ROL DEL AUDITOR EN LA EVALUACIÓN AL PLAN DE CONTINUIDAD DEL NEGOCIO.

Luis Fernando Millán Morales[1]

Resumen

Las empresas siempre han estado y estarán expuestas a eventos disruptivos, los cuales, en el peor de los casos pueden ocasionar el cierre de sus operaciones, por eso, es muy importante que cuenten con un plan de continuidad del negocio, el cual, si se realiza utilizando como marco de referencia la norma ISO 22301, se vuelve una herramienta estratégica para que la empresa pueda garantizar la continuidad de sus operaciones y el trabajo a largo plazo.

El rol del auditor es de suma importancia para que el plan de continuidad del negocio se encuentre lo más afinado posible, brindando su consejo y evaluación sobre los puntos críticos del mismo, en componentes como, el análisis de impacto del negocio, en el plan de recuperación de desastres, ajustes en los simulacros y la verificación de las mejoras incorporadas en el plan

Palabras Claves Plan de Continuidad del Negocio, Auditoria, Evaluación

[1] Luis Fernando Millán Morales, Ingeniero de Sistemas. Estudiante de la Especialización en Auditoría de Sistemas de la Universidad Antonio Nariño.
E-Mail: fermillanmorales@hotmail.com

Abstract

Companies have always been and will be exposed to disruptive events, which, in the worst case can cause the closure of their operations, therefore, it is very important that they have a business continuity plan, which, if carried out using the ISO 22301 standard as a reference framework, it becomes a strategic tool for the company to guarantee the continuity of its operations and long-term work.

The role of the auditor is of utmost importance so that the business continuity plan is as fine-tuned as possible, providing advice and evaluation on its critical points, in components such as business impact analysis, in the business plan disaster recovery, drills adjustments, and verification of improvements incorporated into the plan

Key words Business Continuity Plan, Audit, Assessment

Introducción

En el presente artículo sobre el rol del auditor en la evaluación al plan de continuidad del negocio, se describe de una manera sencilla y somera, los conceptos de auditoria de sistemas, auditor de TI, el rol de TI, el rol del auditor en el plan de continuidad del negocio, el plan de continuidad del negocio y sus componentes.

El plan de continuidad del negocio (PCN), es una valiosa herramienta en cualquier organización, la cual le puede ayudar a seguir con sus operaciones cuando ésta enfrente un evento disruptivo y por esta razón, es muy importante que el auditor tenga un concepto claro de cuáles son los temas a auditar en el PCN, y que, desde su rol y con su experiencia, contribuya a la mejora del mismo.

Se consideran los puntos más generales o globales a auditar en un plan de continuidad del negocio, independientemente del tipo de organización y de su tamaño.

Metodología

El método de investigación utilizado para la elaboración del presente artículo, es el método cualitativo y el tipo es el explicativo descriptivo, a través del cual se pretende conocer e interpretar los aspectos que debe tener en cuenta el auditor de sistemas, para evaluar la correcta aplicación del plan de continuidad de negocio en una organización.

Se utilizará como herramienta de soporte la norma ISO 22301, la cual servirá como guía al auditor para evaluar la correcta actualización, aplicación y la efectividad del plan de continuidad del negocio en la organización.

Resultados y discusiones.

La auditoría de sistemas

La auditoría de sistemas, constituye una evaluación de la gestión de los métodos y procedimientos de uso en una organización, relacionados con el procesamiento de la información, desarrollo de sistemas e instalaciones de infraestructura tecnológica; como parte de la evaluación del control interno.

Pretende identificar los aspectos susceptibles de mejora o de eliminación, tendientes a ayudar a la organización a lograr sus objetivos, alineados con la gestión corporativa, la visión, la misión y los objetivos organizacionales. El auditor de sistemas, tiene funciones como las de analizar y evaluar la infraestructura tecnología en una organización, para asegurar que los procesos y sistemas están funcionando con eficiencia y exactitud, mientras mantiene el cumplimiento de seguridad y de regulaciones.

