UNIVERSIDAD DE COSTA RICA
SISTEMA DE ESTUDIOS DE POSGRADO

ELABORACIÓN DE UN PLAN DE AUDITORÍA PARA EVALUACIÓN DE CUMPLIMIENTO EN SISTEMAS PARA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO BASADO EN LA NORMATIVA ISO 22301

Trabajo final de graduación sometido a la consideración de la Comisión del Programa de Estudios de Posgrado en Administración y Dirección de Empresas para optar al grado y título de Maestría Profesional en Auditoría de Sistemas de Información

SUSTENTANTE

JOSÉ ALBERTO GONZÁLEZ VILLALOBOS

Cuidad Universitaria Rodrigo Facio, Costa Rica
2015

Agradecimientos

Aquí es donde la mula botó a Genaro, pero antes de bajarme quiero darle agradecer:
A Rigoberto y Julieta, por enseñarme el valor del trabajo y que el esfuerzo siempre rinde frutos, son unos padres maravillosos. A Josué y Gerardo por embarcarme, en todo sentido de la expresión, en esta aventura en la UCR, no podría tener mejor amigo y pareja.

Tabla de Contenido

Índice de Tablas

Índice de Figuras

Hoja de Aprobación

Este trabajo final de investigación aplicada fue aceptado por la Comisión del Programa de Estudios de Posgrado en Administración y Dirección de Empresas de la Universidad de Costa Rica, como requisito parcial para optar al grado y título de Maestría Profesional en Auditoría de Sistemas de Información

_____

MSc. Sergio Espinoza

Profesor Guía

_____

MSc Andrés Casas

Lector

_____

Lic. Sofía Víquez Alfaro

Lectora de Empresa

_____

Dr. Aníbal Barquero Chacón Director

Programa de Posgrado en Administración y Dirección de Empresas

_____

José Alberto González Villalobos

Sustentante

Resumen

El presente trabajo ofrece una guía para la elaboración de auditorías de cumplimiento basados en la norma ISO 22301. Dicha guía permite verificar los esfuerzos realizados por la alta gerencia de una organización para brindar las capacidades necesarias para sobrevivir a eventos disruptivos que puedan amenazar la supervivencia de la misma.

La normativa ISO 22301:2012 es el producto final de la evolución constante de esfuerzos descentralizados para brindar una guía práctica en con fin de normar los sistemas de gestión para la continuidad del negocio. En sus secciones establece siete áreas de trabajo que definen los pilares claves para extender las capacidades adquiridas a todos los procesos críticos para el negocio: .

La normativa enfoca los primeros esfuerzos de implementación en canalizar el apoyo de la gerencia y el liderazgo organizacional como pilar que sustente y respalde toda la implementación, una vez obtenido el respaldo de estos se podrá abastecer la iniciativa de recursos suficientes para poder hacer un despliegue ordenado y consistente.

Desde el enfoque operativo, las secciones de planificación, soporte y operación tienen como fin establecer un sistema organizacional, el cual convierta las intenciones gerenciales en mecanismos tangibles que garanticen la supervivencia organizacional ante eventos desastrosos.

En sus últimas secciones, se abarcará el sistema como una entidad en constante mejora y crecimiento, por lo que es indispensable incluirlos en los planes de auditoría de autoevaluación.

Los cuestionarios para aplicación descritos en este plan de auditoría, brindan al auditor los lineamientos requeridos por ISO para verificar el cumplimiento o necesidad de mejora de los esfuerzos desplegados.

Capítulo I – Introducción

Los planes de continuidad del negocio como herramienta estratégica han evolucionado rápidamente en consecuencia de las presiones que impone una sociedad globalizada con cadenas de suministros de servicios distribuidas a lo largo del orbe.

El aumento de las exigencias en la forma de hacer negocios, representa, para las organizaciones modernas, la necesidad de adquirir capacidades estratégicas y tácticas para responder de manera eficiente ante incidentes que afecten la operación de la misma y las obligaciones adquiridas. Extendiendo dichas obligaciones a la organización *per se:* los miembros que la componen, la sociedad en la que se desempeña, los clientes finales, los proveedores y demás entes en la cadena de suministro.

El crecimiento de las capacidades estratégicas, a nivel organizacional, ha aumentado la complejidad de los planes de continuidad, por lo que muchos estudiosos del campo exponen la necesidad de migrar a un modelo de conciencia mayor a la planeación y plantean sistemas de gestión de la continuidad del negocio(BCMS. por sus siglas en inglés).

El ISO 22301:2012 es una normativa que brinda los lineamientos necesarios para la implementación de sistemas que garanticen la continuidad del negocio de las organizaciones. Publicada en 2012, como una evolución constante de la necesidad de armonizar los procesos bajo un solo lineamiento, este documento, a través de sus diferentes secciones, ofrece las bases para trabajar e implementar el BCMS.

Considerando lo anterior, el presente trabajo plantea una serie de herramientas de auditoría basadas en la normativa ISO 22301:2012, el cual tiene como objetivo brindarle a los auditores una guía sistemática aplicada a las organizaciones de

servicios, para que estos puedan emitir recomendaciones de mejora o corrección al respecto

Justificación

La elaboración de un sistema de gestión para la continuidad del negocio brinda a la organización las capacidades estratégicas y técnicas necesarias para responder ante eventos que pueden afectar los procesos críticos que conforman la organización. Un sistema de esta naturaleza representa un esfuerzo organizacional considerable por parte de la gerencia, sin embargo, por sus características, no se puede ver como una iniciativa intrascendente en la organización, que debe convertirse en un proceso institucionalizado entre las partes involucradas de tal manera que se dinamice constantemente.

Para lograr la el mejoramiento constante y la institucionalización de sus capacidades, es importante participar en procesos de mejora continua que permitan ajustar dicho sistema a las necesidades cambiantes del negocio y del entorno.

Un plan de auditoría y evaluación sobre el cumplimiento se vuelve una propuesta atractiva y sencilla para evaluar constantemente los planteamientos organizacionales correspondientes a los BCMS, ya que permite trabajar bajo criterios establecidos por las normativas publicadas, brinda recomendaciones prácticas incorporando el conocimiento de los auditores y ofrece a los responsables dentro de la organización un panorama claro sobre el estado actual y sobre los puntos de mejora de sus sistemas.

Objetivos

Objetivo General:

Brindar a la organización un mecanismo de evaluación para sistemas de gestión para la continuidad del negocio, basado en la norma ISO 2230. Por medio de la elaboración y diseño de un plan de auditoría para el cumplimiento de los controles implementados.

Objetivo Específicos:

1- Desarrollar un plan de auditoría para los sistemas de continuidad del negocio, a través de una herramienta automatizada de control, cumplimiento y tiempos.

2- Proporcionar a la organización un mecanismo de medición y control interno para seguimiento de la auditoría de sistemas de gestión de la continuidad del negocio, esto a través de un instrumento basado en las mejores prácticas de continuidad.

3- Elaborar pruebas de cumplimiento enfocadas en los controles implementados por la organización, utilizando una herramienta de auditoría fundamentada en la normativa seleccionada.

4- Comunicar a la gerencia de cumplimiento y seguridad de la información, el plan elaborado, así como el uso de los papeles de trabajo y pruebas de cumplimiento.

Alcance

El presente trabajo tiene como alcance el diseño de un plan de una auditoría basado en la norma ISO 22301:2012 con el fin de validar el cumplimiento de los controles implementados por la organización sobre el sistema de gestión para la continuidad del negocio durante el año financiero 2014, por lo tanto las evidencias,

controles y cualquier documentación fuera del rango comprendido entre Enero 1, 2014 y Diciembre 31-2014 estarán fuera de la ejecución de este proyecto.

Limitaciones

El fin primordial de la auditoría es validar el cumplimiento y alineamiento del plan de continuidad de la organización basada en la normativa ISO 22301, este ejercicio solicitado por el departamento de cumplimiento responde al plan de mejora de los procedimientos implementados. Sin embargo, dentro de dicho proyecto se excluye:

- Pese que la organización es de naturaleza transnacional, el trabajo se elaborará en español, y se omitirá cualquier traducción a otros idiomas.
- La activación de los planes actuales o ejecución de cualquier actividad que pueda comprometer la correcta operación de la organización.
- La elaboración de una evaluación de riesgo, puesto que las acciones actuales se limitan a verificar el cumplimiento de la existencia de dicha actividad y sus repercusiones en la continuidad del negocio.
- La elaboración de un análisis de impacto del negocio, solo se realiza la evaluación del mismo en caso de existir uno.

Capítulo II - Marco Teórico

Conceptualización de BCMS

De acuerdo con la Organización Internacional para la Estandarización (ISO, por sus siglas en inglés), los sistemas de gestión para la continuidad del negocio (BCMS) son sistemas holísticos que se encargan de administrar, establecer, implementar, monitorear y mantener la continuidad del negocio. (ISO, 2012) Actualmente, las organizaciones emplean planes de continuidad con el fin de dotar de capacidades necesarias a sus procesos críticos para continuar sus operaciones bajo los niveles de servicio acordados ante escenarios de interrupción (ISO, 2012), por lo tanto, la aplicación de BCMS se convierte en una herramienta de gobierno corporativo trascendental para definir la sobrevivencia de la entidad a corto, mediano y largo plazo.

Conforme las tecnologías de información han ido evolucionando y facilitando los procesos de globalización en la forma de hacer negocios, al mismo tiempo las organizaciones han crecido y aumentado su complejidad, incrementando, a su vez, los factores de riesgo que pueden afectar las mismas. Factores como fenómenos naturales, la geopolítica mundial, las personas dentro y fuera de la organización, entre otros pueden impactar los procesos críticos y detener la operación total o parcial de los involucrados.

Contexto histórico y evolución

Las computadoras facilitaron el procesamiento de datos y, rápidamente, se propagaron por muchos procesos de negocios. Sin embargo, la falta de fiabilidad de estos equipos y el riesgo potencial de perder información, revelaron la pronta necesidad de mitigar cualquier evento adverso para la organización (Drewitt, 2013), puesto que, conforme la manera de hacer negocios involucraba el uso de ordenadores, la criticidad de los mismos y sus datos contenidos crecía exponencialmente. Debido a esta necesidad constante de acceso a la tecnología,

surge una disciplina que, para expertos como Tony Drewitt (2013), sería la base para la continuidad del negocio: ITDR *(Information Technology Disaster Recovery).*

La planificación de recuperación ante desastres era una actividad liderada por el gerente de cómputo dado que su perspectiva estaba enfocada en los sistemas y los datos que estos contenían. En el contexto histórico, esta disciplina aceptaba tiempos de recuperación medidos en días, contrario a la actividad moderna, que está basada en horas. (GALLAGHER, 2003)

Como disciplina, la ITDR en los años 70 y mediados de los ochenta satisfacía la necesidad del negocio, la organización podía responder a incidentes operativos y no verse impactada a corto plazo ante dichos eventos. Sin embargo, a partir de mediados de los años ochenta, el crecimiento de la industria tecnológica y el impulso económico del mercado, sustentaron las bases de la continuidad y recuperación del negocio.

Nuevos incidentes de riesgo comenzaron a materializarse dentro y fuera de la organización (Drewitt, 2013). A partir de este punto, las organizaciones empezar a hacer conciencia sobre la continuidad como elemento holístico de la empresa y no solo como un proceso operativo de tecnologías de información.

Los principales propulsores de la continuidad del negocio fueron algunas organizaciones bancarias, dado que los entes rectores como el *Financial Services Authority* (FSA) en Reino unido y el *Securities Exchange Commission* (SEC) en Estados Unidos, establecieron regulación para manejo, respaldo y uso de la información, por lo que la necesidad de modelar una nueva disciplina enfocada en el negocio dio auge a la evolución de DRP/ITDR.

En 1994, el Instituto para la continuidad de los negocios (BCI, por sus siglas en inglés) es establecido por profesionales de tecnologías de información en el sector financiero. Además, en esa misma década, el *British Standards Institution* (BSI) publica un documento llamado *Publicly Available Specification 56* (PAS56), como un primer informe teórico para la continuidad del negocio. (Drewitt, 2013)

Para el año 2007, se publica el BS25999 como una guía estándar para la gestión de la continuidad del negocio, derogando el PAS56. Seguidamente, en el 2012, la Organización Internacional para la estandarización (ISO) publica la “ISO 22301: 2012 Seguridad de la sociedad- Sistemas de gestión de la del negocio - – Requisitos”

Figura 1 Evolución histórica de normas y marcos de referencia sobre BCMS

Fuente: Kosutic, D. (2012).

