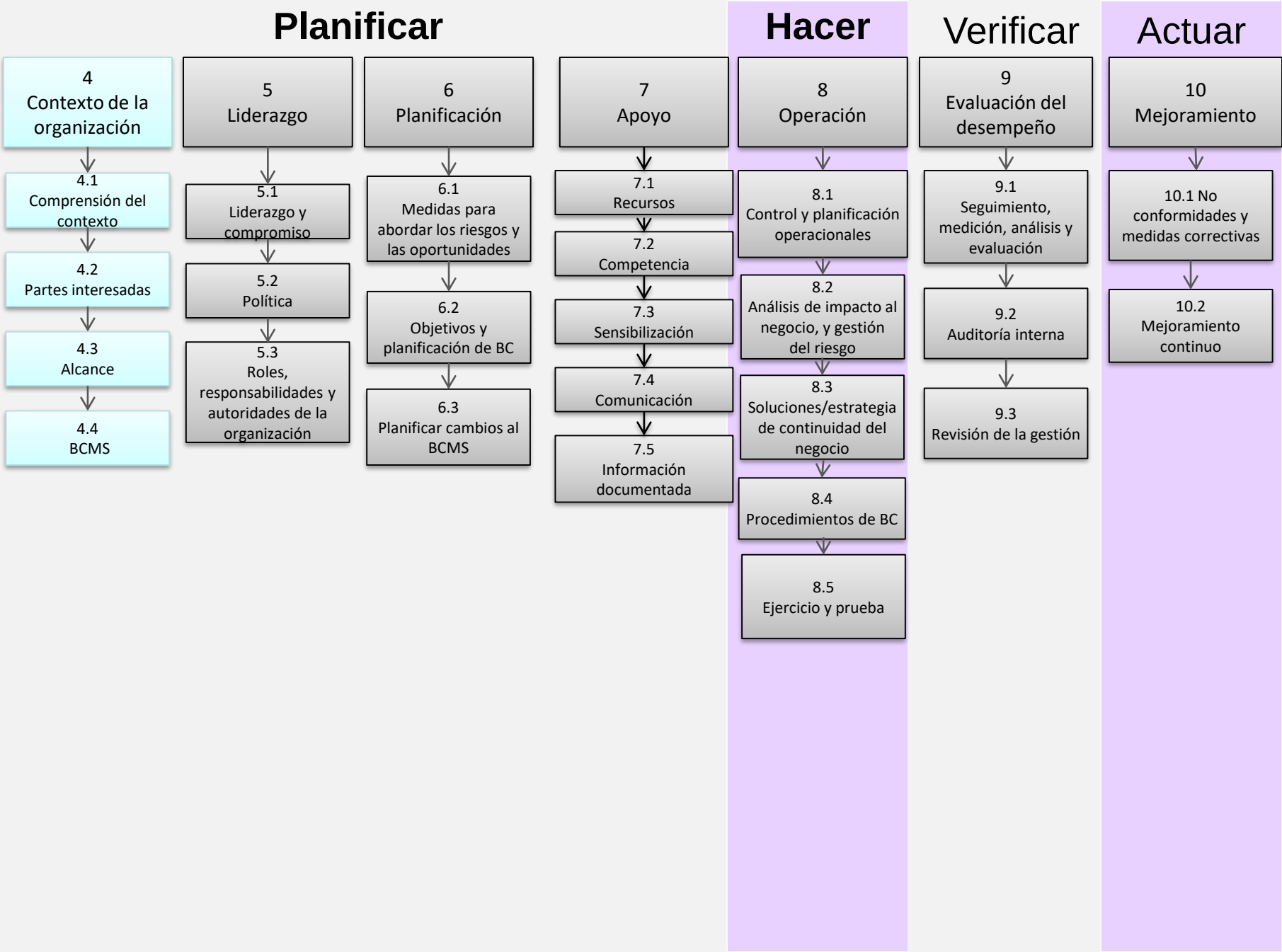


39

Estructura y generalidades de la ISO 22301



40


Planificar
Hacer
Verificar
Actuar
4
Contexto de la organización
4.1
Comprensión del contexto
4.2
Partes interesadas
4.3
Alcance
4.4
BCMS
5
Liderazgo
5.1
Liderazgo y compromiso
5.2
Política
5.3
Roles, responsabilidades y autoridades de la organización
6
Planificación
6.1
Medidas para abordar los riesgos y las oportunidades
6.2
Objetivos y planificación de BC
6.3
Planificar cambios al BCMS
7
Apoyo
7.1
Recursos
7.2
Competencia
7.3
Sensibilización
7.4
Comunicación
7.5
Información documentada
8
Operación
8.1
Control y planificación operacionales
8.2
Análisis de impacto al negocio, y gestión del riesgo
8.3
Soluciones/estrategia de continuidad del negocio
8.4
Procedimientos de BC
8.5
Ejercicio y prueba
9
Evaluación del desempeño
9.1
Seguimiento, medición, análisis y evaluación
9.2
Auditoría interna
9.3
Revisión de la gestión
10
Mejoramiento
10.1 No conformidades y medidas correctivas
10.2
Mejoramiento continuo

