



Los Lunes del Instituto de Auditores Internos

www.auditoresinternos.tv

#LosLunesIAI - @Auditorinterno

LOS LUNES 
EMPIEZA BIEN LA SEMANA



Instituto de
Auditores Internos
de España

**La crisis COVID19:
el papel de Auditoría Interna en la
resiliencia del negocio**

30 de marzo de 2020

Juan Ignacio Sánchez Chillón

Lead Auditor en CN – ISO22301

CISA, CRISK, CPP

Master en Auditoría Informática

Agenda

- 1 ANTECEDENTES
- 2 ÁMBITO DE ACTUACIÓN
- 3 ASPECTOS ESPECÍFICOS DE LA CRISIS COVID-19
- 4 ROL DEL AUDITOR INTERNO EN LA RESILIENCIA DEL NEGOCIO
- 5 Y ... OTROS

ANTECEDENTES

Antecedentes



En **abril de 2015**, celebramos una jornada relativa al papel del auditor interno en relación con los **Planes de Continuidad de Negocio**.

Planes que sirven a las organizaciones para **recuperar su operativa** en caso de desastres, como incendios, inundaciones, terremotos o pandemias.

Ya entonces mencionábamos la **pandemia** como un escenario ante el cual las organizaciones debían estar preparadas.

Las amenazas pueden materializarse en cualquier organización y, frente a ellas, es necesario adoptar una **actitud preventiva** para tratar de mitigar el impacto que puedan provocar y evitar la interrupción de la actividad de la organización.

Una de las conclusiones fue:

“Contar con un Plan de Continuidad de Negocio pasará de ser una necesidad a una obligación”

Antecedentes



Líneas **directrices** que inspiran el desarrollo de la Continuidad de Negocio :

- actitud **preventiva**
- mitigar el **impacto**

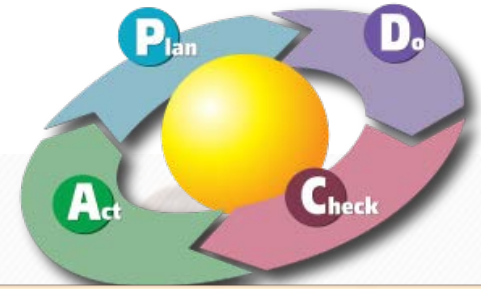
Pero también hay que tener en consideración que cada vez en más **países** y **sectores de actividad** es una **obligación**.

La **presión regulatoria** se ha ido incrementando, lo que hace que las competencias del modelo de seguridad de la compañía abarque:

- ✓ sistemas de información
- ✓ riesgos de seguridad
- ✓ personas
- ✓ instalaciones
- ✓ procesos



Antecedentes



Los planes de continuidad de negocio han **evolucionado** para adaptarse a una realidad cambiante.

Estableciendo un proceso de mejora continua que lleva a que en el siglo XXI ya no hablemos de Planes de Continuidad sino de **Sistemas de Gestión de Continuidad de Negocio.**



CN es algo **vivo**, donde el papel de la **Auditoría Interna** es fundamental, contribuyendo a la pervivencia de la compañía, pues no olvidemos que se trata de una **función clave** en el buen gobierno corporativo

ÁMBITO DE ACTUACIÓN

¿Qué debemos proteger en la empresa?



¿Qué impactos se pueden producir?

La **materialización de un desastre** puede repercutir negativamente en las **actividades** y provocar la interrupción de los procesos, causando **impactos** en la operativa normal:



LEGALES O CONTRACTUALES



EN LA REPUTACIÓN



EN PROCESOS INTERNOS



EN PROCESOS EXTERNOS



ECONÓMICOS

¿Qué es la Continuidad de Negocio?

La **Continuidad de Negocio** actúa desde la declaración de un desastre hasta la vuelta a la normalidad de la actividad, reduciendo su impacto sobre los procesos de negocio

“La Continuidad de Negocio es la capacidad de una Organización para continuar realizando la entrega de productos o servicios a niveles predefinidos aceptables después de un incidente disruptivo”

[Fuente: Norma ISO 22300]

Es un proceso basado en la mejora continua



¿Qué es un Plan de Continuidad de Negocio?

El Plan de **Continuidad** de Negocio es un proceso que **analiza** los posibles efectos de las amenazas para la operativa de negocio y las consecuencias para la compañía en caso de materializarse...