También identifica temas que deben estar cubiertos por la auditoria, especialmente, lo relacionado con gestión de riesgos, siempre bajo los criterios de integridad, objetividad y confidencialidad.

Para lograr lo anterior, el auditor de TI, debe poseer ciertas habilidades personales y profesionales como se describen en la ISO 19011, tales como:

1. *Liderazgo*: debe ser capaz de analizar, aconsejar e influenciar el comportamiento en los altos niveles de la organización; lo que quiere decir es que deben ser buenos tanto escuchando como hablando.
2. *Sin cohibiciones*: deben tener la capacidad de si ven algo que está mal, ser capaces de indagar y hacer preguntas difíciles, notificar a las directivas y solucionar lo que está mal, siguiendo los estándares profesionales.
3. *Persistente:* no solo cumplen con lo mínimo requerido, dedican más tiempo y esfuerzo con el fin de mejorar su trabajo.
4. *Habilidades* con la tecnología: debe tener conocimientos sobre las tecnologías que le permitan desarrollar la auditoria con software que le apoyen este trabajo.
5. *Habilidades interpersonales:* Necesita tener habilidades que le permitan comunicarse con los diferentes niveles de la organización y por lo tanto con diferentes personalidades y así pueda lograr un mejor resultado en su trabajo.
6. *Formación*: Siempre deben estar capacitándose, desarrollando y mejorando sus habilidades como auditor. (Piattini & Del Peso, 2007)

El rol del auditor de sistemas

El rol de un auditor de TI, fundamentalmente consiste en evaluar el desarrollo, la implementación y las pruebas de los procesos de TI. Es responsable de realizar las auditorias de TI o relacionadas con TI, usando las herramientas y apoyándose en los últimos estándares para realizar esta tarea. Su alcance se extiende a las redes, al software, aplicaciones, a los sistemas de comunicación, seguridad en los sistemas y otros servicios que dependen de la infraestructura tecnológica.

Es un rol esencial en la organización, al realizar las auditorias sobre los recursos e infraestructura de TI, propende por que la información y los servicios de la organización se encuentren seguros y disponibles, a pesar de los riesgos internos y externos que los pueden afectar. (White, 2019)

Normatividad

Para elaborar el plan y llevar a cabo el desarrollo de la auditoria a un plan de continuidad del negocio, se toma como base para elaborarla, las normas: ISO 22301, ISO 27031, ISO 19011 y la ISO 31000, las cuales se describen brevemente a continuación:

El estándar ISO 22301 (2016), el cual sustituye al estándar británico BS 25999-2, tiene como propósito ayudar a las organizaciones a asegurar la continuidad de sus operaciones y servicios, para que sigan trabajando cuando un evento disruptivo ocurra y de esta manera ayuda a proteger la marca, su reputación y los intereses de las partes interesadas.

El estándar ISO 27031, sustituye al estándar británico BS 25777; explica los principios y conceptos de la tecnología de información y comunicación (TIC), provee un marco de trabajo de métodos y procesos para identificar aspectos como los criterios de desempeño, diseño e implementación para mejorar la disponibilidad y asegurar la continuidad del negocio. (Recovery, 2020)

El estándar ISO 19011, establece y brinda orientación de que se debe seguir al momento de realizar un programa de auditoria en empresas, independientemente de la naturaleza y tamaño de la mismas; así, se puede programar y planificar la auditoria en función de la empresa a auditar. (Platform, 2018)

El estándar ISO 31000, establece principios y directrices para la gestión y evaluación de riesgos, principalmente en los niveles operativos y de gobierno en una organización, independientemente de la naturaleza y tamaño de la misma, ayudándole a mejorar su planificación y a tomar mejores decisiones referente al riesgo. (Cero, 2020)

Plan de continuidad del negocio (PCN)

Una organización, independientemente el sector en el que opere (público o privado) o de su tamaño (grande, mediana o pequeña), debe estar preparada, protegida y saber cómo actuar ante un evento que pueda ocasionar la perdida de sus operaciones y/o servicios, es ahí en donde es necesario que cuente con un PCN. (Herbane, Elliott a, & Ethne , 2004)

