Ciber-resiliencia, Planes de Contingencia y Continuidad del Negocio

Imagen: pixabay.com

Ramiro Cid

- Region Europe South IT Security Officer en Linde.
- Licenciado en Sistemas de Información. Universidad de Buenos Aires, Argentina.
- Postgrado de Dirección de Empresa. UPF Barcelona School of Management.
- Certificaciones: CISM®, CGEIT®, ISO 27001:2013 LA , ISO 22301:2012 LA, ITIL®(f).
- Profesor de la UPC (Universidad Politécnica de Cataluña). Master Cybersecurity Management.
- Profesor de la APEP (Asociación Profesional Española de Privacidad). Varios cursos de privacidad y ciberseguridad.
- Ponente habitual en eventos en el ICAB (Ilustre Colegio de Abogados de Barcelona) y en organizaciones internacionales como ISACA, itSMF, etc.
- Profesional con más de 20 años de trayectoria profesional en sistemas de información (los últimos 13 en ciberseguridad) en diferentes sectores: Industria química, laboratorio, banca, gobierno, consultoría de sistemas, etc., en diferentes empresas trabajando en Argentina, España y Andorra.

Índice

1. Conceptos principales sobre Ciber-resiliencia	Slide 4
2. DRP y BCP	Slide 11
3. Business Impact Analysis (BIA)	Slide 21
4. ISO/IEC 22301:2019	Slide 27
5. Sistemas de Gestión de la Continuidad del Negocio (SGCN)	Slide 49

1. Conceptos principales sobre Ciber-resiliencia

Definición de conceptos previos

- **Resiliencia:** Este concepto proviene de las características físicas de los materiales (es un concepto físico), donde la característica de recuperación es la capacidad de un material para absorber energía cuando se deforma elásticamente y liberar esa energía al momento de la descarga volviendo a su forma original.

  La elasticidad del material se define como la energía máxima que puede absorber dentro del límite elástico, sin crear una distorsión permanente (es decir conservando su forma).

- **Resiliencia organizacional:** como una analogía, la resiliencia organizacional, es la capacidad de una organización para anticiparse, prepararse y responder y adaptarse a cambios incrementales y disrupciones repentinas para poder sobrevivir y prosperar, pudiendo volver a su operativa habitual con ciertas garantías de éxito luego de pasada una contingencia grave.

¿Cómo debemos entender actualmente la seguridad?

Un estado de **"seguridad"** es un concepto **ideal**, conceptual que está conformado por el uso de los tres procesos:

1) **La prevención de amenazas**
2) **La detección**
3) **La respuesta**

Imagen: pixabay.com

La clave actualmente está en potenciar la última

(no olvidando las otras 2 obviamente).

¿Dónde está el **nuevo perímetro**? -> Posiblemente en los **datos.**

¿Cómo debemos entender actualmente la seguridad?

¿Cuál la nueva filosofía de seguridad?

Pasamos de rechazar ataques a tener **resiliencia organizacional***(1)*, entendiendo que **NO** es posible detener todas las amenazas, por lo que las organizaciones y empresas tienen que poder sobreponerse a los impactos de estas **para poder sobrevivir.**

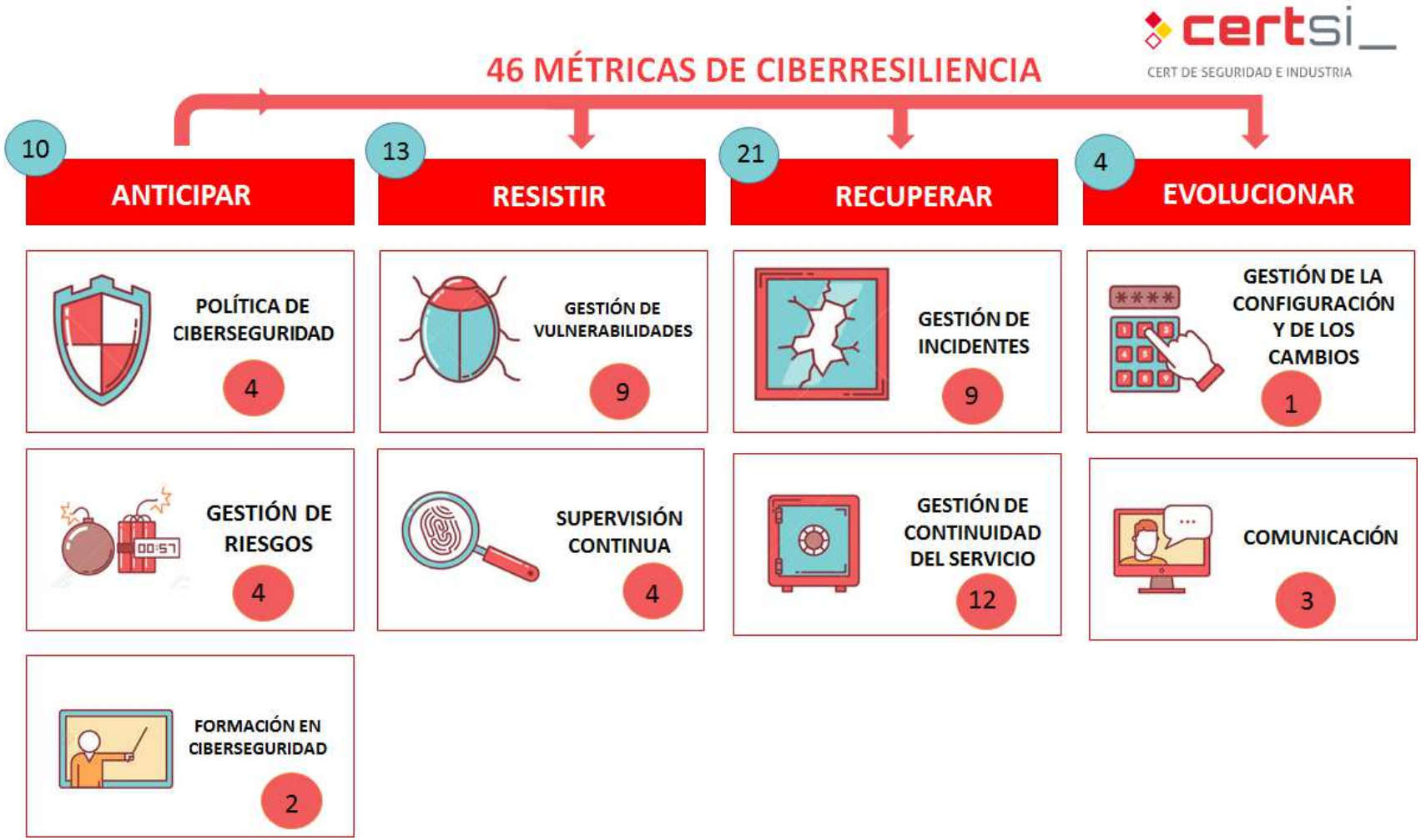
Imagen: pixabay.com

(1) Capacidad de una organización para anticipar, prepararse y responder y adaptarse al cambio incremental y las interrupciones repentinas con el fin de sobrevivir y prosperar.