... entra en acción cuando la amenaza se ha convertido en una realidad y pone a prueba la capacidad para:

- **reducir** el impacto
- **mantener** su operación y
- **retornar** a la normalidad, en el menor tiempo posible



¿Qué es un Plan de Continuidad de Negocio?

Beneficios:



- Personas
- Reputación
- Imagen corporativa
- Requisitos Legales
- Grupos de interés



- Conocimiento del negocio
- Imagen de Marca



- de impactos



- de funciones críticas



- de la competitividad

¿Qué es un Plan de Continuidad de Negocio?

Análisis, elementos e impactos:

En el Plan de Continuidad de Negocio se **analizan los elementos** que la entidad necesita para desarrollar su actividad:



1. Edificios (centros de trabajo)

2. Personas

3. Tecnología

4. Proveedores

Se **valora el impacto** que supone la paralización de cada uno de sus procesos por indisponibilidad. Se **clasifican** los procesos según su **criticidad** y se **diseñan las soluciones** para hacer frente a su interrupción y **recuperar la actividad**.

Un Plan de Continuidad de Negocio está finalizado cuando ha sido **probado** y ha **funcionado**.

¿Qué es un Plan de Continuidad de Negocio?

En definitiva, ya no hablamos de PCN sino de SGCN



Desarrollo del Plan de Continuidad de Negocio



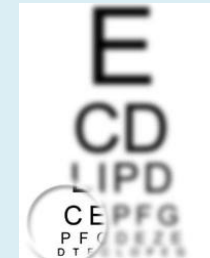
Estrategias de recuperación de la actividad



Formación



El Plan tiene que estar actualizado



Probar el Plan para saber que funciona



Revisar el Plan periódicamente

ASPECTOS ESPECÍFICOS DE LA CRISIS COVID-19



Identificación de Escenarios de Crisis



1.- Identificación de activos

2.- Identificación de amenazas

3.- Identificación de medidas preventivas

4.- Evaluación para la Continuidad de Negocio

▪ Infraestructuras



▪ Tecnología



▪ RRHH



▪ Proveedores



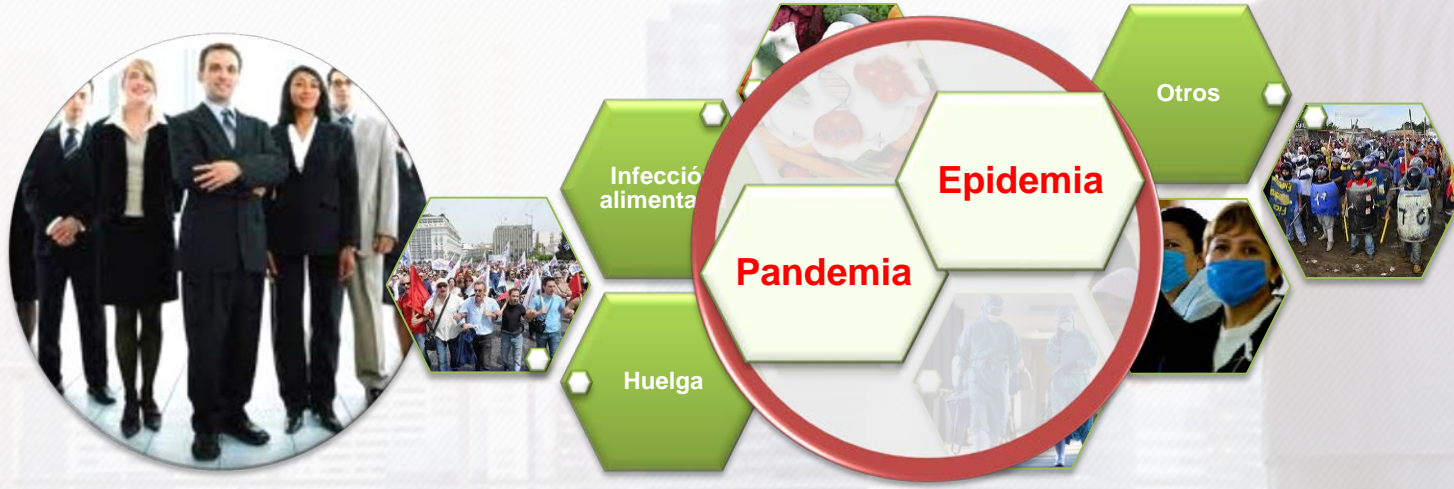
Este análisis supone el **diseño** hipotético de todos los **escenarios posibles de desastre** y la realización de una **estimación del impacto** que ocasionaría la materialización de una amenaza sobre ellos.