Planificar, Hacer, Verificar, Actuar – PHVA

ISO 22301:2012

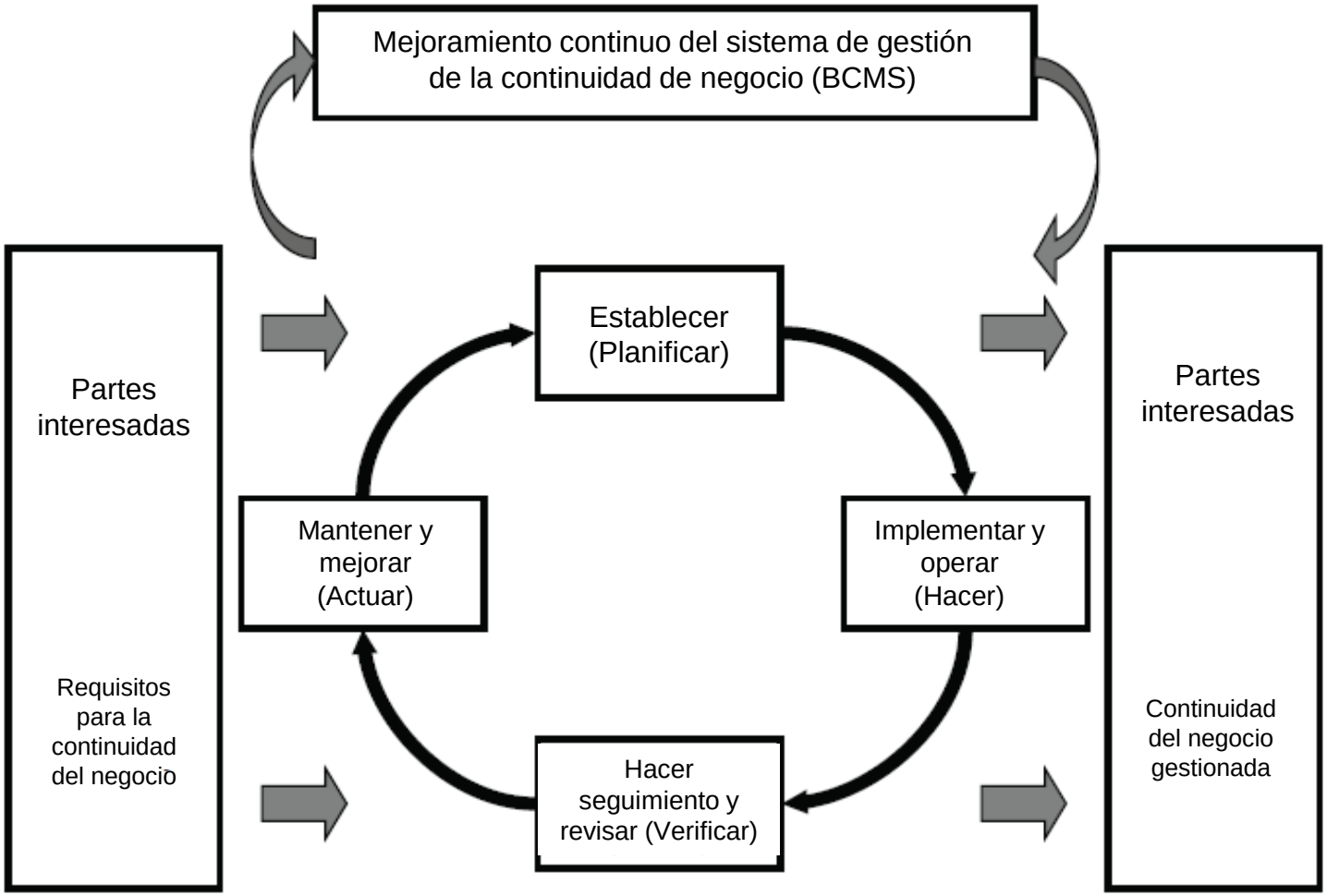


Figura 1 – Modelo PHVA aplicado a procesos BCMS

Requisitos de la ISO 22301
Cláusula 4 – Contexto de la organización

Determinar los **asuntos externos e internos relevantes** para su organización y que sean **relevantes para su dirección estratégica** (4.1)