Riesgos del Siglo XXI vs. Organizaciones resilientes

Aspectos relacionados con el entorno	Características que tienen que tener las organizaciones resilientes
▪ Alta Incertidumbre ▪ Complejidad creciente ▪ Entorno cambiante ▪ Interrelación ▪ Tecnologías disruptivas apareciendo constantemente ▪ Inmediatez (Ej. "*Time to market*" cada vez más corto).	▪ Alta disponibilidad de los servicios críticos que brindan a sus clientes ▪ Alta confiabilidad ▪ Eficiencia operacional bajo estrés constante ▪ Absorber, adaptar, aprender y crecer ▪ Cultura de mejora constante y de aprendizaje de los errores

Métricas de ciber-resiliencia



(1) Fuente CERTSI - INCIBE: https://www.incibe-cert.es/blog/46-metricas-mejorar-ciberresiliencia-servicio-esencial

ISO 22316:2017 - Introducción

Nombre oficial: *"Security and resilience - Organizational resilience - Principles and attributes".*

Creada: por el Comité Técnico "ISO/TC 292 Security and resilience".

Publicada: Marzo 2017 - *URL: https://www.iso.org/standard/50053.html*

Finalidad: Norma enfocada en la mejora de la cultura dentro de las organizaciones en relación con el fomento de la resiliencia.

Contenido: Es el resultado de un largo proceso de desarrollo y representa el consenso global sobre el concepto de resiliencia organizacional. Esta normativa define la **Resiliencia Organizacional** como: "la capacidad de una organización para absorber y adaptarse en un entorno cambiante".

2. DRP y BCP

Diferencia entre DRP y BCP

Disaster Recovery Plan (DRP):

Alcance: Contempla un **entorno limitado**, puede ser una aplicación, un servicio, un proceso crítico, un área, un data center, etc.

Internamente: Son los procedimientos que utilizan los administradores (de sistemas o de una parte del negocio/proceso) relacionados con la restauración de las condiciones normales de flujo de trabajo.

Diferencia entre DRP y BCP

Business Continuity Plan (BCP):

Alcance: Es **toda la organización**. Un BCP **es mucho más que una sumatoria de todos los DRP**, debe tener un BIA(1), un análisis de riesgos, plan de comunicación ante emergencias, un SGCN(2), un comité de SGCN, un manager del SGCN y la implicación completa de dirección.

Internamente: Es lo que los usuarios finales (es decir todos/as) deben realizar para mantener la producción normal de negocios sí el flujo de trabajo se interrumpe.

(1) El análisis de impacto al negocio (Business Impact Analysis o BIA por sus siglas en inglés) es un elemento utilizado para analizar la afectación que podría padecer una empresa u organización como resultado de la aparición de un incidente o un desastre.

(2) SGCN: Siglas de Sistema de gestión de la continuidad del negocio. Es un conjunto de documentos y procedimientos para la administración de la continuidad del negocio. También conocido por BCMS (por sus siglas en inglés de Business Continuity Management System).

Diferencia entre DRP y BCP

Un **DRP** define **cómo volver** a las operaciones normales después de una interrupción del negocio o desastre (es como el "Back office" del SGCN).

Se centra en **"cómo salir de la contingencia lo antes posible"**.

Un **BCP** define **cómo operar** durante una interrupción del negocio de desastres (es como el "Front end" del SGCN).

Se centra en el **"como operar mientras estamos en contingencia"**.

Ambos son necesarios y complementarios. Uno sin el otro es insuficiente para poder garantizar la operatividad y la continuidad de la organización.

Características mínimas de los DRP's y BCP's

Infalible: Debe contar con un correcto plan y adecuada estrategia en relación con las características de la organización, una detallada administración (y su respectiva actualización de los planes) del cambio de tecnología, y que sea probado de forma constante.

Fácil de justificar: Estas soluciones no sólo son redituables cuando existe una contingencia. Además de reducir los riesgos ante un desastre, fortalecen la operación diaria y optimizan procesos existentes (pero para ello es muy importante la puesta en práctica o testeo del SGCN).

Características mínimas de los DRP's y BCP's

Automatizado: En caso de desastre, cabe la posibilidad de que no se pueda acceder a las instalaciones, la infraestructura tecnológica podría no estar disponible y el personal clave podría o no estar en condiciones de operar.

Por todo esto, la importancia de mantener un respaldo y automatización de los procesos desde otra sede y con equipo preparado (distintas soluciones existen en el mercado como veremos en otros *slides* más adelante).

Características mínimas de los DRP's y BCP's

Garantizar la continuidad de las operaciones NO es una opción.

Los clientes, proveedores, empleados y accionistas (puede haber más actores externos como gobierno, colaboradores externos, distribuidores, etc.) esperan una respuesta por parte de la organización en caso de una contingencia sin importar lo que suceda en el exterior.

Por ello, contar con un **Plan de Continuidad de Negocios (BCP) y Recuperación ante Desastres (DRP) no es un gasto sino una inversión**.

Objetivos principales de un DRP

Reservas de memoria: Sí las cintas de *backup* o copias remotas (de contingencia) son llevadas fuera de sitio es necesario controlarlas.

Si se usan servicios remotos de contingencia, se requerirá una conexión de red a la posición remota de reserva (o Internet) para poder contar con los datos en caso de contingencia (se pueden aplicar soluciones de *Cloud computing* también como parte de un *DRP*).

Clientes: La notificación a los clientes sobre el problema (contingencia) que hemos tenido, reduce en gran medida el pánico.

Instalaciones: Teniendo sitios calientes o sitios fríos para empresas más grandes. Instalaciones de recuperación móviles están también disponibles en muchos proveedores.

Objetivos principales de un DRP

Trabajadores con conocimiento: Durante la operación posterior a la contingencia, es posible que a los empleados se les requiera trabajar jornadas más largas y agotadoras.

Debe haber un sistema de apoyo interno para aliviar de tensión (es importante contar por ello con la implicación de RRHH).

La información de negocio: Las copias de seguridad de contingencia deben estar almacenadas completamente separadas de la empresa.

La seguridad y la fiabilidad (integridad) de los datos es clave en ocasiones como estas.