Conceptos claves BC

Activación: Implementación de procesos para recuperación, actividades, y planes en respuesta de una declaración de emergencia asociada a un incidente o desastre. (ISACA, 2014)

Sitio Alterno: Locación alterna, diferente al lugar principal de operación, que puede ser usada eventualmente para realizar funciones de negocio. (Risk Cover, 2009)

Gestión de la Continuidad del Negocio (BCM): Disciplina que prepara a una organización para lo inesperado. Es un proceso de gestión que ofrece un marco de trabajo para darle resiliencia a la operación ante riesgos de interrupción, de tal manera que se garantice la continuidad en los servicios críticos. (Drewitt, 2013)

Plan de Continuidad del Negocio (BCP): Principal salida del proceso de continuidad del negocio. Este documento describe un plan de tratamiento para ciertos riesgos y consecuencias que pueden afectar la operación de la organización. (ISO, 2012)

Programa de Continuidad del Negocio: Proceso de gestión y gobierno soportado por la alta gerencia que brinda recursos y soporte para implementar y mantener una correcta gestión para la continuidad del negocio. (Risk Cover, 2009)

Análisis de Impacto en el Negocio (BIA): Proceso de organización para determinar el impacto de perder el apoyo de cualquier recurso identificado dentro del flujo de proceso. (ISACA, 2014)

Plan de Contingencia: Plan con las acciones a ser seguidas en caso de un evento o desastre que amenace con la interrupción o destrucción de la continuidad del negocio y sus actividades. (ISACA, 2014)

Factores Críticos de Éxito (CSF): Un factor que es esencial para el buen desarrollo de una actividad empresarial clave. (Risk Cover, 2009)

Plan de Recuperación ante Desastres (DRP): Un conjunto de recursos humanos, físicos, técnicos y de procedimiento para recuperar, dentro de un tiempo y coste definidos, una actividad interrumpida por una emergencia o un desastre. (ISACA, 2014)

Alta Disponibilidad (HA): La capacidad de un sistema para realizar su función sin interrupción durante un período prolongado de tiempo. HA se puede lograr a través de un software especial y la implementación de equipos redundantes. (Risk Cover, 2009)

Riego Informacional: La oportunidad o posibilidad de daño que se cause a una empresa como resultado de una (Risk Cover, 2009) pérdida de confidencialidad, integridad y disponibilidad de la información.

Invocación: Acto de declarar que los procesos de continuidad de negocio y sus partes deben ser puestos en marcha con el fin de continuar entregando productos y servicios amparados bajo este proceso. (ISO, 2012)

Interrupción Máximo Aceptada (MAO): Máxima cantidad de tiempo que una actividad clave de negocios puede ser suspendida dado una interrupción antes de que las consecuencias representen un detrimento en la organización. (ISO, 2012)

Objetivo Mínimo de Continuidad: Nivel mínimo de servicios o productos que son aceptables para que una organización obtenga y opere durante una interrupción. (ISO, 2012)

Interrupción: Evento extraordinario de naturaleza natural o inducido por humanos que puede causar una interrupción o pérdida de un proceso clave en la organización, puede representar un impacto significativo en la empresa. (ISACA, 2014)

Punto Objetivo de Recuperación (RPO): Medida que determina con base en la pérdida de datos aceptable en caso de una interrupción de operaciones, indica el punto más temprano en el tiempo que sea aceptable para recuperar los datos. El

RPO cuantifica de manera efectiva la cantidad admisible de la pérdida de datos en caso de interrupción (ISO, 2012)

Tiempo objetivo de Recuperación (RTO): Cantidad de tiempo permitido para la recuperación de una función de negocio o recurso después de un desastre. (ISO, 2012)

Riesgo: Combinación de la probabilidad de un evento y sus consecuencias. (ISO, 2012)

Evaluación del Riesgo: Proceso de identificación, análisis y evaluación de riesgos. (ISACA, 2014)

Gestión del Riesgo Actividades coordinadas dentro de la organización para dirigir y controlar los riesgos identificados por la misma. (ISO, 2012)

Normativa ISO 22301 e ISO 22313

La normativa ISO 22301 es un estándar publicado por la ISO en 2012, con el fin de brindar un documento que ofrezca soporte a las organizaciones para protegerse, mitigar o recuperarse de cualquier evento disruptivo a las operaciones. (Zawada, 2014), dicho documento se convierte en un instrumento para canalizar los esfuerzos de los grupos estratégicos para prolongar la supervivencia de la organización.

ISO 22313, representa una segunda publicación elaborada durante el 2012 donde se brinda una guía para las organizaciones que están en proceso de madurar planes de continuidad de negocios. Este es un documento que resulta un complemento de primero, en donde se describe una guía para comprender y cumplir con los objetivos.

Esta serie de publicaciones tiene como alcance la especificación de los requisitos, planificación, despliegue, operación, monitoreo y revisión de los sistemas documentados para protegerse contra eventos disruptivos. (ISO, 2012)

Componentes

La normativa ISO 22301 cuenta con seis secciones de trabajo, a través de las cuales establece una serie de requisitos y mejores prácticas para la continuidad del negocio.

Dichos elementos se describen a continuación.

- D4 – Contexto Organizacional
- D5- Liderazgo
- D6 Planificación
- D7 Soporte
- D8 Operación
- D9 Evaluación y Desempeño
- D10 Mejora

D4 – Contexto Organizacional

El entendimiento de la organización y su contexto permite determinar las actividades, funciones y responsables que permiten que la misma opere. A través de este ejercicio se puede identificar elementos críticos de la empresa y los posibles eventos que la puedan afectar.

El entendimiento de la organización ayuda a la identificación de las partes interesadas así como las expectativas de los mismos con respecto a la empresa. (Drewitt, 2013). En una primera instancia, las partes interesadas que tienen mayor peso son los clientes, dado que la continuidad de la operación les permitirá disfrutar de los servicios adquiridos. Desde una perspectiva más compleja, esto permite generar confianza y mejorar la imagen de la marca.

Dentro del estudio organizacional, los practicantes de la norma ISO 22301 deben realizar un análisis interno y decidir un alcance realista y fundamentado. (ISO, 2012)Una vez establecido el contexto de la organización y los procesos, personas y tecnologías asociados, es importante establecer los lineamientos para la continuidad del negocio como un elemento estratégico y no solo un requerimiento operativo. El establecimiento de un programa respaldado por la gerencia brindará un mayor apalancamiento y conocimiento del mismo. (Drewitt, 2013)

Tabla 1 Componentes de la Sección

4.1 Entender la organización y su contexto.	• Entender la organización y sus actividades. • Comprender la cultura organizacional. • Entender el apetito del riesgo definido. • Analizar posibles amenazas.
4.2 Entender las necesidades y expectativas de las partes	• Comprender las posibles partes interesadas y sus intereses.

interesadas.	• Analizar las expectativas de: clientes, empleados, accionistas, distribuidores, la sociedad.
4.3 Determinar el alcance del sistema de gestión para la continuidad del negocio.	• Definir el rango de acción que un BCMS debe abarcar según los objetivos y cultura. • Puede ser por áreas, regiones, divisiones, sitios, productos. • Requiere un análisis de impacto en el negocio.
4.4 Sistema de gestión para la continuidad del negocio.	• Establecer un programa oficial con patrocinio de la gerencia. • Garantizar los recursos al programa.

Fuente: Elaboración propia a partir de los criterios de Drewitt (2013) e ISO (2012). D5 - Liderazgo

La normativa busca establecer un ente rector y líder sobre la continuidad del negocio, esto dado a que si los programas surgen descentralizados ya sea por iniciativa interna, requisitos de clientes o regulaciones, puede generar múltiples visiones y desperdicio de recursos.

Parte de esta sección representa la creación de políticas que brinden respaldo al programa de continuidad del negocio. La política representa en múltiples facetas la voluntad y el respaldo de la organización (Drewitt, 2013). Además, parte de una cultura de liderazgo a lo interno del plan de continuidad es el establecimiento de roles y responsabilidades, lo cual evita que un mismo individuo ejecute y sea responsable al mismo tiempo. Permitiendo espacio a la independencia en la auditoría.

Tabla 2 Componentes de la Sección 5

5.1 Política de Continuidad.	• Expresar la voluntad y respaldo al BCMS. • La organización expresa su deseo de ser resiliente. • Mandato ejecutivo a los gerentes para alinear sus áreas y desarrollar medidas de continuidad. • Generación y respaldo a lo interno para promocionar y comunicar.
5.2 Roles y Responsabilidades.	• Seleccionar a los responsables del proceso. • Permitir asignar obligaciones de manera fundamentada. • Brindar autoridad a los miembros del programa y respaldo de la gerencia a través de la política.

Fuente: Elaboración propia a partir de los criterios de Drewitt (2013) e ISO (2012). D6 – Planificación

La sección de planificación se encarga de sistematizar y armonizar las intenciones de la gerencia en objetivos estratégicos con el fin de alinear el programa con los intereses de la organización. (Drewitt, 2013). Para St-GERMAIN (2014), un correcto modelado de los requisitos permite actuar de manera clara y eficiente

ante un evento, en dado contrario el mejor esfuerzo puede resultar entorpecedor y afectar.

Tomando en cuenta lo anterior, se entiende que los objetivos definidos en la etapa de planificación deben ser holísticos y para toda la organización; alineados a la política de continuidad y deben establecer los niveles mínimos de servicios deseados durante un incidente.

Tabla 3 Componentes de la Sección 6

6.1 Acciones para identificar riesgos y oportunidades.	• Identificar y analizar posibles eventos adversos para ser alineados y mitigados. • Establecer procesos vigilantes para identificar riesgos no obvios o nuevos.
6.2 Objetivos de BCMS y planes para conseguiros.	• Alinear el programa a la necesidad de la empresa. • Los objetivos deben responder a la política de continuidad.
6.3 Medición de cumplimiento.	• Los objetivos deben ser claros, documentados, medidos y divulgados. • Se debe tener un panorama claro de los niveles de servicio mínimos aceptados.

Fuente: Elaboración propia a partir de los criterios de Drewitt (2013) e ISO (2012). D7- Soporte

Para poder ejecutar correctamente los objetivos estratégicos en torno a la continuidad del negocio, la organización debe hacer un análisis que le permita evaluar si cuenta con los recursos y capacidades necesarios para ejecutar. (Drewitt, 2013)

La correcta asignación de recursos, permite dar al programa la solidez y confianza para responder en el momento que la organización lo requiere. Parte de los recursos necesarios es el factor humano, por lo que parte del programa debe validar que los miembros cuenten con las competencias y capacidades necesarias.

Una vez elaborado un análisis interno, el programa se debe propagar a través de la organización de manera que cada individuo involucrado tenga claro su importancia (St-GERMAIN, 2014). Los planes de conciencia y comunicación permiten mitigar el impacto de los incidentes y, a la vez, evitar la generación de nuevos eventos adversos durante una situación de crisis.

Según Drewitt (2013), para que el BCMS funcione se debe elaborar la correspondiente documentación para que todo el personal esté informado sobre la operación y activación del mismo, por lo que los miembros del comité de continuidad deberán hacer esfuerzos para llevar controles documentales pertinentes tales como manejo de versiones, seguridad y disponibilidad de los datos.

Tabla 4 Componentes de la Sección 7

7.1 Aprovisionamiento de Recursos.	• Análisis de requerimientos. • Asignación de presupuestos. • Manejo de recurso humano.
7.2 Competencias del Comité.	• Capacitación del personal. • Elaboración de perfiles de trabajo y competencias requeridas.
7.3 Conciencia y Comunicación.	• Sistema de capacitación del personal. • Diseño de programas de conciencia. • Planes y evaluación de conocimiento.

Fuente: Elaboración propia a partir de los criterios de Drewitt (2013) e ISO (2012). s de Drewitt (2013) y ISO (2012). D8 Operación

La etapa D8 describe los elementos claves que sirven de núcleo de operación para fundamentar el trabajo realizado y cumplir con los requisitos de la noma. Dentro de la operación se debe realizar un BIA (Business Impact Analysis), el cual representa un estudio de los procesos críticos del negocio y su impacto en caso de perder el soporte del mismo. Para ISACA (2014), este análisis permite evitar los procesos huérfanos y la omisión de medidas en caso de un evento. Un BIA detallado permite obtener insumos valiosos para el BCMS, como lo es el criterio para fundamentar decisiones y la optimización de los resultados.

En complemento al BIA, una evaluación de riesgos (RA, risk assesment) permite determinar factores internos y externos que pueden afectar los procesos críticos de la organización (Drewitt, 2013). Esto le permitirá establecer una estrategia clara para abarcar cada escenario de riesgo posible.