Identificar las **partes interesadas relevantes** y sus **requisitos relevantes**, incluido un procedimiento para identificar los requisitos legales y reglamentarios aplicables (4.2)

Determinar y documentar el alcance del BCMS (4.3), tenga en cuenta:

- asuntos externos e internos
- requisitos de las partes interesadas
- misiones, objetivos, obligaciones internas/externas de la organización

NB: documentar y explicar **exclusiones**. Estas no deben afectar la continuidad del negocio determinada por el BIA o evaluación de riesgos

Requisitos de la ISO 22301
Cláusula 5 – Liderazgo y compromiso

5.1 y 5.2 (2014), *en revisión, fusionadas en la nueva 5.1*

La alta dirección demuestra liderazgo y compromiso:

- La **política y objetivos** de BC están establecidos y son compatibles con la **dirección estratégica** de la organización
- Los requisitos de BCMS están **integrados con los procesos de negocio**
- **Comunicar** la importancia de la BC eficaz y conforme a los requisitos de BC
- Dirigir y apoyar a las personas para contribuir a la **efectividad** del BCMS
- Apoyar funciones pertinentes de gestión
- Promover el mejoramiento continuo

Requisitos de la ISO 22301
Cláusula 5 – Liderazgo y compromiso

5.3, *nueva 5.2* **Política**

- Es apropiada, proporciona un marco y tiene el compromiso para satisfacer los requisitos aplicables y para el mejoramiento continuo
- Documenta, comunica y está disponible para las partes interesadas

5.4, *nueva 5.3* **Roles, responsabilidades y autoridades de la organización**

- La alta dirección se asegura de que las responsabilidades y las autoridades se asignen y comuniquen
- Asignar responsabilidad y autoridad para
  - garantizar que el MS cumple con los requisitos
  - Informar a la alta dirección sobre el desempeño del BCMS

Requisitos de la ISO 22301
Cláusula 6 – Planeación

6.1 Medidas para abordar los riesgos y las oportunidades

Al planificar el BCMS, **considere** los asuntos planteados en la cláusula 4.1 (contexto) y los requisitos de las partes interesadas relevantes identificadas en la cláusula 4.2, y **determine los riesgos y las oportunidades**

- para garantizar que el MS puede lograr los resultados previstos
- prevenir o reducir los efectos indeseados
- alcanzar el mejoramiento continuo

Planificar **medidas** para abordar los riesgos y las oportunidades

Planificar cómo **integrar e implementar** medidas en los procesos del BCMS y **evaluar la efectividad** de estas

Requisitos de la ISO 22301
Cláusula 6 – Planeación

6.2 Objetivos de BC y planes para lograrlos

Establecer objetivos de BC a niveles y funciones relevantes

Los objetivos de BC deben ser

- Consistentes con la política de BC
- Medibles
- Seguidos, comunicados y actualizados

La organización debe conservar la información documentada.

Al momento de planificar cómo alcanzar los objetivos de BC, determinar:

- Qué se va a hacer y cuándo se completará
- Recursos necesarios
- Quién es el responsable
- Cómo se evaluarán los resultados

Requisitos de la ISO 22301
Cláusula 6 – Planeación

6.3 Planificar cambios al BCMS *(no es el Anexo SL, nuevo y en revisión)*

Los cambios se llevarán a cabo de forma planificada.

La organización debe considerar:

- **Propósito** de los cambios y sus **consecuencias** potenciales
- **Integridad** del BCMS
- Disponibilidad de **recursos**
- Asignación o reasignación de **responsabilidades y autoridades**.