Objetivos principales de un BCP

Los objetivos principales del **Plan de Continuidad del Negocio**, pueden ser resumidos de la siguiente forma:

- **Prevenir:** Limitar al máximo la probabilidad de que tenga lugar cualquier interrupción *(no desde el punto de vista de que la ocurrencia de la amenaza, si no del impacto en caso de que suceda, haciendo un seguimiento y gestión de nuevas amenazas y conseguir una constante reducción del riesgo).*

- **Contener:** Reducir el impacto de cualquier interrupción.

- **Recuperar:** Asegurar una pronta recuperación.

- **Transferir** el riesgo residual*(1)* (seguros, contratos con terceros, etc.).

(1) Riesgo que se calcula luego de la implementación de controles de seguridad, los cuales pueden ser preventivos, reduciendo normalmente la probabilidad de ocurrencia de una amenaza, o remediativos, que suelen reducir el impacto. El riesgo es el resultado del valor del activo, junto con estos otros 2 conceptos, al reducirse, el riesgo intrínseco (previo a los controles) de los activos se reduce.

3. Business Impact Analysis (BIA)

BIA: Aspectos generales

Un ***business impact analysis* (*BIA*)** diferencia funciones/actividades críticas (urgentes) y no críticas (no urgentes) de la organización.

Las funciones **críticas** son aquellas cuya interrupción se considera inaceptable.

Las percepciones de aceptabilidad del riesgo se ven afectadas por el coste de las soluciones de recuperación.

Una función también puede considerarse crítica si así lo establece la ley (*compliance*).

BIA: Aspectos generales

Para cada función crítica (incluidas en el alcance), se asignan dos valores:

***Recovery Point Objective (RPO)*:**

La latencia aceptable de los datos que no se recuperarán.

Ejemplo: ¿Es aceptable que la empresa pierda los últimos 2 días de datos?

***Recovery Time Objective (RTO)*:**

La cantidad de tiempo aceptable para restaurar la función.

Ejemplo: "La empresa requiere que el servicio X quede establecido luego de pasadas 48 horas de ocurrida la incidencia que provocó la contingencia".

Business Impact Analysis (BIA)

Permite decidir que procesos deberán recuperarse con anterioridad en caso de desastre.

Incluye aspectos como:

- Pérdida de ingresos
- Sanciones y multas
- Pérdida de imagen
- Incremento de costes

Imagen: pixabay.com

BIA: Definición de la ISO/IEC 22301:2019

El *business impact analysis* permitirá:

a) **Identificar** actividades que respalden la provisión de productos y servicios.

b) **Evaluar** los impactos a lo largo del tiempo de no realizar estas actividades.

c) **Establecer** plazos prioritarios para reanudar estas actividades a un nivel mínimo aceptable específico, teniendo en cuenta el momento en que los impactos de no reanudarlos serían inaceptables.

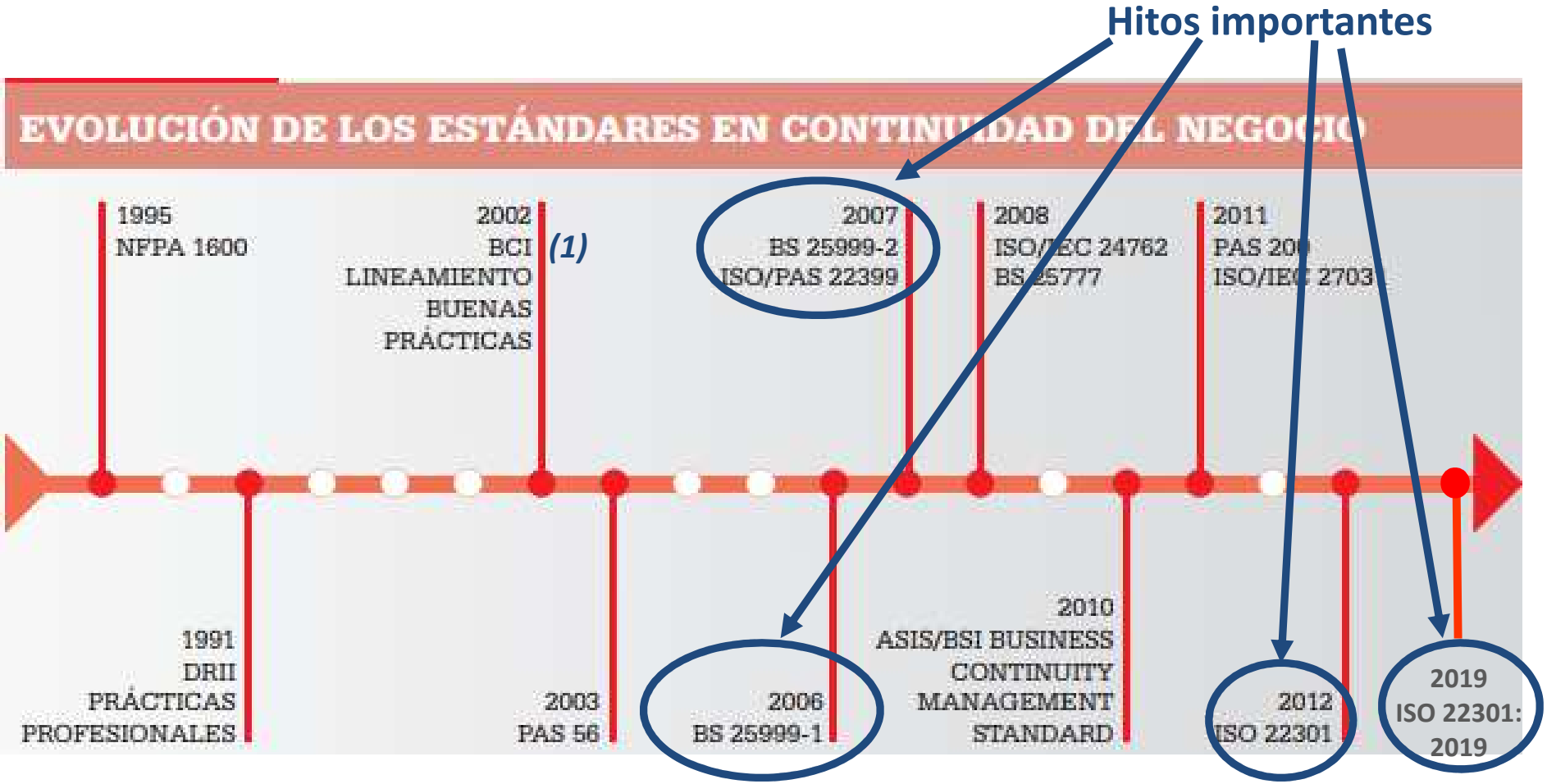
d) **Identificar** las dependencias y los recursos de apoyo para estas actividades, incluidos proveedores, socios externos y otras partes interesadas relevantes.