Otro componente de esta sección es la estrategia para la continuidad del negocio, su función es describir cómo se va a minimizar el impacto de la interrupción en los servicios críticos (Drewitt, 2013). La estrategia describe la forma y el tiempo en el que los elementos identificados por el BIA son restaurados, por lo que esta debe ser integral con toda la organización.

Tabla 5 Componentes de la Sección 8

8.1 Análisis del Riesgo.	• Elaboración de un mapa de procesos críticos.
8.2 Análisis de Impacto.	• determinar las prioridades, objetivos y metas de continuidad y recuperación. • Evaluar el impacto en el tiempo de no realizar estas actividades. • Priorizar los plazos para reanudar estas actividades.
8.3 Estrategia de Continuidad.	• Protección de actividades prioritarias. • Establecimiento de planes para mitigar y responder a los eventos.
8.4 Respuesta a incidentes.	• documentar procedimientos y una estructura de gestión para responder a un incidente disruptivo.

	• Identificar los umbrales de impacto. • Disponer de procesos y procedimientos para la activación, operación, coordinación y comunicación la respuesta.
8.5Pruebas y ejercicios.	• Planes de simulación. • Revisión constante y afinamiento de los planes.

Fuente: Elaboración propia a partir de los criterios de Drewitt (2013) e ISO (2012)

D9 Evaluación del desempeño

La evaluación del desempeño y la mejora continua permiten afinar los sistemas de gestión de tal manera que estos puedan hacer crecer a la organización. A través de este proceso, los niveles superiores pueden concluir si los objetivos y métricas establecidos se están cumpliendo (St-GERMAIN, 2014)

Componentes	***Foco***
Supervisión, medición, análisis y evaluación,	• Se debe contar con métricas asociadas a los objetivos claros y medibles. • Debe existir un plan de seguimiento y control en el cumplimiento de

	métricas. • La organización deberá conservar la información apropiada documentada como evidencia de los resultados.
Auditoría interna.	• Contar con un plan de auditoría interna. • Velar por cumplimiento e independencia de las auditorías.
Revisión por la Dirección.	• Presentar planes a la alta dirección • Elaboración de informes. • Planes de acción sobre oportunidades de mejora.

Fuente: Elaboración propia a partir de los criterios de (Drewitt, 2013) e (ISO, 2012)

D9 Mejora

Al respecto, laa normativa ISO 2012 establece que se debe mejorar continuamente la conveniencia, adecuada y eficacia del sistema. Por lo que la detección de inconformidades al sistema deben ir asociadas a acciones correctivas para armonizar nuevamente el cumplimiento de objetivos.

Tabla 6 Componentes de la Sección 10

Componentes	***Foco***
Mejora.	• Detección de falencias al sistema. • Establecimiento de medidas correctivas. • Planes de mitigación. • Ajustes al sistema.

Fuente: Elaboración propia a partir de los criterios de Drewitt (2013) e ISO (2012).

Modelo de Trabajo

Para poder llevar a cabo la tarea descrita anteriormente, la normativa emplea el círculo de Deming, conocido como circulo PDCA. Mediante esta técnica se busca la mejora continua a través de los cuatro estados descritos en la Figura 2

El modelo de trabajo ofrece un lenguaje de trabajo común para que la organización defina la madurez de sus sistemas, sus capacidades, identifique y desarrolle nuevas prácticas para obtener un objetivo claro. (EverBridge, 2014). Por lo tanto, se puede afirmar que la práctica de este modelo brinda un marco común de trabajo para la ejecución y la búsqueda de un objetivo con cierto nivel de calidad deseada.

Figura 2 Modelo PDAC

Fuente: Elaboración propia basado en la teoría de (Cycle, 2009)

Con respecto a la normativa, la ISO 22301 opera de manera homóloga y lo describe en su apartado tres de la siguiente forma:

- Establecer (Plan): La etapa de establecimiento responde a la publicación de la política de continuidad, así como sus elementos asociados como lo son objetivos, proceso, procedimientos, entre otros Lo anterior en concordancia con los objetivos estratégicos de la organización.

- Implementación y Operación (Do): Corresponde al despliegue organizacional de las políticas, procedimientos, procesos y controles en ambiente de producción.

- Monitoreo y Revisión (Check): Corresponde a la evaluación del desempeño del sistema con respecto a las métricas establecidas y los objetivos. Una

vez realizado el estudio de cumplimiento se establecen acciones remediales o de mejora.

- Mantener y mejorar (Act): El sistema para la gestión de continuidad del negocio crece, mejora y se optimiza a través de acciones correctivas fundamentadas en insumos tales como pruebas de simulación y evaluación de métricas.

Capítulo III: Marco Metodológico

El presente proyecto tiene como objetivo evaluar el cumplimiento de los controles implementados en la organización, por lo que se realizará una evaluación y diagnóstico de la misma siguiendo los lineamientos de la metodología presentados a continuación.

Metodología de trabajo

La investigación a realizar es de tipo cualitativo, ya que se desea exponer la aplicación de una teoría propia de la rama administrativa dentro de un contexto tecnológico y, posteriormente, explicar los efectos sociales empresariales que puede tener.

Siguiendo a Martínez (2006), una investigación de índole cualitativa se basa en la observación natural, centralizándose en los fenómenos y su comprensión así como el enfoque a los procesos que describen el tema Dentro de las investigaciones cualitativas existen diferentes métodos basados en el tipo de realidad a investigar, Martínez (2006) describe en su trabajo los siguientes:

- Métodos hermenéuticos: Consisten en la realización de interpretaciones realizadas inconsciente o conscientemente por la mente humana en razón de dar un significado o justificación a los datos obtenidos
- Métodos fenomenológicos: Estudia fenómenos no vividos por el investigador, por lo que se debe confiar en la veracidad de los datos obtenidos.
- Métodos etnográficos: Investigan colectivos, ya sean sociales o empresariales, adaptando los datos, reglas o modos de vida de manera única correspondiente al grupo en cuestión.

- Método de investigación-acción: Este método se emplea cuando el investigador no solo analiza la situación sino que, además de eso, propone una solución.

La presente investigación empleará un método mixto, ya que se desea tanto conocer los niveles de cumplimiento como proponer una serie de mejoras y recomendaciones a través del informe final de auditoría

Fuentes de información

Para la elaboración de este proyecto se utilizarán varias fuentes de investigación para completar satisfactoriamente los capítulos desarrollados, dentro de las fuentes que se van a utilizar se emplearán fuentes primarias y secundarias, las cuales se definen como:

- **Fuentes primarias:** Dado la naturaleza teórica de la investigación se consultará la literatura correspondiente al tema para establecer los fundamentos teóricos del tema. Posteriormente, se recurrirá a la investigación de campo para tomar datos directamente del contexto empresarial a estudiar. Algunas fuentes a emplear podrían ser, sin limitarse a: libros, tesis doctorales, entrevistas, entre otras.
- **Fuentes secundarias:** Representa las fuentes secundarias para complementar la información obtenida de fuentes primarias, así como el uso de documentos científicos, artículos de revistas, entre otros.

Técnicas para la identificación de los hechos.

Con el fin de lograr los objetivos de este estudio, se emplearán instrumentos y técnicas orientados a extraer la información directamente de las fuentes. Basado en el trabajo de Martínez (200), se trabajarán técnicas como:

Observación participativa: Técnica primaria por excelencia de una investigación cualitativa. Consiste en convivir con los individuos de la población seleccionada para analizar sus conductas en un contexto alusivo al tema en la investigación.

Entrevista semiestructurada: Es un método especial en la recolección de la información, aplicada principalmente a personas que no poseen el tiempo para llenar un cuestionario. Consiste en la realización de diálogos con las personas interesadas, el investigador propone temas de manera estratégica de tal forma que la conversación fluya acorde a los temas.

Cuestionarios: Permite la recolección de información de un grupo grande de personas que se relacionan con el objeto de estudio.

Revisión de registros: Consiste en la revisión de la documentación pública de la empresa, así como de los registros propios del sujeto a investigar.

Instrumentos propuestos

Teniendo en considerando los objetivos de la presente investigación y con el fin obtener los datos necesarios para la investigación, se hará uso de instrumentos estadísticos y descriptivos. La tabla 4 describe los instrumentos propuestos, así como el tipo de aplicación y el objetivo de los mismos.

Tabla 7 Instrumentos Propuestos para la recolección de los datos

Instrumento	Tipo	Descripción	Objetivo
Entrevista de	Entrevista Semiestructur	Entrevista dirigida al oficial de cumplimiento y	Identificar los principales procesos involucrados en

Gerencia.	ada.	al gerente de continuidad del negocio como un primer aproximamiento a la organización.	la gestión diaria de la empresa y el papel que ocupa el BCMS en la misma.
Formulario de Documentación Interna.	Observación Participativa.	Guía para indagar entre los miembros del departamento seguridad de la información y cumplimiento de los procesos.	Identificar los procesos críticos involucrados en la continuidad del negocio.
Instrumento de Auditoría BCMS.	Cuestionario.	Formulario basado en las mejores practica de gestión de para la continuidad del negocio.	Evaluar el sistema actual de gestión para la continuidad de la operación.

Fuente: Elaboración Propia.

Validez y confiabilidad del instrumento

Los instrumentos son sometidos a consideración de profesores con experiencia en el campo de la investigación y la estadística, se someten a validación con un grupo reducido de funcionarios para obtener retroalimentación.

Capítulo IV- Contexto Organizacional

J&A Consulting

La empresa en donde se va a realizar la práctica profesional trabaja con empresas y datos del sector financiero, por lo que cuenta con estrictos controles de seguridad de la información. Por lo anterior, para efectos de este trabajo, su nombre real no será divulgado sino que se trabajará bajo la figura de J&A Consulting.

J&A Consulting fue fundada a mediados de la década de los noventa grupo de empresarios especializados en mercados capitales gracias a una amplia y exitosa trayectoria en el sector financiero en los bloques financieros de Asia y Estados Unidos.

Originalmente la empresa se encargaba de brindar servicios tercerizados bajo el modelo BPO (Business Process Outsourcing), brindando soporte en procesos como planillas, contabilidad y recursos humanos a múltiples clientes Asia y Europa. Sin embargo, durante el año 2001, un proceso reestructuración organizacional los llevó a dirigir sus esfuerzos y planes estratégicos a convertirse en una organización de servicios de KPO (Knowledge Process Outsourcing), por lo cual su cartera de servicios se vio diversificada exponencialmente y fue necesario expandir operaciones desde Asia a lo largo del planeta.

Como parte de la restructuración, el nuevo núcleo de negocios se tornó a la investigación financiera, por lo que una serie de verticales se generó para satisfacer las necesidades de grandes inversores en la bolsa. Algunas de las líneas que actualmente se ofrecen a los clientes son:

- Renta variable: Investigación y modelado financiero con respecto a las acciones de una empresa, elaboración de reportes gracias a información publicada para accionistas e interesados y análisis de predicciones de mercado. Los resultados de estas investigaciones son vendidos a los

posibles inversores, quienes tomarán sus decisiones basados en los criterios financieros estipulados.

- Servicios cuantitativos: En la gama de servicios cuantitativos se brinda soporte a través de modelos matemáticos, análisis estadísticos y soluciones programadas a la medida del cliente. La automatización de resultados y modelos económicos le permitirán a los clientes optimizar los tiempos de investigación y dedicar este a mejorar las inversiones de la organización.
- Renta fijas: Investigación de bonos y monitoreo de los mismos. Permite elaborar estrategias de inversión a partir del análisis de comportamiento y riesgo de estos.
- Auditoría de cumplimiento: Consiste en brindar soporte a la operación de los equipos de Auditoría y Cumplimiento de los clientes; departamento encargado de garantizar el acatamiento de normativas, contratos y estándares implementados por la empresa. Permite a estos realizar labores más complejas en tiempos menores y con resultados óptimos, además de reducir los costes del mismo. Asimismo, hace auditoría de correos, revisión de material para la publicación, vigilancia de transacciones bursátiles por parte de los empleados, soporte a las políticas empresariales, entre otros, son los servicios que se ofrecen en esta área.

Estructura de Operaciones

En la actualidad, la organización cuenta con ocho centros de investigación financiera a lo largo del planeta. Esta plataforma global permite cubrir las diversas necesidades de los clientes con respecto a costos, niveles de servicio y operaciones.

A nivel corporativo, la empresa cuenta con niveles departamentos o niveles jerárquicos, estos se caracterizan de la siguiente manera.