Plan de continuidad del negocio, es una administración integrada de procesos que orientan o dirigen el desarrollo e implementación de actividades que aseguran la continuidad y recuperación del negocio, los cuales se soportan en manuales de usuario, de cómo salvaguardar una organización y en los cuales se contemplan el desarrollo de las

estrategias, la infraestructura, planes y acciones a seguir, ante un evento disruptivo. (Management, 2020)

El PCN se enfoca en sostener todos los procesos y recursos que se involucran en una organización, principalmente los procesos misionales (críticos para ella), durante y después de un evento disruptivo significativo; debe contar con una variedad de escenarios, desde desastres naturales, hasta el error humano, e incluir los procedimientos, el listado de los empleados relacionados con el PCN con sus funciones y datos de contacto, además de cualquier otra información que pueda ayudar a mantener la operación de la organización en funcionamiento ante una crisis. (Herbane, Elliott a, & Ethne , 2004)

Todas las organizaciones deberían tenerlo debidamente implementado, probado y actualizado, ya que, de no ser así, en el momento de presentarse alguno de los posibles eventos disruptivos, podrían llegar a causar graves daños a la organización, los cuales pueden ser de carácter económico, de imagen, de sanciones legales, etc., y que podrían llevar en el peor de los casos, al cierre de la empresa.

Para que este plan pueda lograr su cometido, debe contar con la participación de todas las partes interesadas (generalmente conformado por inversionistas, empleados, clientes y proveedores); dentro de las partes interesadas, son los empleados en todos los niveles organizativos, quienes tienen mayor injerencia y responsabilidad, en el diseño, elaboración y desarrollo del mismo, estos niveles son: el estratégico, el táctico y el operacional. (Verdi, MBCI, MBA, & PMP , 2016)

El nivel estratégico se encuentra conformado por la alta gerencia, el área financiera, el control interno, el área de planeación estratégica, entre otros; quienes definen dentro del

PCN, el objetivo y el alcance del plan, aportan tanto los recursos financieros y de talento humano, para el diseño, elaboración e implementación de éste.

En el nivel táctico, se encuentran los mandos medios de la organización, son quienes proporcionan una gestión de la respuesta, supervisa y dirige el trabajo del nivel operativo, y es quien comunica los avances o problemas al nivel estratégico.

El nivel operativo, está conformado por el personal que realiza el trabajo de recuperación, y son quienes están en la primera línea de operación. (Verdi, MBCI, MBA, & PMP , 2016)

Ciclo de vida del plan de continuidad del negocio

Para que el PCN sea efectivo y oriente todos los componentes del plan, incluidos el plan de recuperación ante desastres, la continuidad del negocio y la recuperación del negocio se debe tener claramente definido el ciclo de vida del PCN, con sus etapas y componentes como se muestra en la figura 1.

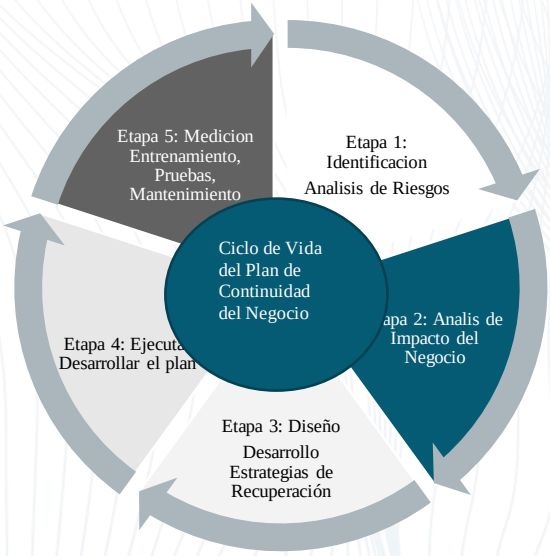

Figura 1. Etapas del PCN
Fuente: Elaboración propia, tomado de: http://bilait.co/continuidad

A continuación, se hace una breve descripción de los elementos del ciclo de vida del plan de continuidad del negocio, como se muestra en la figura 2.