Cambio también tratado en **8.1 Control y planificación operacionales**: controlar los cambios planificados y revisar las consecuencias de los cambios involuntarios, tomando medidas para mitigar cualquier efecto adverso

Requisitos de la ISO 22301
Cláusula 7 – Apoyo

Determinar y proporcionar **recursos** para el establecimiento, implementación, mantenimiento y mejoramiento continuo (7.1)

Determinar la **competencia** necesaria, con base en la educación, capacitación o experiencia apropiadas (7.2)

Garantizar la **concientización** de la política de BC, cómo contribuye a la efectividad y cuáles son las implicaciones de no cumplirla (7.3) , adicionalmente

- *Su propio rol y responsabilidades antes, durante y después de los incidentes perturbadores*

Determinar la necesidad de **comunicaciones internas y externas** relevantes para el BCMS, además del contenido, el momento, el receptor y la manera de comunicar (7.4) *– la revisión abarca las comunicaciones en la cláusula 8*

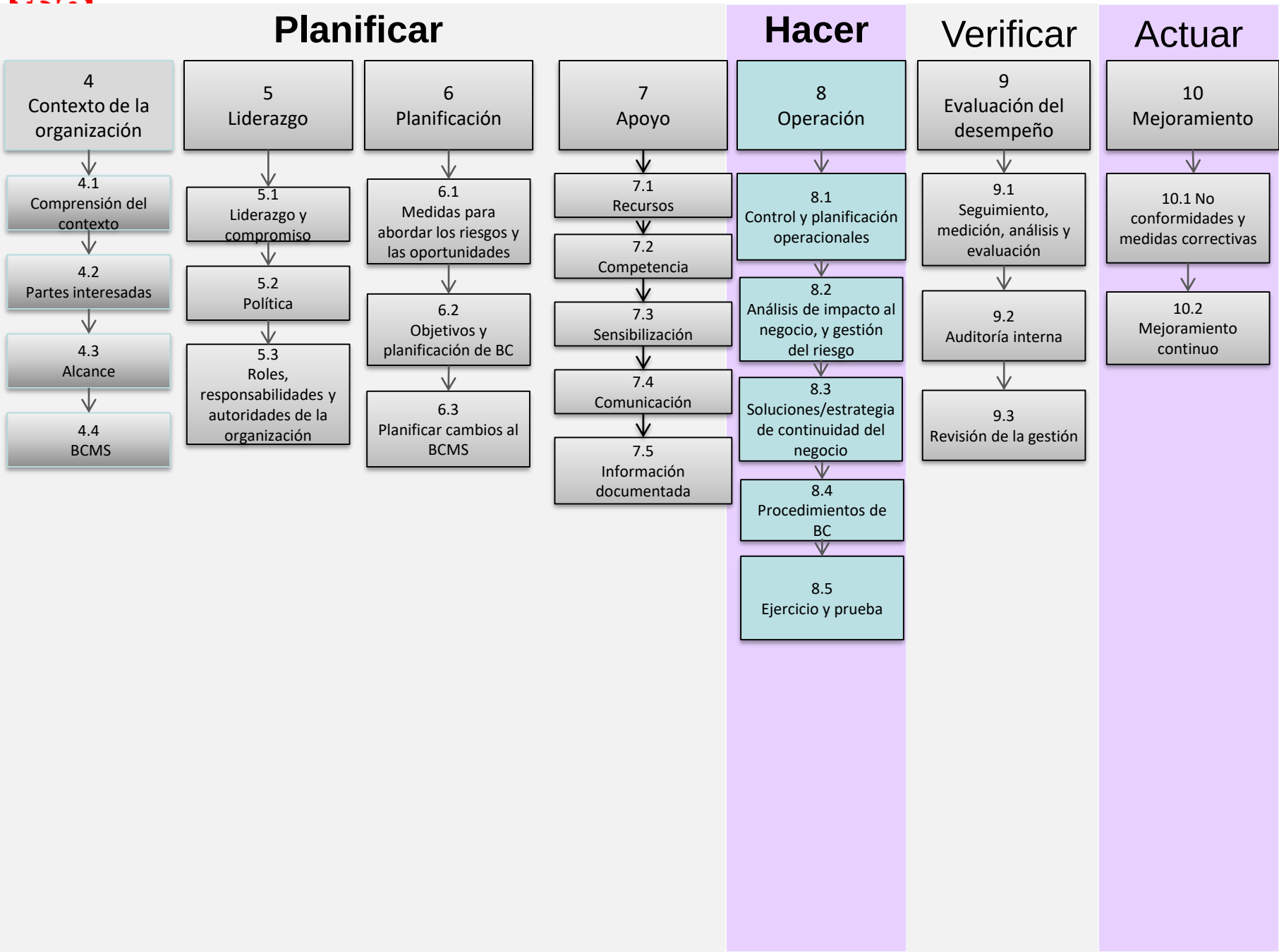
Requisitos de la ISO 22301
Cláusula 7 – Apoyo