Primeramente, el nivel superior de la jerarquía lo compone la junta directiva, la cual está conformada por los socios fundadores y dos representantes de la junta

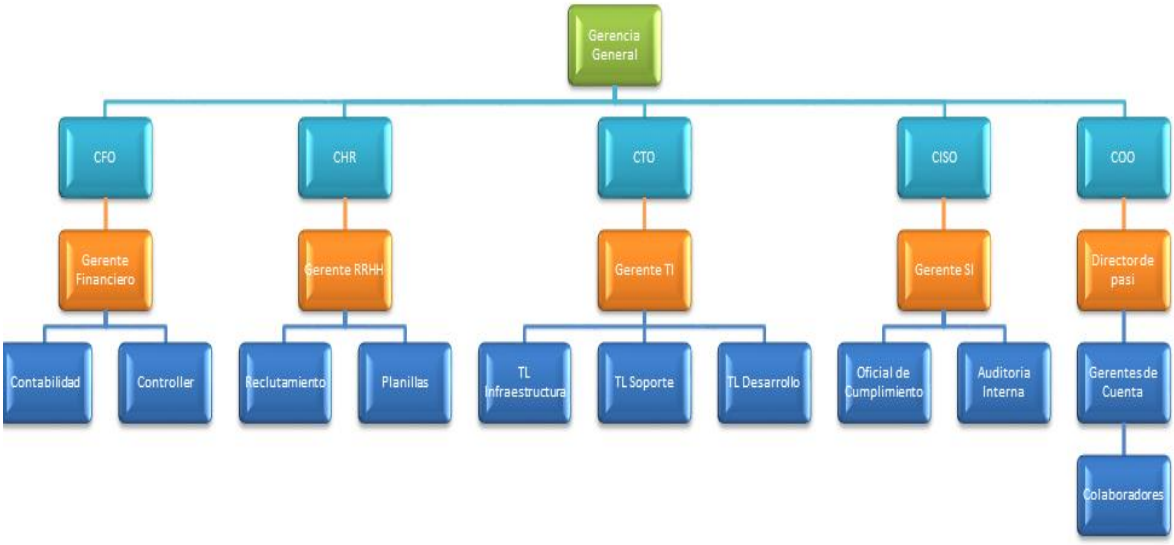
de accionistas minoritarios, estos velan por los intereses financieros de la organización y el crecimiento de la misma.
Seguidamente, se encuentra el comité ejecutivo, en esta entidad se encuentra el CEO de la corporación junto con los principales directores de la empresa: Operaciones (COO), Financiero (CFO), Mercadeo (CMO), Tecnología (CTO), Seguridad de la información (CISO), Recursos Humanos, Cumplimiento y Legal. Cabe decir que este comité vela por la elaboración de la estrategia de la organización, que responda a las necesidades de los accionistas.

El tercer nivel corresponde a las gerencias tácticas ubicadas en cada país, por lo general, cada locación cuenta con un equipo de gerentes, quienes les responden a sus direcciones globales, sin embargo, a la vez responden al director del país.

Un cuarto nivel consiste en el entorno de producción, este está conformado por los consultores , ejecutivos, analistas, entre otros, quienes son facturables a los clientes y generan los ingresos, pues brindar los servicios en el área de negocio. Este nivel está conformado por una subestructura administrativa de ocho rangos y tres roles (Colaborador, Supervisor, Gerente de Cuenta).

Considerando lo anterior, se puede elaborar un organigrama institucional de la siguiente manera:

Figura 3 Organigrama J&A Consulting



4.3 Modelo de negocios

El modelo de negocios está basado en la venta de servicios de investigación a la medida, por lo que cada cliente puede representar un proceso totalmente diferente. Para poder homologar los procesos, se trabaja con paquetes de cliente basados en modelos relacionales, es decir; cada compromiso de servicios actúa según la relación que los analistas de la empresa usuaria desee ejecutar. Algunos de estos modelos son:

- Peer to Peer: Este tipo de relación representa una relación “uno a uno”, pues es con el analista cliente y el analista de servicio, es decir; el cliente incorpora al analista de servicio como un recurso propio, el segundo trabaja bajo la demanda del primero. La diferencia es que la línea de reporte y las obligaciones laborales se mantienen en la empresa de servicios.

- Pool: En este modelo existe un equipo de analistas de la empresa de servicios que trabajan para un único cliente, este equipo factura por horas y no mantienen dedicación exclusiva hacia el cliente.

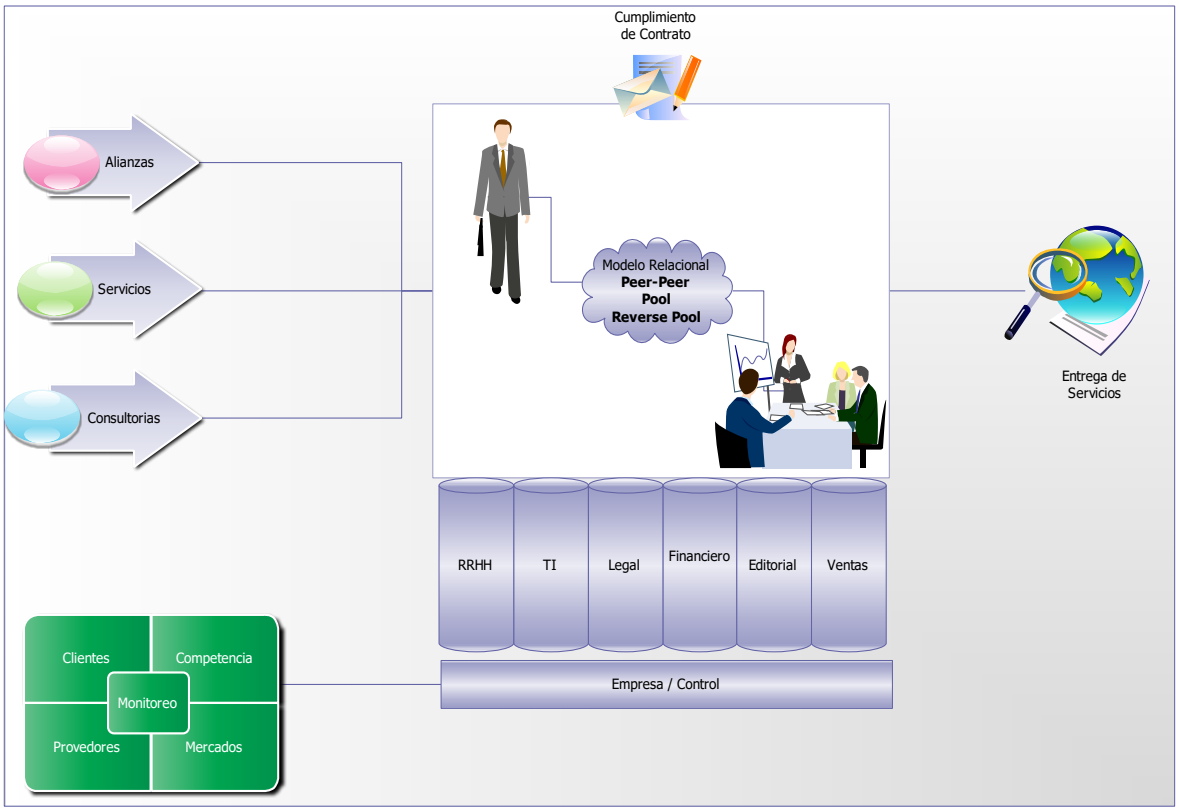
- Reverse Outsourcing: Para este modelo, la empresa vende la dirección de un equipo del cliente, es decir, la empresa usuaria brinda un líder responsable a un equipo de empleados del cliente.

- Fixed: Consiste en la elaboración de una solución a la medida para el cliente a partir de los modelos anteriores.

Al modelo de relación se le considera el núcleo del compromiso con el cliente, sin embargo, para que este modelo opere correctamente se le agrega un marco de soporte funcional que articula las funciones y recursos de los empleados antes de ser entregados a los clientes. De tal forma, los departamentos de soporte como Legal, Cumplimiento, Recursos Humanos, Tecnologías de Información, Editorial, Financiero; modelan el ambiente donde se desarrolla la interacción cliente, limitando siempre este ambiente a los controles establecidos por obligaciones contractuales y los controles internos.

La imagen a continuación describe la operación del modelo de negocio, donde se puede ver cómo la relación cliente-analista de servicios es sustentada por los departamentos de soporte. Además, se observa cómo este tiene como entradas las alianzas del mercado, los servicios ofrecidos y el apoyo de consultorías de implementación.

Figura 4 Modelo de operaciones J&A Consulting



Fuente: Elaboración Propia

Además del modelo representado anteriormente, la compañía emplea un modelo de negocio local, que es una tropicalización del global, pues se basa en un plan estratégico de negocios que es revisado por la junta directiva anualmente. Para efectos administrativos, las gerencias locales responden a los directores en Asia. Sin embargo, los productos y servicios corporativos funcionan como uno solo, pues se sigue la filosofía “Follow the Sum”, en la cual las políticas y los procedimientos globales de cada centro de investigación opera de manera semejante a la casa matriz.

Para efectos de esta investigación, se establece en el alcance la ubicación de Costa Rica, como centro de investigación elegido para la evaluación. Dentro de las particularidades de este centro está su alianza con universidades públicas y los

convenios globales de la organización El modelo de servicios brinda cartera de clientes que opera con más de 80 compañías a nivel mundial, entre ellas seis de los 15 bancos más grandes del mundo, así como firmas de inversiones y corredores de bolsa en Wall Street, entre otros.

Gracias a los servicios ofrecidos, sus clientes se han visto beneficiados al reducir costos y aumentar sus ganancias. Por ejemplo, un banco de inversiones obtuvo ganancias de 18 millones de dólares gracias a las soluciones cuantitativas, y una reducción de costos por 7.2 millones de dólares.

Capítulo V: Propuesta de Plan de Auditoría ISO 22301

Introducción

Con el fin de comprobar y evaluar el cumplimiento de la norma ISO 22301 sobre un Sistema de Gestión para la continuidad del negocio, se ha desarrollado un programa de auditoría el cual verifica el cumplimiento de los controles de la organización con respecto a la normativa.

El programa de auditoría abarca los procesos de aproximación a la organización, comprensión y evaluación de la misma, así como una herramienta automatizada asociada a las pruebas fundamentadas en los riesgos que pueden afectar los sistemas de continuidad.

Figura 5 : Metodología de Auditoría propuesta para el trabajo.

Fuente: Elaboración propia.

Pre-auditoría

La etapa de pre auditoría tiene como fin elaborar una aproximación inicial del grupo ejecutor de la auditoría a la organización. A través de la ejecución de los instrumentos descritos más adelante, se pretende orientar e incluir al equipo en un proceso de inducción tanto a la cultura organizacional como sus procesos administrativos.

A continuación se describen los documentos a emplear para la ejecución de dicha etapa:

Tabla 8 Documentos propuestos para Pre-Auditoría

Identificación	Nombre	Tipo	Objetivo
BCMS-2014-PP-01	Programa Revisión Preliminar	Plan	Brindar al auditor información y conocimiento en general de la organización, los procesos y las actividades involucrados en el proceso de auditoría, así como de los factores externos que, en conjunto, representan el contexto en que la compañía se desarrolla.
BCMS-2014-PP-02	BCMS-2014-PP-02 Guía de Primer Acercamiento	Formulario	Recopilar y analizar información general de las actividades y procesos, con el propósito de adquirir conocimiento sobre las principales funciones que realiza la unidad a evaluar, específicamente en el sistema de gestión para la continuidad

			del negocio.
BCMS-2014-PP-03	Estructura Organizacional	Formulario	Entender la estructura y los procesos de la organización, así como sus demencias y líneas de negocios.
BCMS-2014-PP-04	Organizacional Cultura	Entrevista	Identificar los principales elementos que generan un marco de cultura organizacional, para entender la operación interna de la organización.
BCMS-2014-PP-05	Documentos Institucionales	Formulario	Inducir al equipo de auditoría en el marco de control y gobernanza en que la organización se desempeña.
BCMS-2014-PP-06	Sistemas de información Corporativos	Entrevista	Inducir al equipo de auditoría en el marco de control y gobernanza de tecnologías de información.
BCMS-2014-PP-07	Entrevista semiestructurada BCMS	Entrevista	Interpretar el sentimiento y la percepción de la gerencia de la organización respecto de la continuidad del negocio.
BCMS-2014-PP-08	Visita guiada a la empresa	Guía Visita	Entender el contexto organizacional y asimilar las implicaciones de la operación diaria en la empresa.