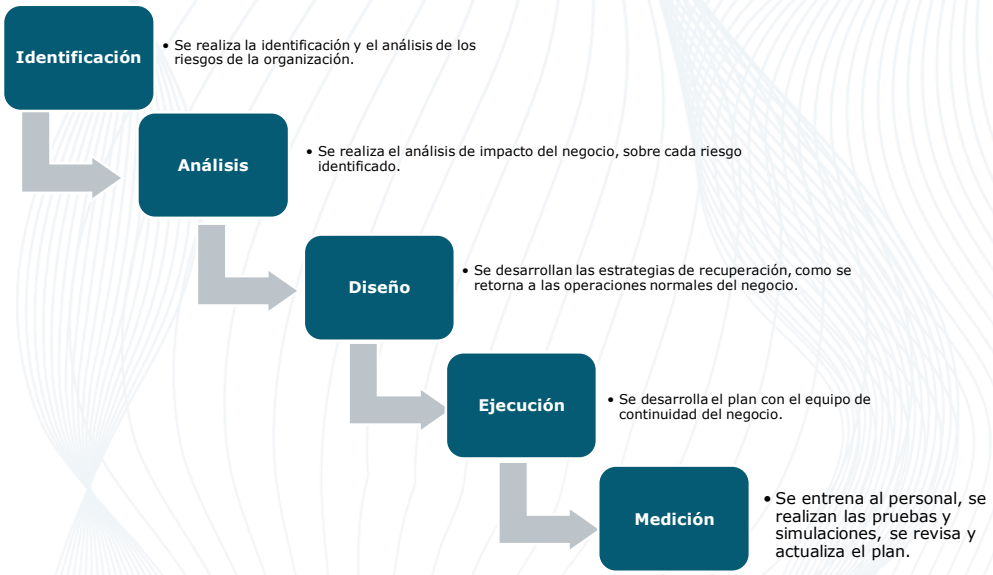

Figura 2. Elementos del ciclo de vida del Plan de Continuidad del Negocio
Fuente: Elaboración propia, tomado de: http://bilait.co/continuidad

El auditor de TI en su rol de auditor del PCN, debe revisar, que en el mismo se hayan analizado, evaluado y desarrollado cada uno de los componentes del PCN, los cuales se describen en la tabla 1.

Tabla 1. *Componentes de un plan de continuidad de negocio*

Evaluación de riesgos - Risk assessment (RA):	Ningún PCN, se puede efectuar sin una evaluación de riesgos. Este ayuda a identificar y direccionar potenciales riesgos y amenazas, cual es la probabilidad de ocurrencia y el impacto esperado, los cuales pueden llegar a causar una disrupción en el servicio y/o en las operaciones. (SupremusGroup, s.f.)
Análisis de impacto del negocio -Business impact analysis (BIA):	Proporciona una imagen clara de la importancia de las operaciones comerciales de la organización en función de los procesos que realiza, identifica las áreas y actividades de misión crítica y sugiere los tiempos óptimos y la logística de recuperación ante un evento mayor que afecte el normal desarrollo de sus operaciones. (Escuela Superior de Administración Pública, 2018)
Plan de recuperación ante desastres – Disaster recovery plan (DRP):	Este plan, documenta los procedimientos, políticas y acciones a seguir ante un fallo en los aspectos relacionados con TI; proporciona a la organización un plan de recuperación para los productos, servicios y áreas que dependen de la infraestructura de TI. Este plan tiene como objetivo ayudar a la organización a resolver problemas de perdida de información y recuperación de la funcionalidad de los sistemas críticos relacionados con TI, definiendo claramente el punto objetivo de recuperación, RPO, del inglés recovery point objective y el tiempo objetivo de recuperación, RTO, del inglés recovery time objective de dichos sistemas. (Ferrer, 2015)
Plan manejo de crisis – Crisis management plan (CMP)	Es pieza clave en el plan de continuidad del negocio; éste describe como una organización debe reaccionar ante una crisis, contiene los componentes de comunicación, facilitando así la información con todas las partes interesadas, incluyendo el personal involucrado y las tareas que deben realizar, el objetivo de éste, es minimizar los daños y restaurar las operaciones tan pronto como sea posible; Para esto se conforma el equipo de administración de crisis, que puede convocar el PCN y usa el CMP, como guía en la toma de decisiones del PCN, para evitar así la improvisación, que podría conducir a empeorar la situación. (Smartsheet, 2020)
Implementación y pruebas	La etapa de pruebas del PCN, no se enfoca solamente en que el resultado de éstas, sea pasa o falla, es muy importante que se estén realizando constantes mejoras en la estrategia implementada, para lo cual se deben realizar sesiones de entrenamiento y ejercicios de simulación con la cierta periodicidad, para que la organización pueda adoptar los cambios requeridos resultados de estas pruebas, las cuales se pueden llevar a cabo de diferentes maneras como son: pruebas de escritorio, simulaciones, pruebas en la vida real. (Susan & Rima, 2014)