7.5 Información documentada *(según el Anexo SL)*

El BCMS debe incluir información documentada tal como lo exige la norma y como lo considere necesario la organización para la efectividad del BCMS (con base en el tamaño y la complejidad)

Garantizar la identificación y descripción, formato, y revisión y aprobación apropiados para la idoneidad y suficiencia

Controlar para garantizar que esté disponible y sea apta para su uso en el momento y lugar que se requiera, y que esté protegida –incluye confidencialidad, uso inapropiado, pérdida de integridad–


Planificar
Hacer
Verificar
Actuar
4
Contexto de la organización
4.1
Comprensión del contexto
4.2
Partes interesadas
4.3
Alcance
4.4
BCMS
5
Liderazgo
5.1
Liderazgo y compromiso
5.2
Política
5.3
Roles, responsabilidades y autoridades de la organización
6
Planificación
6.1
Medidas para abordar los riesgos y las oportunidades
6.2
Objetivos y planificación de BC
6.3
Planificar cambios al BCMS
7
Apoyo
7.1
Recursos
7.2
Competencia
7.3
Sensibilización
7.4
Comunicación
7.5
Información documentada
8
Operación
8.1
Control y planificación operacionales
8.2
Análisis de impacto al negocio, y gestión del riesgo
8.3
Soluciones/estrategia de continuidad del negocio
8.4
Procedimientos de BC
8.5
Ejercicio y prueba
9
Evaluación del desempeño
9.1
Seguimiento, medición, análisis y evaluación
9.2
Auditoría interna
9.3
Revisión de la gestión
10
Mejoramiento
10.1 No conformidades y medidas correctivas
10.2
Mejoramiento continuo

Requisitos de la ISO 22301
Cláusula 8 – Operación

Cinco elementos de la BCM

Control y planificación operacionales (8.1)

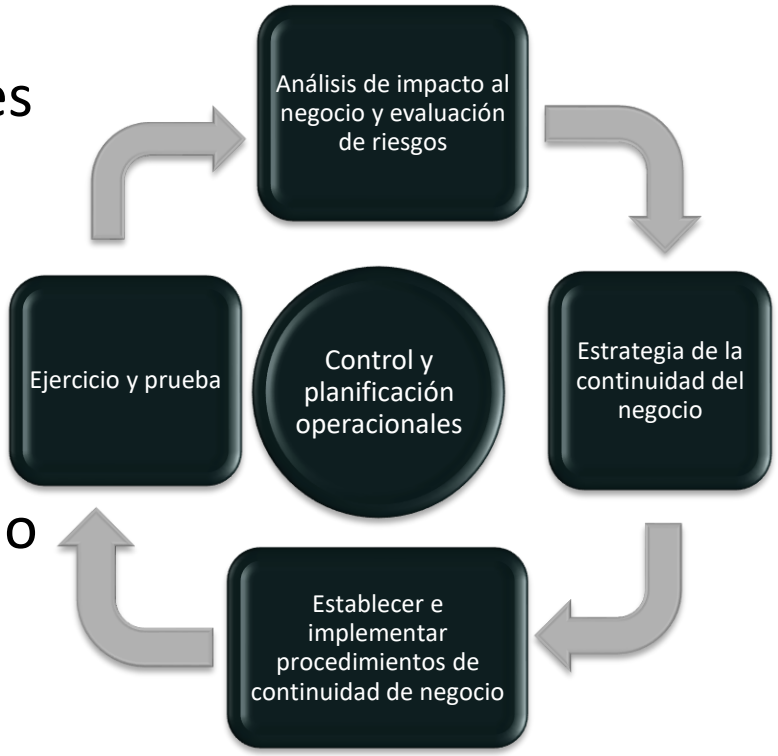
- *en el núcleo de la BCM*

Análisis de impacto al negocio y evaluación de riesgos (8.2)

Estrategia de continuidad de negocio (8.3) *("Soluciones" en la revisión)*

Establecer e implementar procedimientos de BC (8.4) *("Respuesta")*

Ejercicio y prueba (8.5) *("Programa de ejercicio")*



Requisitos de la ISO 22301
Cláusula 8 – Operación

8.1 Control y planificación operacionales *(Anexo SL)*

La organización debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos, y para implementar las medidas determinadas en la cláusula 6.1

- Establecer criterios
- Implementar control
- Conservar la información documentada

La organización debe **controlar los cambios** y revisar las consecuencias de los cambios involuntarios, tomando medidas para mitigar cualquier efecto adverso, según sea necesario

Garantizar que los **procesos tercerizados** ***y la cadena de suministros*** están controlados

Requisitos de la ISO 22301
Cláusula 8 – Operación

8.2 Análisis de impacto al negocio (BIA) y evaluación de riesgos

La organización debe establecer, implementar y mantener un **proceso** para analizar los impactos al negocio y gestionar riesgos.