BIA: Clasificación de las funciones del negocio

Críticos	- Sus funciones no pueden ser ejecutadas a menos que sean remplazadas por recursos idénticos. - No se pueden utilizar métodos manuales. - Costo de interrupción es muy alto.
Vitales	- Sus funciones pueden ser ejecutadas manualmente durante un periodo corto. - Mayor tolerancia a las interrupciones . - Costos de interrupción menores si caída es menor a 3 d.
Sensitivos	- Sus funciones pueden ser ejecutadas manualmente durante un periodo relativamente largo. - Mientras se hace manualmente requiere staff adicional. - Costos de interrupción medios.
NoCríticos	- Sus funciones pueden ser interrumpidas durante un periodo relativamente largo, con poco o ningún costo.

4. ISO/IEC 22301:2019

Historia: Normativas para la creación de los Planes de Continuidad de Negocio



Fuente: gestion.com.do. URL: http://www.gestion.com.do/pdf/018/018-nuevo-estandar-internacional.pdf

(1) The Business Continuity Institute

ISO/IEC 22301:2019 - Introducción

Nombre oficial: *"Security and resilience - Business continuity management systems - Requirements".*

Creada: por el Comité Técnico "ISO/TC 292 Security and resilience".

Publicada: Octubre 2019 - URL: https://www.iso.org/standard/75106.html

Es una normativa certificable.

Finalidad: Marco de referencia para implementar, mantener y mejorar un sistema de gestión de la continuidad del negocio.

Contenido: Esta normativa especifica los requisitos para implementar, mantener y mejorar un sistema de gestión para proteger, reducir la probabilidad de ocurrencia, prepararse, responder y recuperarse de las interrupciones cuando surjan.

ISO/IEC 22301:2019 - Introducción

Imagen: pixabay.com

La **ISO/IEC 22301:2019** cuyo nombre traducido sería “Norma ISO/IEC 22301 - Seguridad y resiliencia - Sistemas de gestión de continuidad del negocio - Requisitos”).

La **ISO/IEC 22301:2019** posee actualmente las versiones en Inglés y francés, siendo la actual versión de la normativa que ha reemplazando la anterior versión ISO/IEC 22301:2012).

Diferencias entre ISO/IEC 22301 y BS 25999-2

La **ISO/IEC 22301:2012** (primera versión ISO que reemplazó a la **BS 25999-2** son 2 estándares bastante similares, pero la norma ISO/IEC 22301:2012 se puede considerar como una actualización de la BS 25999-2 y la **ISO/IEC 22301:2019** la versión actual.*(1)*

	BS 25999-2	ISO/IEC 22301:2012	ISO/IEC 22301:2019
Nombre completo	BS 25999-2 Business Continuity Management - Part 2: Specification	ISO/IEC 22301:2012 Societal security - Business continuity management systems – Requirements	ISO/IEC 22301:2019 Societal security - Business continuity management systems - Requirements
Publicado por	British Standards Institution	International Organization for Standardization	International Organization for Standardization
Fecha de publicación	20/11/2007	15/05/2012	31/10/2019
Requerimientos	56	106	?
Reconocimiento internacional	Aceptada solo en el Reino Unido, pero implementada en todo el mundo.	Internacionalmente aceptado por institutos de estándares en 163 países.	Internacionalmente aceptado por institutos de estándares en 163 países.

(1) Para ver detalles del cambio entre las 2 versiones, consultar:
https://www.linkedin.com/pulse/est%C3%A1ndar-iso-22301-nueva-versi%C3%B3n-2019-para-del-jorge-e-olaya-t-phd

Diferencias entre ISO/IEC 22301:2019 y anteriores versiones de normativas

ISO/IEC 22301:2019 no es tan diferente de la ISO/IEC 22301:2012*(1)* en la mayoría de las áreas de continuidad del negocio, como análisis, estrategia o planificación de impacto empresarial; los cambios más importantes están en la parte de gestión del estándar. **No presenta cambios estructurales importantes**, lo que facilita la transición para las organizaciones que ya dispongan de la certificación ISO/IEC 22301:2012.

ISO/IEC 22301:2012 pone mucho más énfasis en comprender los requisitos que la anterior BS 25999 (posee casi el doble), establecer objetivos y medir el desempeño (KPI*(2)*, KRI*(3)*, KGI*(4)*).

(1) Para más detalles entre la versión ISO/IEC 22301:2019 y la anterior versión consultar aquí: https://www.linkedin.com/pulse/est%C3%A1ndar-iso-22301-nueva-versi%C3%B3n-2019-para-del-jorge-e-olaya-t-phd y aquí: https://dqsiberica.com/2019/02/13/iso-22301/

(2) KPI: Key performance indicators. Los KPIs son una métrica (a pesar de su nombre) aunque no todas las métricas son KPIs.

(3) KRI: Key risk indicators. Es decir "indicadores claves de seguridad". Son KPIs específicos para seguridad que podemos definir como indicador clave que queremos monitorizar y estar alertados en caso de que se supere el valor definido para este.

(4) KGI: Key Goals Indicators. Es decir los "indicadores clave de objetivos". Es un término que se refiere a los indicadores preestablecidos de los objetivos del proceso (metas) que indican lo que se debe lograr mediante un proceso (definen un objetivo). Las métricas usadas deben ser medibles. El término KGI proviene de la metodología de COBIT.

ISO/IEC 22301:2019 - Introducción

Por lo tanto, es aceptado más fácilmente por la alta dirección, lo que a su vez contribuye a la adopción generalizada de esta norma como ISO 27001, ISO 9001 o ISO 14001.

Hasta el año 2018, 4000 empresas en todo el mundo poseían un certificado **ISO/IEC 22301**.*(1)*

Con la publicación de esta nueva versión en 2019 existe un período de transición de tres años. Todos los certificados en la versión 2012 perderían su validez el 30 de octubre de 2022.

(1) Detalles de la nueva normativa ISO/IEC 22301:2019:
https://www.linkedin.com/pulse/est%C3%A1ndar-iso-22301-nueva-versi%C3%B3n-2019-para-del-jorge-e-olaya-t-phd

ISO/IEC 22301:2019: Introducción

“ISO/IEC 22301 Societal security - Business continuity management systems - Requirements”

Este estándar fue creado por expertos líderes en esta área para proporcionar el mejor marco para la gestión de la continuidad del negocio en una organización.