Fuente: Elaboración propia.

Para desarrollar adecuadamente una auditoria al PCN, lo primero que se debe hacer, es establecer el objetivo del PCN, el cual consisten en asegurar la continuidad del negocio, minimizando el tiempo de indisponibilidad de los servicios y/o productos, mientras que ayuda a proteger el personal y a minimizar las pérdidas financieras, de reputación, entre otros, durante un evento disruptivo; además de restaurar las operaciones y la infraestructura critica para el negocio, después del evento. Luego se debe identificar el objetivo de la auditoria al plan de continuidad del negocio, el cual es, proveer a las directivas de la organización, una evaluación independiente de la efectividad del plan de continuidad del negocio, que éste se encuentre alineado a los objetivos del negocio; evaluar que la organización se encuentre preparada en el caso de ocurrir un evento disruptivo e identificar los problemas que puedan limitar la recuperación de la operatividad del negocio. (Rock, 2017)

Para lograrlo, se dividen en los siguientes grupos de acuerdo al estándar para el plan de continuidad del negocio.

1. *Gobierno del PCN:* Verificar que la organización, haya establecido una estructura de gobierno para PCN, las políticas y los procedimientos, que haya identificado y creado el listado de incidentes más críticos y que ha determinado sus controles.
2. *Análisis de impacto del negocio:* Comprobar que la organización realizo un análisis del impacto del negocio, que priorizo sus servicios críticos e identifico los impactos de las interrupciones y los tiempos de recuperación para la organización.
3. *Planes de respuesta y recuperación:* Verificar que la organización haya asegurado el desarrollado de planes que aseguren la continuidad y disponibilidad de los servicios

críticos, que se hayan incluido software, hardware, proveedores y la información sensible que utilice, contar con un árbol de llamadas documentado y actualizado, para poder ser utilizado y así notificar a los involucrados en el plan: empleados, clientes, proveedores y otras partes interesadas, durante el incidente.

Una vez superado el evento disruptivo, se deben incluir los procedimientos para un regreso a la operación normal.

4. *Mantenimiento y pruebas:* Se debe tener un cronograma para el desarrollo de las pruebas al PCN, utilizando cualquiera de las herramientas disponibles, ya sea prueba de escritorio, simulacros o pruebas reales, para asegurar que se encuentra debidamente afinado y sirva como herramienta para apoyar la organización a recuperarse ante un evento disruptivo; es necesario que estas pruebas involucren al personal con funciones relacionadas con el PCN, para garantizar que se le haya impartido la formación adecuada sobre seguridad y continuidad de negocio y que además cuente con los recursos necesarios para enfrentar una contingencia y por lo tanto este preparado para apoyar la organización de una manera adecuada.

Los Planes de Continuidad del Negocio, vienen en muchas formas y tamaños, debido a que cada organización es diferente; es recomendable que el equipo auditor cuente con expertos en administración y en áreas de TI; debido a que los detalles específicos de cada auditoria varían, a continuación, se anuncian algunos de los más generales en una auditoría al PCN.