Una vez finalizado el proceso de auditoría preliminar se espera que el equipo de auditoría cuente con el conocimiento necesario para modelar las pruebas de control y la ejecución de la auditoría.

Planificación

El proceso de planificación de la auditoría le brinda al equipo de auditoría la guía necesaria para ejecutar las evaluaciones sobre los controles implementados por la organización.

El compendio de documentos en la etapa de planificación tiene como fin guiar a los responsables de la ejecución a través de los requerimientos de la normativa y asociarlos a una metodología de trabajo la cual permita posteriormente emitir criterio sobre el sistema de gestión para la continuidad del negocio.

A continuación se describen los documentos asociados a esta etapa:

Tabla 9 Documentos Propuestos para Planificación del a Auditoría

Identificación	Nombre	Tipo	Objetivo
BCMS-2014-P-PA-01	Plan de Auditoría	Plan	Documento principal de guía, elaborado y revisado por el equipo de auditoría, este contiene el propósito, objetivos, alcances y procedimientos a realizar durante la etapa de ejecución.
BCMS-2014-PC-01	Sección 4	Prueba de Control	Prueba de control que tiene como fin realizar una evaluación del contexto de la organización, los marcos regulatorios, las partes interesadas, dimensionamiento del alcance del plan de continuidad y la utilización de sistemas de continuidad del negocio como elemento habilitador de capacidades ante un incidente

			disruptivo.
BCMS-2014-PC-02	Sección 5	Prueba de Control	Prueba de control que tiene como fin analizar el compromiso del equipo estratégico de la organización como elemento responsable del liderazgo y patrocinio del sistema de continuidad del negocio. Además, confirmar la existencia de un comité gerencial y del manejo de las políticas de compromiso en torno al tema de continuidad del negocio.
BCMS-2014-PC-04	Sección 6	Prueba de Control	Prueba de control que tiene como fin estudiar el proceso de planificación realizado para sustentar el proceso de continuidad del negocio y sus actividades de soporte.
BCMS-2014-PC-05	Sección 7	Prueba de Control	Indagar los mecanismos de soporte al sistema de continuidad del negocio, así como los procesos de asignación de recursos al programa, el manejo del personal ante incidentes, capacidades y competencias del equipo responsable, los planes de capacitación, concientización y soporte.
BCMS-2014-PC-06	Sección 8	Prueba de Control	Prueba de control que tiene como fin verificar la correcta operación del sistema de gestión de la continuidad del negocio, así como la existencia de

			componentes claves
BCMS-2014-PC-07	Sección 9	Prueba de Control	Prueba de control que tiene como fin revisar los mecanismos de evaluación y desempeño, así como el proceso de establecimiento de métricas en concordancia a los requerimientos del negocio y los objetivos estratégicos a los que corresponde.
BCMS-2014-PC-08	Sección 10	Prueba de Control	Prueba de control que tiene como fin Demostrar la existencia de procesos de mejora continua a través del tratamiento de planes de corrección, manejo de inconformidades y aseguramiento de calidad.

Una vez finalizada la revisión de las pruebas descritas anteriormente, el equipo de auditoría deberá realizar los ajustes necesarios a las mismas o redimensionar el trabajo con el fin de adaptar el plan de auditoría a la organización, esto con ayuda de la información recopilada durante la pre-auditoría.

Ejecución

El proceso de ejecución de la auditoría permitirá al equipo ejecutor analizar los controles implementados por la organización auditada bajo el marco de referencia ISO 22301. De tal forma que los auditores, con ayuda de varias herramientas, el criterio experto y la norma como tal podrán evaluar, de manera ordenada y sistemática, las políticas, los procedimientos, los procesos de trabajo, los controles y demás elementos asociados a su sistema para la gestión de la continuidad del negocio.

El equipo de auditoría tendrá como responsabilidad convocar al encargado del proceso y a los líderes de área con el fin de ejecutar los cuestionarios descritos en las pruebas, a través de esta herramienta los auditores deberán recopilar información y documentarla en las hojas de hallazgos y papeles de trabajo. Una vez finalizada la prueba de control el auditor empleará dicha información como base para su informe de resultados.

Los documentos disponibles para esta etapa de ejecución son:

Tabla 10 Documentos Propuestos para Ejecución del a Auditoría

Identificación	Nombre	Tipo	Objetivo
BCMS-2014-E1	Notificación de Inicio de Auditoría	Oficio	A través de este oficio el departamento de auditoría notifica a los auditados del comienzo de la auditoría como solicitud de la alta gerencia.
BCMS-2014-E2	Formulario de Entrevista	Formulario	Mediante este formulario el auditor da constancia de que clase de prueba va a ejecutar sobre el auditado, así como los parámetros de la misma. El auditado antes de iniciar debe firmar como prueba de que se le ejecuto el mismo.
BCMS-2014-E3	Cedula de Hallazgo	Plantilla	Documento estándar para reportar un hallazgo de auditoría.
BCMS-2014-E4	Índice de Hallazgos	Formulario	Documento de control de todos los hallazgos identificados, la sección correspondiente y sus datos

			asociados.
BCMS-2014-E5	Sección 4	Herramienta Electrónica	Herramienta automatizada para la evaluación y la estandarización de resultados.
BCMS-2014-E6	Sección 5	Herramienta Electrónica	Herramienta automatizada para la evaluación y la estandarización de resultados.
BCMS-2014-E7	Sección 6	Herramienta Electrónica	Herramienta automatizada para la evaluación y la estandarización de resultados.
BCMS-2014-E8	Sección 7	Herramienta Electrónica	Herramienta automatizada para la evaluación y la estandarización de resultados.
BCMS-2014-E9	Sección 8	Herramienta Electrónica	Herramienta automatizada para la evaluación y la estandarización de resultados.
BCMS-2014-E10	Sección 9	Herramienta Electrónica	Herramienta automatizada para la evaluación y la estandarización de resultados.
BCMS-2014-E11	Sección 10	Herramienta Electrónica	Herramienta automatizada para la evaluación y la estandarización de resultados.

Comunicación

Para la etapa de comunicación, el equipo de auditoría deberá brindar un informe detallado de los hallazgos encontrados durante la etapa anterior. Para ello se empleará el formato de reporte de auditoría descrito más adelante. Este informe final tiene como fin informar a la gerencia los resultados obtenidos y el criterio que el equipo ha de emitir con respecto al BCMS. Esta etapa propone el siguiente documento:

Tabla 11 Documentos Propuestos para Comunicación de Resultados de la Auditoría

Identificación	Nombre	Tipo	Objetivo
BCMS-2014-C1	Informe Final de Auditoría	Plantilla	Presentar los hallazgos obtenidos durante la auditoría a la alta gerencia de la organización y a las partes interesadas, así como un conjunto de recomendaciones basadas en los criterios técnicos de los auditores.

Capítulo VI Conclusiones

Los entornos globalizados representan riesgos mucho más complejos para las corporaciones debido al cambio de paradigma en las operaciones, por lo que para mitigar la posibilidad de la materialización de amenazas que impacten el negocio se deben implementar mecanismos tales como procesos de gestión de la continuidad del negocio.

Se entiende que una correcta aplicación de estándares para la continuidad del negocio brinda a la organización las capacidades necesarias para sobrevivir a eventos disruptivos, los cuales pueden comprometer las funciones críticas del negocio.

Además, el elemento clave para que una organización pueda implementar de manera integral y armonizada un sistema de gestión para la continuidad del negocio, es necesario el compromiso de las máximas autoridades, de tal manera que los objetivos, alcances, políticas y procedimientos para BCMS estén alineados con el negocio.

Uno de los principales elementos para modelar los sistemas de continuidad de negocio es la correcta elaboración de un BIA (Business Impact Analysis) en donde se determinen los procesos críticos para el negocio y las dependencias necesarias para continuar brindando los servicios acordados a un nivel aceptable.

Como consecuencia de las entradas obtenidas a partir del BIA, la organización puede tener un mayor entendimiento del contexto organizacional y, así, poder asociar los procesos críticos al alcance de los planes de gestión para la continuidad del negocio.

Asimismo, se puede afirmar que la elaboración de herramientas automatizadas para validar el cumplimiento de los requisitos estipulados por la normativa ISO facilita la toma de decisiones, identifica fácilmente puntos de mejora y permite a

los equipos de auditoría controlar el sistema para la continuidad del negocio de manera eficiente.

Capitulo VII Recomendaciones

Los procesos de operación para la continuidad del negocio deben llevarse a cabo por personal capacitado y empoderado por la política para BCMS publicada y elaborada por la alta gerencia. En caso contrario, se corre el riesgo de que el funcionamiento del sistema no sea preciso y acorde a los objetivos organizacionales.

Asimismo, una correcta gestión de incidentes permite detectar eventos o conductas críticas que pueden impactar la organización y desencadenar el proceso de activación de los planes de continuidad y recuperación del negocio.

Relacionado con el punto anterior, los sistemas de continuidad del negocio y las iniciativas gerenciales para la gestión de los mismos deben ser evaluados periódicamente, ya sea para la mejora continua y los planes programados o por cualquier cambio en el entorno que pueda afectar a la organización.

Un mecanismo recomendado para la mejora y cumplimiento de los BCMS son las auditorías de cumplimiento, estas permiten analizar la eficiencia y eficacia de los controles asociados a los procesos para la continuidad del negocio elaborados por el comité para la continuidad del negocio.

Para poder llevar a cabo una auditoría de manera ordenada y estructurada se debe establecer un plan de auditoría, el cual corresponde a un documento que detalla los objetivos, alcances, actividades y responsables de la evaluación de los diferentes dominios o secciones que norman los sistemas.

En el caso de la normativa ISO 22301, dada lo importante del seguimiento y del control de las actividades descritas, es importante contar con herramientas automatizadas de evaluación.

La elaboración de pruebas de cumplimiento tiene como fin la validación de la existencia de controles asociados a los requisitos de la normativa ISO 22301, de tal forma que dichas actividades en concordancia a los objetivos de auditoría

brindan una metodología al auditor para identificar la eficiencia y eficacia de los controles y actividades realizadas acabo.

Finalmente, una vez elaboradas las pruebas de control, el auditor debe recabar información suficiente y adecuada para justificar los hallazgos que, posteriormente, comunicará a la gerencia.

Referencias

Alcantara, P. (2014). COUNTING THE COST. *Business Continuity Awareness* .

Cycle, E. o. (2009). *Ronald Moen,Clifford Norman.* Associates in Process Improvement-Detroit.

Drewitt, T. (2013). *A Manager´s Guide to ISO22301.* Cambridgeshire: IT Governance Publishing.

EverBridge. (15 de 11 de 2014). ISO 22301 & 22313 Business Continuity Management System Standards and Application for Incident Communication Plans. Obtenido de Everbridge: http://go.everbridge.com/rs/everbridge/images/Whitepaper_ISO22301_022513.pdf

FFIEC. (2003). *BCP - IT Examintation Handbook.* Federal Financial Institutions Examination Council.

GALLAGHER, M. (2003). *Business Continuity : How to protect your company.* Prentice Hall.

ISACA. (06 de 11 de 2014). *Glosario ISACA*. Obtenido de http://www.isaca.org/Pages/Glossary.aspx

ISO. (2012). *Societal security - Business Continuity management systems.* International Standard Organization .

MARTÍNEZ, M. (2006). LA INVESTIGACIÓN CUALITATIVA (SÍNTESIS CONCEPTUAL). *REVISTA IIPSI*, 123 - 146.

Ponemon Institute LLC. (2013). *2013 Cost of Data Center Outages.* Michigan: Ponemon Institute© Research Report.

Risk Cover. (2009). *BUSINESS CONTINUITY MANAGEMENT GUIDELINES.* Australian: Risk Cover.

St-GERMAIN, R. (06 de 11 de 2014). *Socieltal Sercurity Business Continuity management Systems.* Obtenido de http://pecb.org/iso22301es/iso22301_whitepaper_es.pdf

Zawada, B. (2014). The practical application of ISO 22301. *Journal of Business Continuity & Emergency Planning Volume 8 Number 1*, 83-90.

Anexos

Anexo #	1	**Nombre**	BCMS-2014-PP-01 Programa Revisión Preliminar
Etapa	Planificación Preliminar	**Archivo**	 BCMS-2014-PP-01 Programa Revision F

Programa para la Revisión Preliminar

Objetivo:

Brindar al auditor información y conocimiento en general de la organización sobre los procesos y actividades involucrados en el proceso de auditoría y sobre los factores externos que, en conjunto, representan el contexto en que la misma se desarrolla.