Objeto:

ISO/IEC 22301:2019 especifica los requisitos para **planificar**, **establecer**, **implementar**, **operar**, **supervisar**, **revisar**, **mantener** y **mejorar continuamente** un sistema de gestión documentado para proteger la organización ante las contingencias, trabajando en los pasos necesarios en la preparación de la misma para responder y recuperarse de los incidentes perjudiciales cuando surgen procurando reducir el impacto (intensidad y temporalidad).

ISO/IEC 22301:2019: Introducción

Alcance:

Los **requisitos** especificados en **ISO/IEC 22301:2019** son **genéricos** y están destinados a ser aplicables a **todas las organizaciones**, o partes de las mismas, independientemente del tipo, tamaño y naturaleza de la organización.

El grado de aplicación de estos requisitos depende del entorno operativo y la complejidad de la organización.

¿Quién puede implementar este estándar?

Cualquier organización, grande o pequeña, con o sin fines de lucro, privada o pública.

El estándar está concebido de tal manera que es aplicable a cualquier tamaño o tipo de organización.

ISO/IEC 22301:2019: Aplicabilidad en las organizaciones

Aplicabilidad de la ISO/IEC 22301:2019

Este estándar internacional es aplicable en organizaciones y empresas de cualquier tipo, **no importa el tamaño** o el **sector** de las mismas que deseen:

a) Establecer, implementar, mantener y mejorar un SGCN*(1)*.

b) Asegurar la conformidad con la política de continuidad del negocio establecida.

c) Demostrar conformidad con terceros.

d) Solicitar la certificación o registro de su SGCN por parte de un organismo de certificación acreditado.

e) Hacer una autodeterminación y auto declaración de conformidad con esta norma internacional.

(1) SGCN: Siglas de Sistema de gestión de la continuidad del negocio. Es un conjunto de documentos y procedimientos para la administración de la continuidad del negocio. También conocido por BCMS (por sus siglas en inglés de Business Continuity Management System).

ISO/IEC 22301:2019 - Términos básicos utilizados

- **Recovery Time Objective (RTO)**: El tiempo predeterminado en el que debe reanudarse una actividad, o en la que los recursos deben ser recuperados.

- **Recovery Point Objective (RPO)**: Pérdida máxima de datos, es decir, cantidad mínima de datos que deben restaurarse.

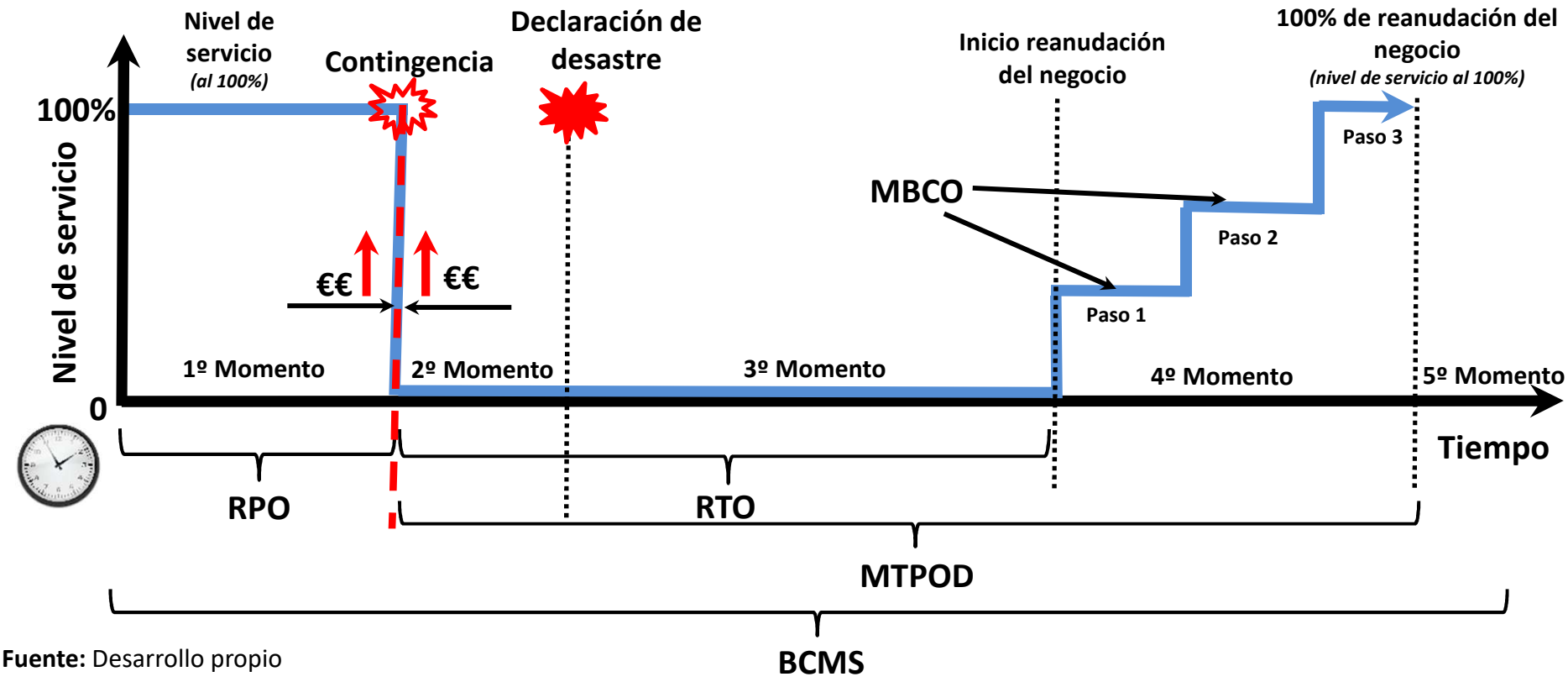
- **Maximum Tolerable Period of Disruption (MTPOD):** La cantidad máxima de tiempo que se puede interrumpir una actividad sin incurrir en daños inaceptables (también conocido como Maximum Acceptable Outage - MAO).

ISO/IEC 22301:2019 - Términos básicos utilizados

- **Business Continuity Management System (BCMS)**: El SGCN parte de un sistema de gestión general que cuida la continuidad del negocio, se planifica, implementa, mantiene y mejora continuamente.

- **Minimum Business Continuity Objective (MBCO)**: El nivel mínimo de servicios o productos que una organización debe producir después de reanudar sus operaciones comerciales.