La complejidad y costos relacionados con el PCN, depende de muchos factores como, por ejemplo: de la naturaleza del negocio, de la infraestructura física, infraestructura de TI, entre otros.

El plan de trabajo para una auditoria de sistemas al PCN

De manera general, el rol de la auditoria de sistemas al PCN debe considerar por cada componente actividades o interrogantes como se muestra en la tabla 2.

Tabla 2: P*lan de trabajo para una auditoria de sistemas al PCN*

Políticas y procedimientos relacionados con el PCN		Revisión de las políticas y procedimientos para el Plan de Continuidad del Negocio.
	1	Determinar si está documentado el PCN
	2	Revisar si cubre todos los procesos de misión crítica de la organización?
	3	Tiene asignado el plan un administrador?
	4	Cuenta con representación de todas las partes críticas de la organización?
	5	Hay evidencia de las revisiones y aprobaciones del plan?
	6	El plan ha sido debidamente comunicado a todas las partes interesadas?
	7	Verificar la información de contacto establecida en el PCN, esta actualizada?
	8	Tiene el plan la lista de estrategias a utilizar?
	9	Como o cual es el proceso para tener actualizado el plan?
	10	Determinar si hay copias del PCN, en sitios fuera de la oficina principal
	11	Se tiene un sitio alterno contratado con capacidad de procesamiento de datos?
	12	Obtener evidencias del presupuesto asignado para el PCN
Administración de riesgos		Verificar la Administración de Riesgos
	1	Obtener los documentos donde se identificaron los riesgos (Matriz de riesgos), que estén asociados a posibles eventos disruptivos
	2	Verificar si se hizo una valoración de riesgos (Matriz de seguimiento de riesgos), cuyo tratamiento de riesgo esté relacionado con el posible evento disruptivo
	3	Obtener las actas de reuniones de Administración de Riesgos
	4	Se encuentran identificados todos los terceros críticos para los procesos relacionados con tecnología e infraestructura en el BIA
	5	Se tiene la evaluación de riesgos elaborada por cada proveedor
	6	Se identificaron los tratamientos de acuerdo a los objetivos del PCN
Análisis de Impacto del Negocio (BIA)		Obtener y revisar el Análisis de Impacto del Negocio (BIA)
	1	Determinar si el BIA sirve como base para tomas de decisiones para la continuidad del negocio
	2	Revisar la metodología usada para el desarrollo del BIA

	3	Determinar si todos los procesos críticos han sido identificados y cuenta con un plan adecuado
	4	El BIA identifica los equipos claves en la continuidad del negocio, con sus datos de contacto?
	5	Están incluidos en los equipos claves sus roles y responsabilidades?
	6	Determinar si la organización tiene los RTO (Tiempo Objetivo de Recuperación) y los RPO (Punto de Recuperación Objetivo), por cada aplicación critica
	7	Evaluar si los RTO y RPO son prácticos y razonables para cada aplicación o sistema critico a recuperar
	8	Determinar si se tiene un listado con la información necesaria para contactar a los proveedores claves en una recuperación
	9	Cuenta con procedimientos de las copias de seguridad actualizadas?
	10	Determinar si el BIA cuenta con las acciones claras a tomar en una emergencia
	11	Se cuenta con los litados del personal critico involucrado en la recuperación y las herramientas necesarias para retomar la operación?
	12	Se tienen identificados los documentos de los objetivos críticos a recuperar con los tiempos de recuperación?
	13	Determinar si se tienen documentados todos los procesos, sistemas, aplicaciones, redes y datos, que soportan la función normal del negocio
	14	Revisar que todo el personal listado en el BCP, este en el listado del personal activo en la organización
	15	Cuenta con mapas y direcciones de los sitios alternos
	16	Los planes están razonablemente ordenados y depurados de procesos no esenciales
Respuesta a incidentes		Obtener y revisar las políticas y procedimientos a la respuesta de incidentes
	1	Obtener, Identificar y comprender las políticas y procedimientos a la respuesta de incidentes
	2	Cronograma de simulacros de incidentes
Plan de Recuperación		Obtener y revisar los resultados del Plan de Recuperación Ante Desastres
	1	Los objetivos del plan de recuperación ante desastres, están alineados con los resultados del BIA?
	2	Se identificaron los puntos débiles y puntos de falla
	3	Se han establecido e implementado las medidas de mitigación
	4	Cuenta con los roles de recuperación críticos identificados
	5	Revisar si los Acuerdos de niveles de Servicio (SLA), están realizando de acuerdo a lo especificado en los contratos de los proveedores
Pruebas del Plan		Obtener evidencias de la última actualización del plan
	1	¿La organización cuenta con sitios alternos para la recuperación?
	2	Cuenta con las herramientas para la recuperar los sistemas y la información?
	3	Cuenta con procedimientos para las pruebas y simulacros
	4	Cuenta con copias de seguridad de la información en sitios seguros fuera de la oficina o en la nube?
	5	Cuenta con la información de los proveedores de software o hardware, incluidos los acuerdos de niveles de servicio