Alcance

Se analizará y recopilará información sobre las actividades sustantivas de la organización y de otros aspectos que se consideren importantes para el estudio. El periodo de la revisión es el ciclo 2014, comprendido entre enero 1 y diciembre 31.

	Procedimientos	***Responsable***	***Ref. P/T.***
1	***Aspectos Generales***		
	1.1- Antecedentes de la actividad sustantiva de la unidad ejecutora a evaluar.		*BCMS-2014-PP-02*
	1.2- Estructura orgánica y funcional, a fin de		*BCMS-2014-PP-03*

	Procedimientos	Responsable	Ref. P/T.
	determinar los niveles de jerarquía y responsabilidad de las dependencias que componen la unidad ejecutora. Verificar si la organización de la unidad responde a dicha estructura aprobada.		
	1.3- Revisión y análisis de la programación estratégica y operativa de la unidad, a fin que determine los objetivos estratégicos y operativos y los mecanismos que se aplican para su control y evaluación.		*BCMS-2014-PP-04*
	1.4- Solicitud de los reglamentos, manuales de procedimientos, instructivos, circulares, políticas, pronunciamientos, estudios técnicos, etc., de interés, que fundamenten la actividad o proceso a evaluar. Verificar si están actualizados.		*BCMS-2014-PP-05*
	1.5- Indagación sobre el sistema de información, referente a los programas informáticos en operación y los diferentes reportes o informes que se emiten.		*BCMS-2014-PP-06*
2	***Informes de Auditorías***		
	2.1- Revise y analice los últimos informes de evaluaciones realizadas por la Auditoría Interna, Contraloría General de la República u otras instancias. ***Fuente**: Archivo permanente de la Auditoría Interna.*		*N/A*
3	***Entrevistas***		
	3.1- Seleccione y aplique entrevistas a los		*BCMS-2014-PP-07*

	Procedimientos	Responsable	Ref. P/T.
	funcionarios encargados de las actividades sustantivas de la unidad, con el fin de conocer y ampliar la información sobre la ejecución de las funciones de la unidad ejecutora. *Elaborar una guía de los aspectos a tratar en la entrevista, considerando los siguientes asuntos;* *- Objetivos de la actividad* *- Como se planifican las actividades.* *- Volumen de producción o resultados de la actividad.* *- Procedimientos de control y evaluación de resultados establecidos.* *- Recursos humanos y materiales asignados.* *- Problemas o limitaciones presentados en la ejecución de la actividad a evaluar.* *- Planes a corto y mediano plazo.* *- Otros que considere necesario.* *Una vez concluida la entrevista efectuar un resumen de los aspectos relevantes. En este caso no se requiere la firma de la entrevista por parte del funcionario, ya que la misma versa sobre aspectos generales.* ***Fuente**; Funcionarios de la unidad a auditar.*		

	Procedimientos	Responsable	Ref. P/T.
4	***Inspección Física***		
	4.1- Inspeccione las instalaciones de la unidad ejecutora a evaluar, para tales efectos solicite a la Jefatura la colaboración para que lo acompañe en el recorrido. - *Observación sobre seguridad y mantenimiento de la infraestructura.* - *Distribución de áreas de trabajo, accesibilidad y seguridad.* *4.2.- Visita a otras instituciones o empresas para realizar análisis comparativo referente al tema de estudio.* ***Fuente**; Instalaciones de la unidad a auditar*		*BCMS-2014-PP-08*
Fecha Inicio:			***Fecha Finalización:***
Responsable:			

Anexo #	2	**Nombre**	BCMS-2014-PP-02 Guía de Primer Airamiento
Etapa	Planificación Preliminar	**Archivo**	 BCMS-2014-PP-02 Guia de Primer Aera

GUIA DE PRIMER ACERCAMIENTO

1- Objetivo:

Recopilar y analizar información general de las actividades y los procesos, con el propósito de adquirir conocimiento sobre las principales funciones que realiza la unidad a evaluar, específicamente en el sistema de gestión para la continuidad del negocio.

2- Procedimiento:

Recopile la siguiente información de la organización en estudio:

- Contexto histórico de la organización.
- Ubicación de oficinas centrales y sucursales.
- Sector en que la organización se desenvuelve.
- Principales productos y servicios.
- Agentes internos de operación.
- Agentes Externo de operación.
- Estructura organizacional.
- Modelo de negocios.
- Clientes.

3 Consideraciones

Las evidencias obtenidas deben ser indexadas en los papeles de trabajo empleando la nomenclatura BCMS-2014-PA-P-02-PPn. La información obtenida debe ser utilizada para la elaboración de un perfil fijo de la organización.

4 Control de auditoría

Asignado		Revisado	
Fecha		Fecha	

Anexo #	3	**Nombre**	BCMS-2014-PP-03 Estructura Organizacional
Etapa	Planificación Preliminar	**Archivo**	BCMS-2014-PP-03 Estrutura Organizaic

Estructura Organizacional

1. Objetivo:

Recopilar y analizar información general de las actividades y procesos, con el propósito de adquirir conocimiento sobre las principales funciones que realiza la unidad a evaluar, específicamente en el sistema de gestión para la continuidad del negocio.

2. Procedimiento:

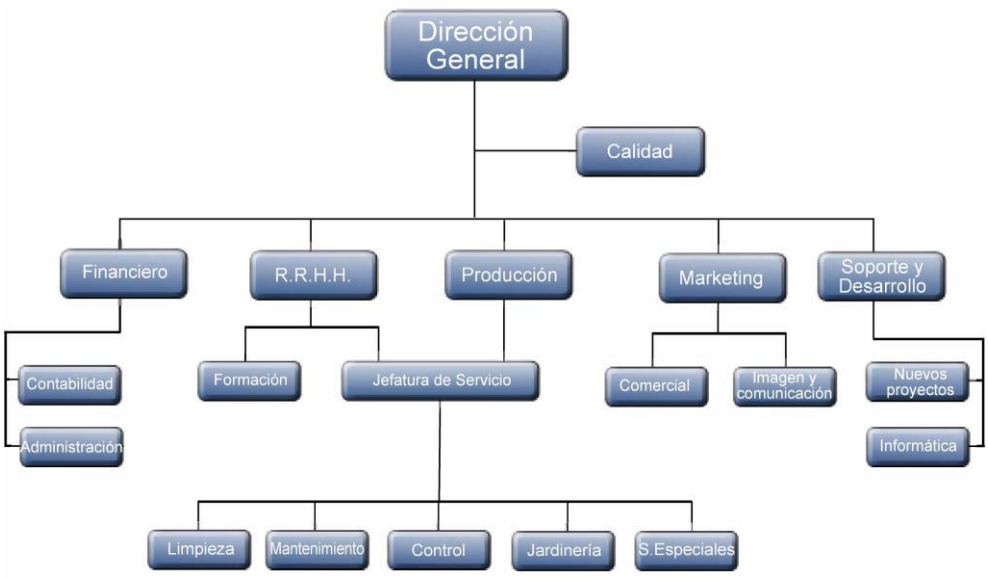
2.1. Identifique al máximo jerarca de la organización y sus líneas de reporte globales.

Nombre	Puesto	Teléfono	Email	Ubicación

2.2. Identifique las gerencias estratégicas y sus representantes.

Departamento	Representante	Contacto	Ubicación	# de Miembros

2.3. Solicite el organigrama de la institución(Muestra).



3. Consideraciones

Las evidencias obtenidas deben ser indexadas en los papeles de trabajo empleando la nomenclatura BCMS-2014-PA-P-03-PPn. La información obtenida debe ser utilizada para la elaboración de un perfil fijo de la organización.

4. Control de auditoría

Asignado		Revisado	
Fecha		Fecha	

Anexo #	4	**Nombre**	BCMS-2014-PP-04 Organizacional Cultura
Etapa	Planificación Preliminar	**Archivo**	BCMS-2014-PP-04 Organizaional Cultu

Estructura Organizacional

1. Objetivo:

Recopilar y analizar información general de las actividades y procesos, con el propósito de adquirir conocimiento sobre las principales funciones que realiza la unidad a evaluar, específicamente en el Área de Teletrabajo.

2. Procedimiento:

Identifique los siguientes elementos de la cultura organizacional:

- Misión
- Visión
- Valores
- Simbolismos
- Objetivos.

3. Consideraciones

Las evidencias obtenidas deben ser indexadas en los papeles de trabajo empleando la nomenclatura BCMS-2014-PA-04-PPn. La información obtenida debe ser utilizada para la elaboración de un perfil fijo de la organización.

4. Control de auditoría

Asignado		Revisado	
Fecha		Fecha	

Anexo #	5	**Nombre**	BCMS-2014-PP-05 Documentos Institucionales
Etapa	Planificación Preliminar	**Archivo**	BCMS-2014-PP-05 Documentos Institu

Estructura Organizacional

1. Objetivo:

Recopilar y analizar información general de las actividades y procesos, con el propósito de adquirir conocimiento sobre las principales funciones que realiza la unidad a evaluar, específicamente en el Área de Teletrabajo.

2- Procedimiento:

Identifique los siguientes documentales:

- Políticas
- Procedimientos
- Instrucciones de trabajo
- Manuales de operaciones

Para entendimiento y control llenar la siguiente tabla:

Nombre	Categoría	Departamento	Descripción	Versión

3. Consideraciones

Las evidencias obtenidas deben ser indexadas en los papeles de trabajo empleando la nomenclatura BCMS-2014-PA-05-PPn. La información obtenida debe ser utilizada para la elaboración de un perfil fijo de la organización.

4. Control de auditoría

Asignado		Revisado	
Fecha		Fecha	

Anexo #	6	**Nombre**	BCMS-2014-PP-06 Sistemas de información Corporativos
Etapa	Planificación Preliminar	**Archivo**	 BCMS-2014-PP-06 Sistemas de informa

Sistemas de Información Corporativos

1. Objetivo:

Recopilar y analizar información general de las actividades y los procesos, con el propósito de adquirir conocimiento sobre las principales funciones que realiza la unidad a evaluar, específicamente en el Área de Teletrabajo.

2. Procedimiento:

Solicite la información correspondiente a los sistemas de información que brindan soporte a las operaciones:

Nombre	Categoría	Departamento	Descripción	Plataforma	Servicio

3. Consideraciones:

Las evidencias obtenidas deben ser indexadas en los papeles de trabajo empleando la nomenclatura BCMS-2014-PA-06-PPn. La información obtenida debe ser utilizada para la elaboración de un perfil fijo de la organización.

4. Control de auditoría:

Asignado		Revisado	
Fecha		Fecha	

Anexo #	7	**Nombre**	BCMS-2014-PP-07 Entrevista semiestructurada BCMS
Etapa	Planificación Preliminar	**Archivo**	 BCMS-2014-PP-07 Entrevista semiestru

Entrevista semiestructurada BCMS

1. Objetivo:

Recopilar y analizar información general de las actividades y los procesos, con el propósito de adquirir conocimiento sobre las principales funciones que realiza la unidad a evaluar, específicamente en el Área de Teletrabajo.

2. Procedimiento:

Elaborar una entrevista a los miembros de las diferentes áreas funcionales de la organización, con el fin de entender cada unidad y sus características en el contexto de la continuidad del negocio. La entrevista consistirá en una serie de preguntas abiertas a discusión. El equipo de auditoría tomará nota sobre los aspectos relevantes.

Entrevista Departamentos y Continuidad del Negocio			
Nombre		Puesto	
Antigüedad		Departamento	
Cuestionario			
1	Por favor describa la función de su departamento en la organización.		

2	Describa los principales procesos que componen su departamento.
3	¿Cuáles son los principales productos y servicios que ofrece su departamento?
4	¿Cuál es el perfil de las personas que operan en su departamento?
5	¿Cuáles son los principales insumos para su departamento?
6	¿Considera que una eventual suspensión de sus operaciones puede impactar críticamente la organización?
7	Por favor mencione las principales amenazas que pueden afectar la operación de su departamento.
8	¿Cuáles son las principales regulaciones de la organización sobre su departamento?
9	¿Cuáles son las principales métricas de operación para su departamento?
10	Describa los planes remediales que cuenta su departamento ante eventuales incidentes disruptivos.
11	¿Sabe que son los sistemas para la continuidad del negocio?
12	Considera que la aplicación de técnicas de continuidad del negocio es beneficiosa para su departamento.