ISO/IEC 22301:2019 - Esquema temporal del SGCN



Fuente: Desarrollo propio

Referencias:
BCMS: Business Continuity Management System
MTPOD: Maximum Tolerable Period of Disruption
RTO: Recovery Time Objective
RPO: Recovery Point Objective
MBCO: Minimum Business Continuity Objective

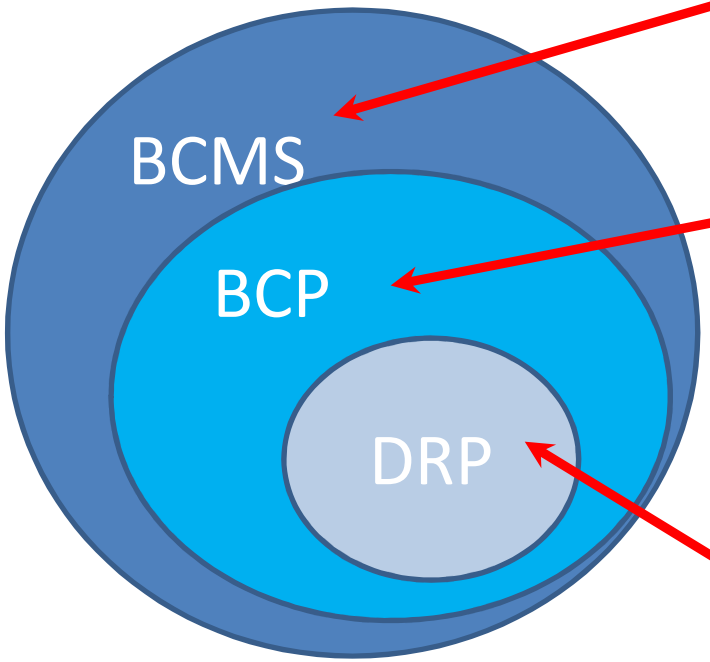
ISO/IEC 22301:2019: ¿Cómo gestionarla?

¿Cómo encaja la continuidad del negocio en la gestión general?

La continuidad del negocio es parte de la gestión general del riesgo en una compañía y tiene áreas superpuestas con la gestión de seguridad y tecnología de la información.

ISO/IEC 22301:2019: Ámbitos

¿Cómo encajan los distintos ámbitos dentro del SGCN?



Sistema de Gestión de la Continuidad del negocio (SGCN) -> ISO/IEC 22301:2019

- Identificación de activos y procesos críticos -> BIA
- Análisis de riesgos
- Pruebas de recuperación del negocio

- DRP (Planes de contingencia)
- Pruebas de recuperación de entornos TI

ISO/IEC 22301:2019 - Documentación obligatoria

Si una organización quiere implementar este estándar, la siguiente documentación es obligatoria:

1. Lista de los requisitos legales, reglamentarios y de otro tipo aplicables.
2. Alcance del BCMS
3. Política de continuidad del negocio
4. Objetivos de continuidad del negocio
5. Evidencia de las competencias del personal
6. Registros de comunicación con las partes interesadas
7. Análisis de Impacto del Negocio (BIA)
8. Evaluación de riesgos, incluido el apetito por el riesgo
9. Estructura de respuesta al incidente
10. Planes de continuidad del negocio
11. Procedimientos de recuperación (DRP's)
12. Resultados de acciones preventivas
13. Resultados de monitorización y medición
14. Resultados de auditoría interna
15. Resultados de la revisión de la administración
16. Resultados de acciones correctivas

Imagen: pixabay.com

Familia ISO 22300 - Normativas relacionadas

ISO/IEC 22301 ha sido desarrollado por el Comité Técnico "ISO/TC 292 Security and resilience"

Otras normativas de la familia ISO/IEC 22301:

- ISO 22300:2018, Societal security - Terminology.
- ISO 22311, Societal security - Video-surveillance - Export interoperability.
- ISO/TR 22312:2011, Societal security - Technological capabilities.
- ISO 22313, Societal security - BCMS - Guidance.
- ISO 22315, Societal security - Mass evacuation.
- ISO/TS 22317:2015, Societal security - BCMS - Guidelines for business impact analysis
- ISO/TS 22318:2015, Societal security - BCMS - Guidelines for supply chain continuity
- ISO 22320:2011, Societal security - Emergency management – Requirements for incident response.
- ISO 22322, Societal security - Emergency management - Public warning.

Beneficios de la gestión de continuidad de negocio ISO/IEC 22301:2019

¿Cuáles son los beneficios de la gestión de la continuidad del negocio ISO/IEC 22301?

1. Identificar y administrar las **amenazas actuales y futuras** para su empresa.
2. Adoptar un **enfoque proactivo** para minimizar el impacto de los incidentes.
3. Mantener las **funciones críticas** en funcionamiento durante los momentos de crisis.
4. Responder a los requisitos de **cumplimiento legal**
5. Contribuir a la **resiliencia organizacional**

Beneficios de la gestión de continuidad de negocio ISO/IEC 22301:2019

¿Cuáles son los beneficios de la gestión de la continuidad del negocio ISO/IEC 22301? *(continuación)*

6. Minimizar el **tiempo de inactividad** durante los incidentes y mejorar el tiempo de recuperación.

7. Reducir los **costes de interrupción**

8. Demostrar **capacidad de recuperación** a clientes, proveedores y solicitudes de licitación.

9. Proteger la **reputación de la organización**

10. Crear una **ventaja competitiva**

Dominios de la ISO/IEC 22301:2019

La **ISO/IEC 22301:2019** es una normativa de sistemas de gestión, en este caso de un Sistema de Gestión de la Continuidad del Negocio conocido también por sus siglas SGCN, que contiene la **nueva estructura de alto nivel y el texto normalizado en ISO**.

La **ISO/IEC 22301** se compone de **10 dominios principales**, comenzando por el alcance, las referencias normativas y los términos y definiciones.