6	Obtener copia de los procedimientos utilizados para una comunicación efectiva
7	Obtener una copia del Plan de Recuperación ante desastres
8	Verificar la pertinencia del material, los procedimientos y guía de entrenamiento
9	Revisar los planes de pruebas y cualquier prueba ya realizada
10	Evaluar la preparación de los empleados y su familiaridad con el PCN
11	Revisar el Impacto de nuevas regulaciones en el plan
12	Revisar los contratos de proveedores y contratistas relacionados con el plan
13	Verificar si existe un ciclo de pruebas para probar regularmente el plan
14	Obtener los documentos donde se evidencie si el plan de continuidad ha sido probado con regularidad
15	Obtener copia de las políticas de pruebas del plan
16	Determinar si los resultados de las pruebas del plan fueron documentados, actualizados o corregidos en el plan
17	Cuando fue la última vez que se probó el plan
18	Se han comunicado los resultados de las pruebas a las directivas de la organización?

Fuente: Elaboración propia Tomado de: https://assets.hcca-info.org/

El plan de trabajo sugerido, le brinda al auditor, una guía con el objetivo de apoyar el rol del auditor en el desarrollo de auditorías al cumplimiento de los principales componentes del plan de continuidad del negocio.

Conclusiones

El Plan de continuidad del negocio, es una valiosa herramienta para cualquier organización, sin importar su naturaleza o tamaño, el cual le ayuda al momento de enfrentar un evento disruptivo, brindándole lineamientos y procedimientos claros y precisos a seguir, para que pueda continuar funcionando con las operaciones criticas del negocio.

Igual de importante, como tener el PCN, es que se le realicen pruebas (de escritorio, simulacros o pruebas reales) y mantenerlo actualizado, son las pruebas y las actualizaciones, las que hacen que el plan realmente este depurado y sirva al momento de necesitarlo. El PNC, debe ser conocido por todas las partes interesadas e involucradas en él,

para que lo puedan aplicar correctamente y cada involucrado sepa cómo, cuándo y dónde actuar.

El rol del auditor en la auditoria al PCN, contribuye en gran medida a la mejora del plan, al detectar deficiencias y omisiones que se hayan pasado en el diseño, elaboración, implementación y en las actualizaciones del mismo.

Las directivas de una empresa confían en los hallazgos de las auditorias, los cuales sirven de insumo para mejorar el funcionamiento de los controles sobre los sistemas y los procesos críticos de la organización. De tal forma, la auditoria al PCN, se vuelve fundamental para una organización, al ser su función, la de confirmar que la organización cuenta con los planes, la infraestructura, el personal y, que se encuentra adecuadamente protegida, en cuanto a lo relacionado con el plan de continuidad del negocio, siempre teniendo como marco de referencia la norma ISO 22301.

Estas labores requieren de auditores que conozcan la organización y sus procesos, debe contar con las habilidades personales y profesionales y con el manejo de herramientas de gestión, control estadístico, trabajo en equipo, planificación, normativas legales entre otras.