3 Control de auditoría

Asignado		Revisado	
Fecha		Fecha	

Anexo #	8	**Nombre**	BCMS-2014-PP-08 Visita guiada a la empresa
Etapa	Planificación Preliminar	**Archivo**	 BCMS-2014-PP-08 Visita guiada a la en

Visita guiada a la organización

1. Objetivo:

Recopilar y analizar información general de las actividades y los procesos, con el propósito de adquirir conocimiento sobre las principales funciones que realiza la unidad a evaluar, específicamente en el Área de Teletrabajo.

2. Procedimiento:

Visitar los departamentos de la organización identificados como parte del sistema de continuidad del negocio e indagar los siguientes aspectos:

- Funciones que se realizan en las distintas oficinas o unidades visitadas;
- Conocer al personal que participa en los procesos del área.
- Consultar y determinar durante su visita la localización de las distintas áreas.
- Identifique claramente al personal clave en cada departamento.
- Determine en qué grado los sistemas de información se llevan manual o electrónicamente.
- Observe cualquier aspecto que no se encuentre dentro de los procesos normales y al que sea necesario referirse.

Documente en lo posible la información obtenida en etapas anteriores y la visita guiada.

3 Control de auditoría Asignado		Revisado	
Fecha		Fecha	

Anexo #	9	**Nombre**	BCMS-2014-P-PA-01 - Plan de Auditoría
Etapa	Planificación	**Archivo**	 BCMS-2014-P-PA-01 - Plan de Auditoria.c

Plan de Auditoría

BCMS-2014-P-PA-01

1 Propósito de la auditoría

El objetivo fundamental del presente plan de auditoría es validar el cumplimiento de la normativa ISO 22301:2012 en la organización A&J Consulting. El nivel estratégico de esta organización ha elaborado una serie de esfuerzos sistematizados con el fin de brindar la misma de las capacidades necesarias para sobrevivir a eventos disruptivos, por lo cual desea evaluar dicho mecanismo denominado Sistema para la Gestión de la Continuidad del Negocio.

2 Objetivo General

Analizar el sistema para la gestión de la continuidad del negocio a través de la validación y estudio del cumplimiento para los controles implementados en la organización en concordancia con la normativa ISO 22301:2012.

3 Objetivos Específicos

- Identificar el grado contextualización de la organización y las partes interesadas de la misma dentro del ciclo de vida de los procesos de continuidad del negocio.
- Analizar el cumplimiento de los controles de liderazgo y compromiso organizacional sobre las partes interesadas con respecto a la continuidad del negocio.

- Evaluar el proceso de planificación de la continuidad del negocio y sus actividades a través del análisis de los controles implementados por la organización.
- Validar los procesos de soporte de operación para la continuidad del negocio a través de la verificación del cumplimiento del mecanismo de asignación de recursos, concientización, capacitación, competencia y comunicación en la firma.
- Examinar el grado de acatamiento de la normativa ISO 22301:2012 en la operación de los sistemas de continuidad del negocio.
- Demostrar la existencia de un proceso de evaluación y mejora continua en las actividades relacionadas a la continuidad del negocio.
- Acatar las obligaciones contractuales con las cuentas de nivel empresarial

4 Alcance

El presente plan de auditoría tiene como alcance el cumplimiento para validar la eficiencia y eficacia de los controles implementados por la organización sobre el sistema de gestión para la continuidad del negocio durante el año financiero 2014, por lo tanto las evidencias, controles y cualquier documentación fuera del rango comprendido entre Enero 1, 2014 y Diciembre 31-2014 estarán fuera de la ejecución del mismo.

5 Procedimiento

N°	Procedimiento de Auditoría	Referencia (BCMS-2014)	Responsable	Fecha		Horas
				Inicio	Final	
1	Realizar una evaluación del contexto de la	P-PC-01	AGV			16

	organización, los marcos regulatorios, las partes interesadas, dimensionamiento del alcance del plan de continuidad, y la utilización de sistemas de continuidad del negocio como elemento habilitador de capacidades ante un incidente disruptivo.					
2	Analizar el compromiso del equipo estratégico de la organización como elemento responsable del liderazgo y patrocinio del sistema de continuidad del negocio. Además confirmar la existencia de un comité gerencial y del manejo de las políticas de compromiso en torno al tema de continuidad del negocio.	P-PC-02				6
3	Estudiar el proceso de planificación realizado para sustentar el proceso de continuidad	P-PC-03				8

	del negocio y sus actividades de soporte.					
4	Indagar los mecanismos de soporte al sistema de continuidad del negocio, así como los procesos de asignación de recursos al programa, el manejo del personal ante incidentes, capacidades y competencias del equipo responsable, los planes de capacitación y concientización y soporte.	P-PC-04				12
5	Verificar la correcta operación del sistema de gestión de la continuidad del negocio, así como la existencia de componentes claves tales como: • Planificación y Control • Análisis de Impacto en el negocio. • Evaluación del riesgo.	P-PC-05				32

	• Estrategia de continuidad, • Planes de continuidad. • Practica y prueba.					
6	Revisar los mecanismos de evaluación y desempeño, así como el proceso de establecimiento de métricas en concordancia a los requerimientos del negocio y los objetivos estratégicos a los que corresponde.	P-PC-06				3
7	Demostrar la existencia de procesos de mejora continua a través del tratamiento de planes de corrección, manejo de no conformidades y aseguramiento de calidad.	P-PC-07				2

6 Planificación de Recursos

TIEMPO ESTIMADO DEL ESTUDIO

Fecha de Asignación:	Tiempo Estimado: 80 horas por miembro.	Tiempo Real:	Diferencia:
Justificación de la diferencia en cumplimiento del tiempo:			
Observaciones:			
Fecha inicio:			
Fecha Finalización:			

Anexo #	10	**Nombre**	BCMS-2014-PC-01 - Sección 4
Etapa	Planificación	**Archivo**	BCMS-2014-PC-01 - Seccion 4.docx

Prueba de Cumplimiento: Sección 4

I PROPÓSITO

Realizar una evaluación del contexto de la organización, los marcos regulatorios, las partes interesadas, dimensionamiento del alcance del plan de continuidad, y la utilización de sistemas de continuidad del negocio como elemento habilitador de capacidades ante un incidente disruptivo.

II DESCRIPCIÓN DE LA PRUEBA

La prueba de cumplimiento para la sección 4; Contexto Organizacional, corresponde en la aplicación de un cuestionario digital por parte del auditor al auditado; este ofrecerá evidencia suficiente para argumentar y justificar sus respuestas. Una vez procesados los datos la herramienta brindará un grado de cumplimiento la cual deberá cumplir con los parámetros definidos por la auditoría.

III JUSTIFICACIÓN

El entendimiento de la organización y su contexto, permite determinar las actividades, funciones y responsables que permiten que la misma opere. A través de este ejercicio se puede identificar elementos críticos de la empresa y los posibles eventos que le pueden afectar.

El entendimiento de la organización ayuda a la identificación de las partes interesadas así como las expectativas de los mismos con respecto a la empresa. (Drewitt, 2013).

IV PROCEDIMIENTO

Para realizar esta prueba de cumplimiento se debe convocar a una reunión al auditado y él contestar las siguientes preguntas:

1. ¿La organización ha determinado los factores internos y externos que son relevantes para su propósito y que puedan afectar su capacidad para lograr los resultados esperados de su BCMS?
2. ¿La organización ha identificado y documentado sus actividades, funciones, servicios, productos, asociaciones, cadenas de suministro, las relaciones con las partes interesadas y el impacto potencial relacionado con un incidente perturbador?
3. ¿La organización ha identificado y documentado los vínculos entre su política de continuidad del negocio y los objetivos de la organización y otras políticas?
4. ¿La organización ha identificado y documentado los vínculos entre su política de continuidad del negocio y su estrategia general de gestión de riesgos?
5. ¿La organización ha establecido y documentado su apetito de riesgo?
6. ¿La organización ha definido el propósito de los BCMS?
7. ¿Tiene la organización una política documentada sobre la contratación, prestación y gestión de bienes y servicios tercerizados a través de su cadena de suministro?

8. ¿La organización reconoce plenamente que la externalización de una función de negocio no transfiere el riesgo del negocio asociado con el proveedor de proveedor y / o servicio?
9. ¿Tiene la organización un proceso documentado sobre la contratación de actividades priorizadas, externalizados sus recursos de apoyo y dependencias?
10. ¿Tiene la organización un proceso documentado en relación con la gestión de las actividades priorizadas, externalizados sus recursos de apoyo y dependencias?
11. ¿Realiza la organización evaluaciones periódicamente para auditar la capacidad de continuidad de negocio de sus proveedores?
12. ¿Son la continuidad del negocio, la evaluación del impacto del negocio, evaluación de riesgos operacionales y procesos de de diligencia integrados en proceso de adquisición de la organización?
13. ¿Tiene la organización una especificación de requisitos de la continuidad del negocio estandarizado para las licitaciones y contratos relativos a la cadena de suministro, especialmente sus actividades priorizadas, sus recursos de apoyo y sus dependencias?
14. ¿El BCMS de la organización mantiene documentado los proveedores internos y / o subcontratados y / o proveedores de servicios de actividades priorizadas y / o sus dependencias y los puntos únicos de fallo?
15. ¿Tiene la organización un conjunto estándar de los términos y condiciones del contrato con respecto a la continuidad del negocio que son un requisito obligatorio dentro de cada contrato de cadena de suministro o SLA de proveedores subcontratados y / o proveedores de servicios de actividades priorizadas y / o sus dependencias?
16. ¿El proceso de gestión y ejecución de los contratos de la organización cuenta con un requisito obligatorio para verificar y validar en periodos definidos las capacidades de continuidad del negocio en los proveedores de actividades críticas?

17. ¿La organización cuenta con una estrategia de traslado y abastecimiento en la cadena de suministro que le permita cambiar o trasladar sus actividades prioritarias y sus dependencias a otros proveedores?
18. ¿Tiene términos y condiciones de un contrato de outsourcing o estándares de la organización SLA para el suministro y prestación de las actividades priorizadas o sus dependencias requieren del proveedor / prestador para informar de inmediato a la organización cualquier incidente interno o externo que incide en ellos y su capacidad potencial o real para prestar el servicio o suministro contratado?
19. ¿Es la continuidad del negocio un tema permanente en las revisiones de contrato y evaluación de la gestión del rendimiento con proveedores tercerizados que brindan soporte en las actividades priorizadas y sus dependencias?
20. ¿La organización tiende a retener información documentada como la evidencia de su adquisición, cadena de suministro y gestión de contratos?
21. ¿La organización ha identificado sus grupos de interés y las partes interesadas que son relevantes para los BCMS?
22. ¿La organización ha establecido e incorporado las necesidades, requerimientos y expectativas de las organizaciones y partes interesadas en su BCMS?
23. ¿Tiene la organización un proceso que identifica y aplica sus legales, condiciones de las licencias contractuales y operativas reglamentario que se refieren a la continuidad de las operaciones, los productos, los servicios e intereses de las partes interesadas pertinentes?
24. ¿La organización ha tenido en cuenta los requisitos aplicables, legales, reglamentarios y de cualquier otro tipo en el establecimiento, implementación y mantenimiento de la BCMS?
25. ¿Son los requisitos legales, nuevos o actualizaciones, reglamentarios y otros comunicados a los empleados afectados, administradores y otras partes interesadas en el momento oportuno?

26. ¿Es el BCMS consistente con la regulación industrial reconocida o legislación?
27. ¿Ha determinado la organización y documentado el alcance de su BCMS?
28. ¿La organización ha determinado los límites y aplicabilidad del BCMS en el establecimiento de su alcance?
29. ¿La organización ha establecido las partes de la organización que se incluirán en el BCMS?
30. ¿La organización ha identificado los productos y servicios, y todas las actividades relacionadas en el ámbito de BCMS?
31. ¿Tiene el alcance de la BCMS relación con el propósito de los BCMS?
32. ¿El alcance de las BCMS refleja los problemas internos y externos que son relevantes para su propósito?
33. ¿El alcance del BCMS refleja el tamaño, la naturaleza, el alcance y la complejidad de la organización?
34. ¿El alcance del BCMS refleja la concordancia con las legislaciones y regulaciones de industria, país u otras de la empresa y el entorno donde se ejecuta?
35. ¿El alcance del BCMS refleja e incorpora las necesidades, requerimientos y expectativas de los grupos de interés de la organización y de las partes interesadas?
36. ¿El alcance del BCMS refleja el apetito de riesgo de la organización?
37. ¿El alcance del BCMS está documentado y explica las excepciones pertinentes al mismo?
38. ¿El alcance del BCMS incluye la cadena de suministro de la organización?
39. ¿Es el ámbito de BCMS de la organización proporcional al riesgo de la organización y consistente con su apetito de riesgo?
40. ¿La organización ha establecido e implementado un sistema de gestión de continuidad de negocio ?
41. ¿La organización posee un proceso para mantener y mejorar su sistema de gestión de continuidad de negocio ?