Identificación de Escenarios de Crisis



Principales amenazas

R
R
H
H



Análisis de impacto en el negocio - BIA



Cimientos de la Gestión de Continuidad de Negocio



Análisis de Impacto en el Negocio

Identifica y **cuantifica los impactos** sobre el negocio de una posible interrupción en los procesos de la **compañía** y ofrece los datos a partir de los que se determinarán las estrategias de continuidad adecuadas.

Análisis de Requisitos de Continuidad

Recopila información acerca de los **recursos necesarios** para **continuar** las actividades de negocio en caso de contingencia, al nivel suficiente para satisfacer las obligaciones y las necesidades **de la compañía**.

Análisis de impacto en el negocio - BIA



Obtención de información sobre procesos y actividades



Flujos de entrada y salida

- Quién genera la información
- A quién se remite
- Por qué medios
- Identificación de proveedores necesarios

Dependencias de la actividad

- Interrelaciones entre actividades

Recursos asignados a la actividad

- RR.HH. (internos y externos)
- Tecnológicos
- Otros (teléfonos, impresoras, etc.)
- Aplicaciones

En situación de:

- Normalidad
- Desastre

Registros vitales

Estrategias de recuperación



... con los resultados del BIA, hay que tomar decisiones...



Factores a considerar para la selección de estrategias:

- ✓ **Actividades** a recuperar
- ✓ **Tiempos de recuperación** identificados en el BIA
- ✓ **Mejor manera** de recuperar
- ✓ Las **distintas opciones**
- ✓ ... **Decisión de la Dirección**



Estrategias de recuperación



... en una PANDEMIA: indisponibilidad de RRHH





Acciones y recursos necesarios para gestionar un incidente



Gestión de Crisis

Objetivo

Definir los pasos que permitan afrontar de forma **sistemática y homogénea** una situación de posible crisis en un determinado centro de trabajo

Alcance

- ❖ Todos los centros de trabajo
- ❖ Un Manual para cada centro

Como respuesta ante cualquier tipo de incidente en los centros de trabajo, se adoptarán **Procedimientos de Gestión de Situaciones de Crisis: Alerta, Evaluación y Declaración de Desastre**

ROL DEL AUDITOR **INTERNO** EN LA RESILIENCIA DEL NEGOCIO

Rol del auditor interno en la RESILIENCIA del negocio



Punto de Partida



El PCN es algo vivo, donde el papel de la Auditoría Interna es fundamental, pues contribuye a la pervivencia de la compañía.

La Auditoría Interna, como función clave del buen gobierno, debe evaluar y revisar los elementos involucrados en la continuidad de negocio, desde los requisitos a tener en consideración hasta la capacidad de respuesta ante la materialización de una crisis que pudiera interrumpir la actividad, reduciendo la probabilidad de que se produzcan y garantizando la recuperación de las actividades.

Y atender los requisitos legales y regulatorios.



Rol del auditor interno en la RESILIENCIA del negocio



REFERENCIA: Familia de normas ISO 22300

ISO 22300

Protección y Seguridad de los Ciudadanos:

Terminología



ISO 22301

Protección y Seguridad de los Ciudadanos:

SGCN-
Especificaciones



ISO 22313

Protección y Seguridad de los Ciudadanos:

SGCN-
Directrices



ISO 22320

Protección y Seguridad de los Ciudadanos:

Gestión de Emergencias

Requisitos de respuesta a incidentes



ISO 22398

Protección y Seguridad de los Ciudadanos:

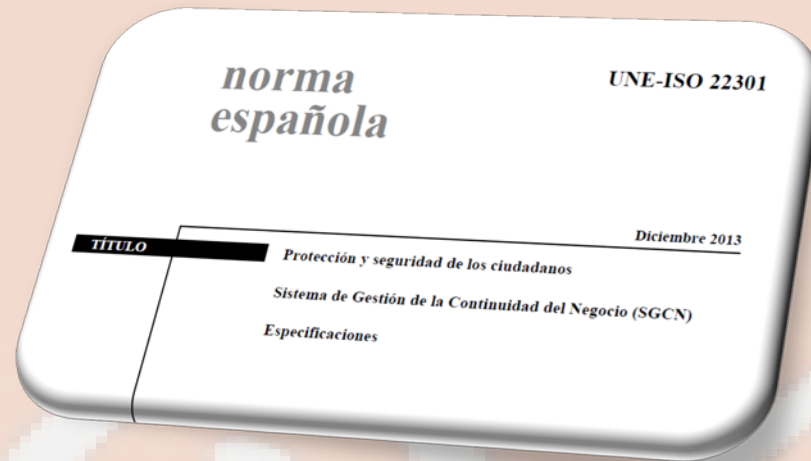
Guidelines for exercises



Rol del auditor interno en la RESILIENCIA del negocio



ISO 22301: Auditoría Interna de la Continuidad de Negocio



Primer estándar internacional que, a nivel mundial, establece la metodología para implantar un SGCN; y responder y recuperarse de eventos disruptivos.

Los requerimientos en la ISO22301 son genéricos, con el objetivo de que sean aplicables a todo tipo y tamaño de organización



Rol del auditor interno en la RESILIENCIA del negocio

ISO 22301: Cláusulas Clave en Auditoría de CN

Cláusula 4

Contexto: Identificar el **alcance**, teniendo en cuenta sus objetivos estratégicos, sus productos y servicios, su tolerancia al riesgo y los objetivos de sus partes interesadas

Cláusula 5

Liderazgo: La Alta Dirección debe demostrar un **compromiso continuo** con el Sistema de Gestión de la Continuidad de Negocio

Cláusula 6

Planificación: Se establecen los **objetivos estratégicos** y **principios** que deben inspirar el SGCN

Cláusula 7

Soporte: **Recursos** adecuados, Sistemas de comunicación (interna y externa), Sistema de Gestión de la documentación

Cláusula 8

Operación: Análisis de Impacto en el Negocio, Evaluación del riesgo, Estrategias de Recuperación y procedimientos de CN, Ensayos y pruebas

Cláusula 9

Evaluación del desempeño: Sistemas de seguimiento, Sistemas de medición, Sistemas de evaluación: **Auditoría Interna**

Cláusula 10

Mejora: Acciones que aumentan la eficacia y la eficiencia del SGCN

Rol del **auditor interno** en la RESILIENCIA del negocio



ISO 22301: Documentación requerida

1. Lista de requerimientos legales, normativos y de otra índole
2. Alcance del SGCN
3. Política de la Continuidad de Negocio
4. Objetivos de la Continuidad de Negocio (alineamiento estratégico)
5. Evidencias de la competencia del personal
6. Registros de comunicación con las partes interesadas
7. Análisis de Impacto en el Negocio (BIA)
8. Evaluación de Riesgos
9. Planes de Continuidad de Negocio (Diseño e Implantación de ER)
10. Procedimientos de recuperación
11. Resultado de acciones preventivas
12. Resultados de supervisión y medición
13. Resultados de **Auditoría Interna**
14. Revisión por parte de la Dirección
15. Ejecución de acciones correctivas

Y ... OTROS

NOTICIAS: virus informático



SER
PROGRAMAS Y PODCAST EMISORAS DEPORTES BOLETÍN INFORMATIVO ▶
CORONAVIRUS COVID-19

La Policía detecta un intento de ataque por email para "romper todo el sistema informático de los hospitales"

Personal sanitario ha recibido correos electrónicos con un virus, ha explicado el portavoz de la Policía en rueda de prensa

El DAO de la Policía también alerta de la detección de 200 bulos sobre el coronavirus

> Sigue EN DIRECTO la última hora sobre el coronavirus



Coronavirus · Bulos Internet · Coronavirus Covid-19 · Policía Nacional

CADENA SER | Madrid | 23/03/2020 - 12:11 h. CET

Personal sanitario ha recibido en las últimas horas **correos electrónicos** con un virus destinados a atacar los sistemas informáticos de los hospitales. Según ha explicado el Director Adjunto Operativo (DAO) de la Policía Nacional en rueda de prensa han detectado **"un virus muy peligroso"** enviado por correo electrónico a personal sanitario destinado a "romper todo el sistema informático de los hospitales", además de haber detectado **"más de 200 bulos** para crear miedo y pánico en la población".