- Comprender los impactos al negocio en caso de que las actividades se detengan le permite a la organización **establecer prioridades** para reanudar las actividades
- También es importante comprender las interrelaciones y los requisitos de recursos de las actividades de la organización y las amenazas sobre estas
- El análisis efectivo le permite a la organización identificar las estrategias*/soluciones* de BC para:
  - Limitar el impacto de la perturbación en la organización
  - Reducir la duración del evento perturbador
  - Reducir la posibilidad de un incidente perturbador

Requisitos de la ISO 22301
Cláusula 8.2 – BIA y evaluación de riesgos

8.2.2 Análisis de impacto al negocio (BIA)

Debería permitirle a la organización:

- Comprender sus productos y servicios
- Comprender las actividades que permiten la entrega de dichos productos o servicios
- Determinar las prioridades y cronogramas para la reanudación (RTO, Tiempo objetivo de recuperación)
- Identificar recursos que posiblemente se requieran para la continuidad y la recuperación
- Identificar dependencias, tanto internas como externas

Requisitos de la ISO 22301
Cláusula 8.2 – BIA y evaluación de riesgos

Análisis de impacto al negocio (continuación)

Los impactos a evaluar pueden ser:

- Financieros – multas/sanciones, pérdida de utilidades
- Reputacionales – imagen negativa o daño a la marca
- Legales y regulatorios – litigios, retiro de la licencia
- Contractuales – incumplimiento del contrato
- Incapacidad de cumplir los objetivos o de aprovechar las oportunidades

La revisión de la ISO 22301 proporciona más detalles sobre los procesos y el análisis

Requisitos de la ISO 22301
Cláusula 8.2 – BIA y evaluación de riesgos

8.2.3 Evaluación de riesgos *[Gestión de riesgos]*

Establecer un proceso de evaluación de riesgos para identificar, analizar y evaluar de manera sistemática el riesgo de perturbaciones *[incidentes perturbadores]*

Intentar responder las siguientes preguntas fundamentales:

- ¿Qué podría suceder y por qué (identificación de riesgos)?
- ¿Cuál podría ser la consecuencia?
- ¿Cuál es la probabilidad de que suceda?
- ¿Hay algo que mitigue las consecuencias o la probabilidad?

Acorde con la norma ISO 31000 para la gestión de riesgos, se debe:

- ✓ IDENTIFICAR RIESGOS
- ✓ ANALIZAR
- ✓ EVALUAR

Requisitos de la ISO 22301
Cláusula 8 – Operación

8.3 Estrategia de la continuidad del negocio *[soluciones]*

Con base en los resultados del BIA y la evaluación de riesgos, se necesita una estrategia para:

- Proteger las actividades prioritarias (p. ej., reducir el riesgo, transferir, cambiar)
- Estabilizar, continuar, reanudar y recuperar las actividades prioritarias (p. ej., reubicación, procesos alternos, soluciones temporales)
- Mitigar, responder y gestionar los impactos (p. ej., seguros, restablecimiento de bienes, gestión de la reputación)

Incluye:

- aprobación de los cronogramas prioritarios para la reanudación
- evaluaciones de las capacidades de BC de los proveedores.

Las normas ISO 22313 y ISO/TC 22331 proporcionan mayor orientación

Requisitos de la ISO 22301

Cláusula 8.3 – Estrategia de continuidad del negocio

La organización necesita establecer **requisitos de recursos** para implementar las estrategias, incluyendo personas, equipos, instalaciones, transporte, finanzas, aliados y proveedores

Para los riesgos identificados que necesitan tratamiento, se deben considerar medidas que

- reduzcan la probabilidad de perturbación
- acorten el periodo de perturbación
- limiten el impacto de la perturbación en los productos y servicios clave de la organización.

La organización debe escoger e implementar tratamientos de riesgos apropiados de acuerdo con su apetito de riesgo.

Requisitos de la ISO 22301
Cláusula 8 – Operación

8.4 Establecer e implementar procedimientos de BC *[Respuesta]*

Los planes y procedimientos de BC ayudarán a gestionar un incidente perturbador y continuar las actividades basados en los objetivos de recuperación identificados en el BIA.