Es importante aclarar en este punto, que el requisito establecido en la Norma ISO 9001:2008, 8.2.2 “Los auditores no deben auditar su propio trabajo”, ya no se menciona en la versión 2015 (Jimenez, 2015); el requisito de asegurar la objetividad, imparcialidad, e independencia en el proceso de auditoría, sigue en firme; por lo tanto, es recomendable que la persona que va a realizar el proceso de auditoría, no haya participado en la elaboración del PCN, esto con el fin de asegurar la objetividad e imparcialidad requerida en el proceso,

aunque esto no siempre es posible, se debe tratar de quitar los sesgos y animar la objetividad.

Referencias

assets.hcca-info.org. (2016). Obtenido de https://assets.hcca-info.org/Portals/0/PDFs/Resources/Conference_Handouts/Compliance_Institute/2016/W8handout6.pdf

Cero, R. (2020). *https://www.riesgoscero.com/*. Obtenido de https://www.riesgoscero.com/academia/especiales/guia-del-sistema-de-gestion-de-riesgos-iso-31000

Escuela Superior de Administración Pública. (1 de 6 de 2018). *http://www.esap.edu.co/*. Obtenido de http://www.esap.edu.co/portal//wp-content/uploads/2019/03/Plan-de-continuidad-del-negocio-v1.pdf

Ferrer, R. (2015). *https://cintel.co/*. Obtenido de https://cintel.co/wp-content/uploads/2013/05/Metodolog%C3%ADa-para-la-Gesti%C3%B3n-de-la-Continuidad-del-Negocio.pdf

Herbane, B., Elliott a, D., & Ethne , S. (2004). *Long Range Planning.*

INCIBE. (26 de 09 de 2019). *Fases de un Plan de Continuidad de Negocio.* Obtenido de https://www.incibe.es/protege-tu-empresa/blog/fases-plan-continuidad-negocio

isotools. (12 de abril de 2016). *isotools.cl*. Obtenido de https://www.isotools.cl/iso-22301-sistema-gestion-continuidad-negocio/#:~:text=Continuidad%20de%20negocio%20es%20el,cibern%C3%A9ticos%2C%20accidentes%20o%20errores%20humanos.

Jimenez, D. (7 de 11 de 2015). *https://www.pymesycalidad20.com/*. Obtenido de https://www.pymesycalidad20.com/cambios-proceso-auditorias-iso-90012015-3-realizacion.html

Management, O. O. (2020). *https://www.toronto.ca/*. Obtenido de https://www.toronto.ca/wp-content/uploads/2018/01/94bf-Guide-to-Business-Continuity-Planning.compressed.pdf

Piattini, M., & Del Peso, E. (2007). *Auditoría Informática Un enfoque práctico* (2a ed.). AlfaOmega.

Platform, O. B. (2018). *https://www.iso.org/*. Obtenido de https://www.iso.org/obp/ui#iso:std:iso:19011:ed-3:v1:es

Recovery, D. (2020). *SDR México*. Obtenido de https://sdr.com.mx/index.php/iso-27031-norma-para-crear-un-plan-de-continuidad/

Rock, T. (18 de 1 de 2017). *https://invenioit.com/*. Obtenido de https://invenioit.com/continuity/business-continuity-plan-objectives/

Smartsheet. (2020). *www.smartsheet.com*. Obtenido de Step-by-Step Guide to Writing a Crisis Management Plan: https://www.smartsheet.com/content/crisis-management-plan

SupremusGroup. (s.f.). *https://www.supremusgroup.com/*. Obtenido de https://www.supremusgroup.com/business-contingency-strategy/risk-assessment-package/

Susan, S., & Rima, C. (2014). *https://www.sciencedirect.com/*, 2a.

Verdi, J., MBCI, MBA, & PMP . (21 de 04 de 2016). *avalution.com*. Obtenido de https://avalution.com/business-continuity-implementation-an-overview-of-bci-professional-practice-5/

White, S. K. (5 de 3 de 2019). *cio.com*. Obtenido de https://www.cio.com/article/3346029/it-auditor-role-defined.html