Dominios de la ISO/IEC 22301:2019

0. Introducción
0.1 General
0.2 Beneficios de un Sistema de Gestión de la Continuidad del Negocio NEW
0.3 El ciclo Planificación-Implementación-Verificación-Mantenimiento (PDCA)
0.4 Contenido de este documento

1. Alcance

2. Referencias a otras normativas

3. Términos y definiciones

4. Contexto de la organización
4.1 Conocimiento de la organización y de su contexto
4.2 Conocimiento de las necesidades y expectativas de las partes interesadas
4.3 Determinación del alcance del sistema de gestión
4.4 Sistema de gestión de la continuidad del negocio

5. Liderazgo
5.1 Liderazgo y compromiso
5.2 Política
5.3 Funciones, responsabilidades y autoridades

6. Planificación
6.1 Acciones para tratar riesgos y oportunidades
6.2 Objetivos de la continuidad del negocio y planes para alcanzarlos
6.3 Planificación de cambios en el sistema de gestión de continuidad del negocio NEW

7. Soporte
7.1 Recursos
7.2 Competencia
7.3 Concienciación
7.4 Comunicación
7.5 Información documentada

8. Operación
8.1 Planificación operativa y control
8.2 Análisis de impactos en el negocio y evaluación de riesgos
8.3 Estrategia de la continuidad del negocio y soluciones
8.4 Planes y procedimientos de la continuidad del negocio NEW
8.5 Programa de pruebas
8.6 Evaluación de la documentación y las capacidades de continuidad del negocio NEW

9. Evaluación del desempeño
9.1 Monitorización, medición, análisis y evaluación
9.2 Auditoría interna
9.3 Revisión por parte de la dirección

10. Mejora
10.1 No conformidades y acciones correctivas
10.2 Mejora continua

Bibliografía

Referencia:

NEW *= Nuevo respecto a la pasada edición ISO/IEC 22301:2012*

ISO/IEC 22301: Ciclo PDCA aplicado al proceso de BCP

Fuente: gestion.com.do. URL: http://www.gestion.com.do/pdf/018/018-nuevo-estandar-internacional.pdf

5. Sistemas de Gestión de la Continuidad del Negocio (SGCN)

Definición de SGCN según ISO 22301:2019

Concepto

Un **Sistemas de Gestión de la Continuidad del Negocio (SGCN)** siguiendo la definición de la ISO/IEC 22301:2019 es parte del sistema de gestión general que establece, implementa, opera, monitorea, revisa, mantiene y mejora la continuidad del negocio.

Similar a PDCA (Círculo de Deming)

El SGCN debe integrase dentro de otros SG (SGSI, Sistemas de gestión de la calidad, del servicio, etc.)

El sistema de gestión incluye estructura organizativa, políticas, actividades de planificación, responsabilidades, procedimientos, procesos y recursos.

Sistemas de Gestión de la Continuidad del Negocio (SGCN) según ISO/IEC 22301:2019

Desde su establecimiento (el SGCN) hasta el momento de obtención de la certificación (en caso de ser este el deseo de la organización), se deben **llevar a cabo distintos aspectos relacionados con la monitorización y seguimiento permanentes** que aseguran el mantenimiento continuo del SGCN.

La **organización debe establecer, implementar, mantener y mejorar continuamente un SGCN**, incluidos los procesos necesarios y sus interacciones, de acuerdo con los requisitos de esta Norma Internacional.

Cómo poner en funcionamiento el SGCN en la organización: ISO/IEC 22301:2019

La **ISO/IEC 22301:2019** da lugar a la implantación de un Sistema de Gestión de la Continuidad del Negocio (SGCN), el cual permite a las empresas controlar continuamente los riesgos de su negocio y saber cuál es el nivel de preparación ante situaciones imprevisibles con el que cuenta la misma para hacerle frente.

Imagen: pixabay.com

Cómo poner en funcionamiento el SGCN en la organización: ISO/IEC 22301:2019

Los requisitos establecidos en la norma **ISO/IEC 22301:2019** para programar, implantar, especificar, elaborar, controlar, mejorar continuamente un SGCN son comunes y procuran ser de aplicación a todas las organizaciones con independencia del tipo, naturaleza o tamaño.

La aplicación de estos requisitos depende de la complejidad de la empresa y del entorno operativo.

Cómo poner en funcionamiento el SGCN en la organización: ISO/IEC 22301:2019

El SGCN ayuda a reducir el impacto de posibles incidentes en el negocio:

- Disminuyendo costes generales.
- Garantizando la dirección corporativa.
- Cumpliendo con las exigencias aplicables.
- Haciendo que la cadena de suministro sea cada vez más sólida y fiable.
- Protegiendo y haciendo que su imagen corporativa adquiera más prestigio.
- Creando un ambiente de seguridad y franqueza con los empleados, clientes, proveedores e interesados.

Cómo poner en funcionamiento el SGCN en la organización: ISO/IEC 22301:2019

La **ISO/IEC 22301:2019** hace que la estandarización de la continuidad de negocio se produzca añadiendo:

- Perspectivas claras y precisas sobre la dirección.
- Mayor redundancia en la creación de objetivos, búsqueda del desempeño y de los indicadores.
- Proyección y organización de los recursos necesarios con más detenimiento para la continuidad del negocio.

Sistemas de Gestión de la Continuidad del Negocio (SGCN) según ISO/IEC 22301:2019

Hitos en el desarrollo del SGCN:

1. Análisis de impacto en el negocio (*BIA*).
2. Planes de continuidad del negocio y recuperación ante desastres (DRP).
3. Elaboración del manual del sistema de gestión.
4. Establecimiento de indicadores para medir la eficacia (métricas e indicadores).

Sistemas de Gestión de la Continuidad del Negocio (SGCN) según ISO/IEC 22301:2019

Hitos en el desarrollo del SGCN: *(continuación)*

5. Formación y concienciación en seguridad.
6. Auditoría interna SGCN.
7. Acompañamiento en la fase de certificación.
8. Oficina técnica/servicio de oficial de seguridad *(normalmente liderada por el CISO).*

Cómo poner en funcionamiento el SGCN en la organización: ISO/IEC 22301:2019

El proceso de planificación de continuidad del negocio se realiza de la siguiente manera:

1. Involucrando a la dirección en los procesos de un SGCN.

2. Transmitir la necesidad de establecer un SGCN.

3. Instaurar un Comité de Proyecto.

4. Reconocer y efectuar los requerimientos presupuestales.

Cómo poner en funcionamiento el SGCN en la organización: ISO/IEC 22301:2019

El proceso de planificación de continuidad del negocio se realiza de la siguiente manera: *(continuación)*