LO MÁS VISTO



El Ejército localiza a ancianos en residencias 'conviviendo' con

cadáveres



La Policía detecta un intento de



Estudio del impacto económico COVID-19 en las empresas

Publicada el 20 de marzo de 2020



Continuum Instituto de Continuidad de Negocio
Junta del Instituto en Instituto de Continuidad de Negocio

4 artículos [✓ Siguiendo](#)

El Análisis de Impacto para el Negocio, también conocido como BIA, por su acrónimo en inglés, es una de las etapas que se cubren durante la planificación de la continuidad en las operaciones de la empresa.

En esta etapa, el responsable de continuidad de negocio plantea los distintos escenarios de contingencia a los responsables de las diferentes líneas de actividad, y entre otras cuestiones, les pide que hagan un cálculo aproximado del impacto económico que se derivaría para la empresa como consecuencia de una eventual paralización o degradación de las actividades productivas que dirigen, en el caso de que se concretaran alguno de dichos escenarios de contingencia. Este impacto puede ser sobre activos tangibles como personas y bienes, o sobre intangibles, como la reputación o imagen de marca.

Entre los escenarios de contingencia que suelen plantearse durante la realización de un BIA se encuentra la indisponibilidad del personal, bien sea propio o de terceros que colaboran en procesos críticos.

CONTINUAM: infografía protocolos de actuación



Protocolo INTEGRAL COVID 19

Objetivos

- 1) **Minimizar la exposición** personal manteniendo la actividad económica estratégica
- 2) **Proteger** a la población más vulnerable

Segmentación de la Población

Determinar el potencial transmisor individual según las actividades desarrolladas para aplanar la curva de contagio

Nivel de Exposición Social	+	<p>PUNTOS CALIENTES Labores de cercanía imprescindibles</p> <ul style="list-style-type: none"> - Limitación de contactos  <p>Supermercados, homedelivery, farmacias</p>	<p>PERSONAL CRÍTICO Estamos en vuestras manos</p> <ul style="list-style-type: none"> - Reducir su número al máximo - Garantizar canales de movilidad limpios - Virtualización de actividades  <p>Autoridad, logística material, personal sanitario</p>
	-	<p>LA NUEVA NORMA La vida común durante la pandemia</p> <ul style="list-style-type: none"> - Mejora de protocolos - Reparto de tareas - Desarrollo actividad digital - Células coordinadas*  <p>Unidades familiares y teletrabajo</p>	<p>MÍNIMO RIESGO Protéjendo a los más vulnerables</p> <ul style="list-style-type: none"> - Identificación y asignación temprana - Confinamiento como "cuidador"  <p>Personas de riesgo con cuidador confinado o con mínima exposición</p>
		-	+
		Nivel de Adopción de los Protocolos de Contacto	

Líneas de ACCIÓN URGENTE

Responsabilidad de las autoridades y de toda la sociedad civil

- Desarrollo vida **digital** y virtual.
- Facilitar la **minimización de contactos**
- Incrementar la **adopción de protocolos**
- Limitar **actividades prescindibles**
- Deplegar **servicios de limpieza protocolizados** para todos los "puntos calientes" y canal de paso activos
- Fortalecimiento del **sistema inmune**. Alimentación y hábitos diarios
- Atender las **recomendaciones sanitarias oficiales**

PROTOCOLO DOMÉSTICO

Creación de Zona Limpia

①

Asegurar al máximo la limpieza de espacios y puntos de contacto.

Zonas de entrada y salida consideradas zonas de riesgo.

Ventilación diaria

Limpieza y colada regulares

Colutorio bucal, buena alimentación

Fuera de Zona Limpia

③

Limitar contactos con superficies fuera de zona limpia

Mantener distancia de seguridad con gente

Desinfectar habitáculo de vehículo propio

Limitar el uso del móvil. Nunca compartirlo

Protocolos específicos

Salida de Zona Limpia

②

Lavarse las manos y ponerse mascarilla o equivalente.

Ponerse zapatos en la puerta o zona de salida y no en la zona limpia

Disponer de desinfectante portátil

Entrada a Zona Limpia

④

Minimizar contactos con superficies a la entrada.

Lavarse las manos con agua y jabón o gel de alcohol y quitarse la ropa en el baño.

Desinfectar móvil.

Como último paso, quitarse la mascarilla y guardarla en sitio contenido.

¿Preguntas?



Muchas Gracias

¡¡Gracias!!

Síguenos en

www.audidoresinternos.es



@Auditorinterno

Instituto de Auditores Internos de España