Los procedimientos de BC deben:

- Establecer un protocolo de **comunicaciones** interno y externo
- Ser **específicos** respecto a los pasos inmediatos a seguir
- Ser **flexibles** para responder a las amenazas no anticipadas y cambiar las condiciones internas y externas
- Enfocarse en el **impacto** de los eventos que pueden perturbar las operaciones
- Ser desarrollados con base en supuestos establecidos y un análisis de interdependencias
- Ser efectivos al minimizar las consecuencias mediante la mitigación

Requisitos de la ISO 22301

Cláusula 8.4 – Establecer e implementar procedimientos de BC

Establecer una **estructura de gestión de respuesta a incidentes** (8.4.2) para responder a un incidente perturbador usando personal con la responsabilidad, autoridad y competencia necesaria para gestionar un incidente.

La estructura debe:

- Identificar los umbrales de impacto justificando el inicio de la respuesta formal
- Evaluar la naturaleza y el alcance de un incidente perturbador y su impacto
- Activar una respuesta de BC apropiada
- Contar con procesos y procedimientos para la activación, operación, coordinación y comunicación de la respuesta
- Contar con recursos disponibles
- Comunicarse con las partes interesadas, las autoridades y los medios de comunicación

Requisitos de la ISO 22301
Cláusula 8.4 – Establecer e implementar procedimientos de BC

Puede ser necesario considerar si se debe **comunicar externamente** sobre riesgos e impactos significativos; la **seguridad de la vida** es la primera prioridad, pero también consultar con las partes interesadas pertinentes. Si se decide comunicar, se necesitan procedimientos para comunicar, alertar y advertir (incluidos los medios de comunicación).

Guía de la norma ISO 22313:

- La estructura debe ser simple y capaz de conformarse rápidamente
- Las organizaciones más grandes deben considerar un enfoque escalonado, con diferentes equipos que se enfoquen en diferentes aspectos; p. ej., respuesta a incidentes, gestión de incidentes, comunicaciones, reanudación del negocio.
- En las organizaciones más pequeñas, todos los aspectos pueden ser manejados por un equipo pero nunca debe ser responsabilidad de una sola persona.
- Competencia demostrada mediante capacitaciones y ejercicios.

Requisitos de la ISO 22301
Cláusula 8.4 – Establecer e implementar procedimientos de BC

Procedimientos de **advertencia y comunicación** (8.4.3) para:

- Detectar un incidente y hacerle seguimiento
- Comunicarse internamente y con/a las partes interesadas
- Recibir/responder al sistema de alerta de riesgos regional/nacional
- Garantizar medios de comunicación
- Comunicarse de manera estructurada con los servicios de emergencia
- Registrar información, acciones y decisiones vitales

La revisión a la norma ISO 22301 proporciona mayor detalle

Los procedimientos de comunicación y advertencia se deben llevar a cabo de manera regular

Requisitos de la ISO 22301

Cláusula 8.4 – Establecer e implementar procedimientos de BC

Establecer un **plan de continuidad del negocio** (8.4.4) para dar respuesta a un incidente perturbador y cómo reanudará o recuperará sus actividades dentro de un cronograma predeterminado. Los planes de BC contendrán:

- Roles y responsabilidades definidos para personas y equipos
- Procesos para activar la respuesta
- Detalles para gestionar las consecuencias inmediatas
  - bienestar de las personas
  - opciones estratégicas/tácticas/operacionales para dar respuesta
  - Prevención de pérdidas adicionales
  - *"Protección del medio ambiente" se agregó a la revisión*

Requisitos de la ISO 22301

Cláusula 8.4 – Establecer e implementar procedimientos de BC

Continuación del plan de BC…

- Detalles sobre cómo y bajo cuáles circunstancias la organización se comunicará con los empleados y sus familiares, partes interesadas clave y contactos de emergencia
- Cómo la organización reanudará o recuperará sus actividades prioritarias dentro de los cronogramas predeterminados
- Detalles de la respuesta a los medios de comunicación, incluida una estrategia de comunicación, interfaz preferida con los medios, directrices o plantilla para hacer un borrador de una declaración a los medios, portavoces apropiados
- Un proceso para retirarse una vez haya terminado el incidente.