5. Desarrollar y combinar las actividades de implementación del SGCN.

6. Reconocer los grupos de planificación y sus respectivas obligaciones o responsabilidades.

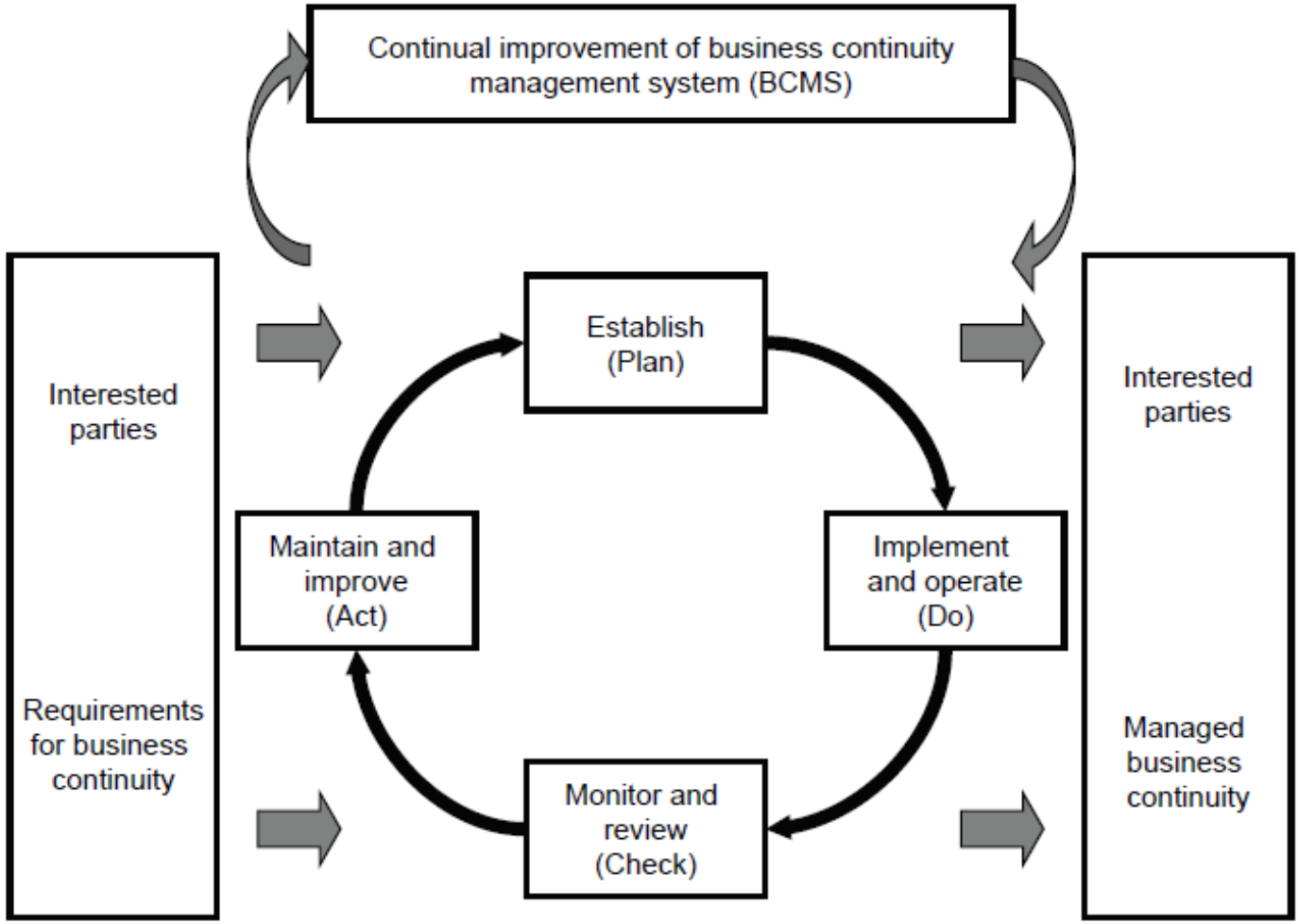
7. Dar respuesta a las exigencias de la dirección y de la documentación de los procesos del SGCN.

8. Lograr la aprobación de la evolución del proyecto.

Desarrollo de los PCN

Nº	Función	Responsable	Resultado
1	Considerando el Análisis de Riesgos. Describir el esquema de los PCN.	Comité Seguridad Responsable Seguridad	Estructura PCN PCN a desarrollar por los responsables PCN
2	Para cada PCN describir los puntos y procesos de cada uno de ellos.	Responsable de los PCN	PCN Registros definitivos
3	Revisar los PCN para coordinar acciones y asegurar la coherencia.	Comité seguridad Responsable Seguridad	Aprobación formal de los planes
4	Establecer y aprobar la programación de las pruebas y revisiones de los PCN.	Comité seguridad Responsable seguridad	Aprobación formal de los planes de pruebas
5	Asegurar la disponibilidad de los recursos necesarios para aplicar los planes.	Responsables del PCN	Recursos disponibles
6	Distribución de los planes y formación del personal.	Responsable de los PCN	Conocimiento y preparación del personal implicado
7	Desarrollo de pruebas y revisiones.	Responsable de PCN	Mejora y mantenimiento de los PCN

ISO/IEC 22301:2019 - PDCA



PDCA model applied to BCMS processes

ISO/IEC 22301:2019 - PDCA

Plan (establecer)	Establecer una política de continuidad del negocio, objetivos, metas, controles, procesos y procedimientos relevantes para mejorar la continuidad del negocio con el fin de entregar resultados que se alineen con las políticas y objetivos generales de la organización.
Hacer (implementar y operar)	Implementar y operar la política de continuidad del negocio, controles, procesos y procedimientos.
Verificar (monitorear y revisar)	Monitorear y revisar el desempeño en contra de la política y objetivos de continuidad del negocio, informar los resultados a la gerencia para su revisión, y determinar y autorizar acciones para remediar y mejorar.
Actuar (Mantener y mejorar)	Mantener y mejorar el SGCN mediante la adopción de medidas correctivas, sobre la base de los resultados de la revisión por parte de la administración y la nueva evaluación del alcance del SGCN y las políticas y objetivos de continuidad del negocio.

Alcance del SGCN según ISO/IEC 22301:2019

La organización deberá:

a) Establecer las partes de la organización que se incluirán en el SGCN.

b) Establecer los requisitos SGCN, teniendo en cuenta la misión de la organización, los objetivos, las obligaciones internas y externas (incluidas las relacionadas con las partes interesadas) y las responsabilidades legales y reglamentarias.

c) Identificar productos y servicios y todas las actividades relacionadas dentro del alcance del SGCN.

Alcance del SGCN según ISO/IEC 22301:2019

La organización deberá: *(continuación)*

d) Tener en cuenta las necesidades e intereses de las partes interesadas, tales como los clientes, los inversores, los accionistas, la cadena de suministro, los aportes y necesidades públicas, comunitarias y las expectativas e intereses (según corresponda).

e) Definir el alcance del SGCN en términos de y apropiado al tamaño, naturaleza y complejidad de la organización.

¿Preguntas?

Imagen: pixabay.com

¡Muchas gracias!

Ramiro Cid

CISM, CGEIT, ISO 27001 LA, ISO 22301 LA, ITIL

ramiro@ramirocid.com
www.linkedin.com/in/ramirocid
ramirocid.com
es.slideshare.net/ramirocid
@ramirocid
www.youtube.com/user/cidramiro