Requisitos de la ISO 22301
Cláusula 8.4 – Establecer e implementar procedimientos de BC

Recuperación (8.4.5)

Contar con procedimientos documentados para restablecer y retomar las actividades del negocio de las medidas temporales después de un incidente

Ejercicio y prueba (8.5) *[Programa de ejercicio]*

- Ser consistente con el alcance y los objetivos del BCMS
- Contar con escenarios apropiados y bien planeados con propósitos/objetivos claros
- Desarrollar el trabajo en equipo, la competencia, la confianza y el conocimiento
- Minimizar el riesgo de perturbación de las operaciones
- Producir informes, resultados y recomendaciones formales para mejorar
- Ser revisado dentro del contexto de mejoramiento continuo
- Llevarse a cabo durante intervalos planeados o cuando se produzcan cambios significativos

Requisitos de la ISO 22301
Cláusula 9 – Evaluación de desempeño

Identificar a qué se necesita hacerle seguimiento y medición, métodos y tiempos, y cuándo analizar y evaluar los resultados (Anexo SL)

Evaluación de planes, procedimientos y capacidades de BC (9.1.2): debe evaluarse la **idoneidad, suficiencia y efectividad** de los planes, procedimientos y capacidades de BC, incluyendo: revisiones periódicas, análisis, ejercicios, pruebas, informes posteriores al incidente y evaluaciones de desempeño

Evaluar periódicamente el cumplimiento con los requisitos legales y regulatorios, las mejores prácticas industriales y cumplimiento con su propia política y objetivos de BC.

Llevar a cabo evaluaciones en intervalos planificados después de un incidente o activación.

Requisitos de la ISO 22301
Cláusula 9 – Evaluación de desempeño

Auditoría interna (9.2)

Debe llevarse a cabo en **intervalos planificados** para proporcionar información sobre el cumplimiento del BCMS con los requerimientos y si está siendo implementado y mantenido de manera efectiva.

La auditoría debe ser **objetiva**, los resultados se deben **informar** a la gerencia pertinente, y debe **conservar la información documentada**.

Revisión de la gestión (9.3)

Debe llevarse a cabo en **intervalos planificados** para garantizar la **idoneidad, suficiencia y efectividad** , y debe incluir:

- Cambios relevantes en asuntos internos y externos
- Tendencias en no conformidades y acciones correctivas, resultados de evaluaciones y auditorías internas...

Requisitos de la ISO 22301
Cláusula 9 – Evaluación de desempeño

Elementos a incluir en la revisión de la gestión… continuación

- Oportunidades de mejoramiento continuo
- Resultados de ejercicios y pruebas
- Lecciones aprendidas y acciones derivadas de incidentes perturbadores
- Buenas prácticas emergentes y guías

Los **resultados** de la revisión de la gestión incluyen

- Decisiones para el mejoramiento continuo
- Cambios al alcance del BCMS
- Modificación de los procedimientos y controles para responder a los incidentes internos o externos que puedan tener un impacto en el BCMS

Los resultados deben **conservarse** como información documentada, **comunicarse** a las partes interesadas relevantes y **tomarse en consideración**.

Requisitos de la ISO 22301
Cláusula 10 – Mejoramiento

No conformidades y medidas correctivas (10.1)

- Reaccionar, adoptar medidas y enfrentar la situación
- Evaluar la necesidad de medidas para eliminar las causas, implementarlas, revisar cualquier medida correctiva, realizar cambios al BCMS
- Las medidas correctivas deben ser apropiadas a los efectos de las no conformidades
- Conservar la información documentada

Mejoramiento continuo (10.2)

Debe mejorar continuamente la idoneidad, suficiencia y efectividad del BCMS

Revisión de la norma ISO 22301 – Cambios clave

Actualmente en el “Borrador del Comité”, se amplió la consulta para recibir comentarios hasta principios de 2019, se publica a fines de 2019

- Se revisó la definición de “**actividad**”: *un conjunto de una o más tareas con un resultado definido*
- “Estrategia de continuidad del negocio” ahora es “**Soluciones de continuidad del negocio**”
- “Evaluación de riesgos” ahora es “**Gestión de riesgos**”
- Se mejoró la Evaluación de impacto al negocio (BIA)
- 8.4 ahora es “**Respuesta**” (de Establecer e implementar procedimientos de BC), con más en las cláusulas “Advertencia y comunicación” (8.4.2), “Estructura de respuesta” (8.4.3) y “Planes de respuesta” (8.4.4)
- Los elementos de la cláusula 6 - Planificación ahora se encuentran en la cláusula 8 - Operación

PARA FINALIZAR...

GRACIAS A

- ICONTEC, mis anfitriones, por su invitación
- Esta increíble ciudad
- Y a ustedes, la audiencia, por escucharme
- Como irlandés, y como Secretario, mis puertas siempre estarán abiertas… mike.henigan@bsigroup.com