42. ¿La organización ha determinado y proporcionado los recursos necesarios para establecer, implementar, operar, mantener y mejorar los BCMS?
43. ¿Está el BCMS alineado con la norma ISO 22301, o ISO 22313 o cualquier ley u otros estándares, directrices, normativas u otros ?
44. ¿Están las funciones, responsabilidades y autoridad de los empleados dentro de la BCMS claramente definidas, documentadas y asignadas?
45. ¿La organización ha determinado los problemas externos e internos que son relevantes para su propósito y que afectan su capacidad para lograr los resultados esperados de su BCMS?
46. ¿El enfoque del BCMS está alineado a las actividades prioritarias de la organización y sus dependencias a nivel de productos y servicios?
47. ¿El programa BCMS se ha definido y diseñado dentro de un sistema BCM?
48. ¿Los objetivos y resultados de la continuidad se establecen y definen en el BCMS?
49. ¿Se aplica el ciclo PDCA (Planear-Hacer-Verificar-Actuar) como modelo para implementar y mantener el BCMS?
50. ¿Los objetivos del BCMS y los resultados alineados están establecidos acorde a las estrategias y planes de negocio de las empresas?
51. ¿El BCMS establece y define mecanismos para la ejecución y la evaluación con evidencia suficiente, concreta y veraz del mismo.
52. ¿Existe un presupuesto anual dedicado y recursos asignados a BCMS para su implementación, mantenimiento y mejora?
53. ¿Tiene la organización a retener información documentada como la evidencia de su BCMS?
54. ¿El BCMS ha documentado el proceso de control de cambio / procedimiento para garantizar que siga siendo actual, apropiado (adecuados a los objetivos) y plausible?
55. ¿Es el BCMS revisado por lo menos una vez cada 12 meses o en intervalos planificados, cuando ocurren cambios significativos o que repercuten en la organización?
56. ¿El BCMS proporciona un informe anual de evaluación opinión?

57. ¿La organización asegura que todo el personal al que se asigna funciones y responsabilidades dentro de los BCMS son competentes y capaces de realizar sus tareas?
58. ¿Son profesionales de continuidad de negocio profesionalmente cualificados y experimentados empleados en la ejecución, el ejercicio y el mantenimiento del BCMS y sus procedimientos de continuidad de negocio y arreglos en particular?
59. ¿Mantiene el BCMS un cronograma de actividades prioritarias de la organización o sus dependencias y puntos únicos de fallo?
60. ¿Ha designado la organización para la gestión a una o varias personas que sean las responsables de implementar y mantener el BCMS independientemente de otras responsabilidades?
61. ¿Tiene la organización un proceso de garantía documentada y programa para el BCMS y sus componentes?
62. ¿Tiene la organización un conjunto de indicadores clave de rendimiento (KPI objetivos, metas y estándares) para el BCMS?
63. ¿Son los indicadores clave de rendimiento de una parte del sistema de información de gestión BCMS (MIS)?
64. ¿Son los indicadores clave de rendimiento tanto cuantitativa (objetivo) y cualitativa (subjetiva)?
65. ¿Son los indicadores clave de rendimiento comunicados a todo el personal?
66. ¿Hay un proceso documentado para supervisar y revisar los indicadores clave de rendimiento?
67. ¿Están los indicadores clave de desempeño monitoreados y revisados por un comité de riesgos y de gestión ejecutiva nivel?
68. ¿Están los indicadores clave de rendimiento asignados a funciones dentro de la organización?
69. ¿Están los planes de acción correctores desarrollados para abordar las brechas de desempeño programa de garantía dentro de un plazo de tiempo acordado?

70. ¿Tiende la organización a retener información documentada como la evidencia de sus actividades de aseguramiento y los resultados?
71. ¿Tiene la organización un sistema de información gerencial BCMS (MIS) como parte de su gestión general, la supervisión y el programa de evaluación del desempeño del BCMS?
72. ¿El sistema de información de gestión BCMS (MIS) supervisa y proporciona información periódica sobre la situación de los BCMS?
73. ¿Hay un programa previsto para monitorear y evaluar el estado del BCMS?
74. ¿El informe de estado del BCMS es comunicada a las partes internas y externas claves y relevantes?
75. ¿Tiende la organización a retener información documentada como la evidencia de sus actividades de MIS y los resultados?

VI CRITERIO DE HALLAZGO

Las empresas certificadas o en proceso de certificación deberán contar con un grado de cumplimiento superior al 85%, una nota inferior representará un hallazgo de auditoría.

Para las empresas en proceso de autoevaluación no certificadas, el cumplimiento debe ser superior a 75%.

.

Anexo #	11	**Nombre**	BCMS-2014-PC-02 - Sección 5
Etapa	Planificación	**Archivo**	BCMS-2014-PC-02 - Seccion 5.docx

Prueba de Cumplimiento: Sección 5

I PROPÓSITO

Realizar una evaluación del contexto de la organización, los marcos regulatorios y las partes interesadas, dimensionamiento del alcance del plan de continuidad y la utilización de sistemas de continuidad del negocio como elemento habilitador de capacidades ante un incidente disruptivo.

II DESCRIPCIÓN DE LA PRUEBA

La prueba de cumplimiento para la sección 5; Liderazgo, corresponde a la aplicación de un cuestionario digital por parte del auditor al auditado; este ofrecerá evidencia suficiente para argumentar y justificar sus respuestas. Una vez procesados los datos, la herramienta brindará un grado de cumplimiento, de modo que se cumplan los parámetros definidos por la auditoría.

III JUSTIFICACIÓN

El entendimiento de la organización y su contexto permite determinar las actividades, las funciones y los responsables que permiten que la misma opere. A

través de este ejercicio se puede identificar elementos críticos de la empresa y los posibles eventos que la pueden afectar.

El entendimiento de la organización ayuda a la identificación de las partes interesadas, así como las expectativas de los mismos con respecto a la empresa. (Drewitt, 2013).

IV PROCEDIMIENTO

Para realizar esta prueba de cumplimiento, se debe convocar al auditado y contestar las siguientes preguntas, quien, por su parte, debe aportar la evidencia suficiente para defender el proceso asociado:

1. ¿La alta dirección de la organización y otras funciones de gestión pertinentes en toda la organización demuestran liderazgo, apoyo y un fuerte compromiso con respecto a la BCMS?
2. ¿El programa del BCMS fue respaldado abiertamente y activamente por la alta dirección?
3. ¿Está la alta dirección de la organización de manera proactiva y visiblemente involucrada en el programa del BCMS?
4. ¿La alta dirección controla el programa BCMS y lo evalúa periódicamente?
5. ¿Es el BCMS un tema permanente en las reuniones del Comité de Gestión de Riesgos de la organización?
6. ¿Es la continuidad del negocio un tema permanente en las reuniones operativas y de gestión empresarial en toda la organización?
7. ¿La alta dirección de la organización y otras funciones de gestión pertinentes promueven fuertemente y garantizan la integración de los requisitos BCMS en los procesos empresariales de la empresa?

8. ¿La alta dirección de la organización y otras funciones de gestión pertinentes garantizan los recursos necesarios para el BCMS?
9. ¿La alta dirección de la organización y otras funciones de gestión pertinentes apoyan otras funciones de gestión pertinentes para demostrar el liderazgo y compromiso que se aplica a sus áreas de responsabilidad?
10. ¿Se ha asegurado la alta dirección la existencia de una estrategia para el BCM organizacional?
11. ¿Los funcionarios de nivel ejecutivo se involucran y participan en las actividades de continuidad?
12. ¿Se asegura la alta dirección de la organización que las políticas y los objetivos de BCMS responden a las necesidades de la empresa?
13. ¿Se asegura la alta dirección de la organización que las políticas y objetivos para el BCMS son compatibles con la dirección estratégica de la organización?
14. ¿Ha establecido y publicado la alta gerencia una política organizacional de la continuidad del negocio?
15. ¿Ha nominado a la alta dirección (o nombrado) a una persona con la antigüedad y la autoridad apropiada para ser responsable de la política BCM y su ejecución, supervisión y la presentación de informes?
16. ¿La política de BC incluye y hace referencia al ámbito de la continuidad del negocio, así como las limitaciones y excepciones de la misma?
17. ¿La alta dirección ha demostrado su expresa voluntad de brindar soporte para los planes de contenía tener voz?
18. ¿La política de continuidad de negocio es comunicada a todo el personal de la organización?
19. ¿La política de continuidad del negocio se encuentra disponible para todas las partes interesadas en la misma?
20. ¿La política de continuidad del negocio se verifica periódicamente o cuando hay un cambio significativo dentro una organización?

21. ¿La organización tiene procesos para garantizar y asegurar que todas las partes interesadas han sido informadas de la política de continuidad del negocio?
22. ¿La alta dirección de la organización ha designado a uno o más representantes de la dirección con la autoridad competente, las competencias y la capacidad de ser responsable de la BCMS, para ser responsable de su creación, implementación, mantenimiento y efectivo funcionamiento?
23. ¿Existe un rol definido para un responsable de la alta gerencia que vele por el correcto funcionamiento, mantenimiento y actualización de los planes de continuidad del negocio?
24. ¿Se seleccionan los empleados clave para apoyar e implementar el programa del BCMS?
25. ¿Los empleados asignados al sistema de continuidad del negocio reciben documentos apropiados?
26. ¿Están las funciones de continuidad de negocio, las responsabilidades, las obligaciones y las autoridades integradas en las descripciones de puestos que pueden ser reforzados mediante su inclusión en la organización de evaluación, la recompensa y la política de reconocimiento?
27. ¿La alta dirección de la organización ha asignado la autoridad y la responsabilidad de informar sobre el desempeño de la BCMS a la alta dirección?

¿La alta dirección ha asignado la autoridad y la responsabilidad de asegurar que el BCMS se ajuste a los requisitos de la norma ISO, regulatorios y legales

VI CRITERIO DE HALLAZGO

Las empresas certificadas o en proceso de certificación deberán contar con un grado de cumplimiento superior al 85%, una nota inferior representará un hallazgo de auditoría.

Para las empresas en proceso de autoevaluación no certificadas, el cumplimiento debe ser superior a 75%.

Anexo #	12	**Nombre**	Prueba de Cumplimiento: Sección 6
Etapa	Planificación	**Archivo**	BCMS-2014-PC-03 - Seccion 6.docx

Prueba de Cumplimiento: Sección 6

I PROPÓSITO

Realizar una evaluación del contexto de la organización, los marcos regulatorios, las partes interesadas, el dimensionamiento del alcance del plan de continuidad, y la utilización de sistemas de continuidad del negocio como elemento habilitador de capacidades ante un incidente disruptivo.

II DESCRIPCIÓN DE LA PRUEBA

La prueba de cumplimiento para la sección 6; Planificación, corresponde a la aplicación de un cuestionario digital por parte del auditor al auditado; este ofrecerá evidencia suficiente para argumentar y justificar sus respuestas. Una vez procesados los datos, la herramienta brindará un grado de cumplimiento, el cual deberá cumplir con los parámetros definidos por la auditoría.

III JUSTIFICACIÓN

El entendimiento de la organización y su contexto permite determinar las actividades, funciones y responsables que permiten que la misma opere. A través de este ejercicio se puede identificar elementos críticos de la empresa y los posibles eventos que la pueden afectar.

El entendimiento de la organización ayuda a la identificación de las partes interesadas así como las expectativas de los mismos con respecto a la empresa. (Drewitt, 2013).

IV PROCEDIMIENTO

Para realizar esta prueba de cumplimiento, se debe convocar al auditado y contestar las siguientes preguntas, este por su parte debe aportar la evidencia suficiente para defender el proceso asociado:

1. ¿La alta dirección de la organización ha establecido sus objetivos de continuidad del negocio?
2. ¿Los objetivos de continuidad del negocio protegen las actividades críticas de la organización, así como el abastecimiento de recursos a las mismas?
3. ¿El plan de continuidad del negocio es verificado periódicamente y revisado acorde a la planificación anual de auditoría?
4. ¿La alta dirección de la organización ha comunicado los objetivos de continuidad del negocio en concordancia a lo planeado?
5. ¿Los objetivos de continuidad del negocio son coherentes con la política de BCMS?
6. ¿Los objetivos de continuidad del negocio de la organización tienen en cuenta el nivel mínimo de los productos y servicios que sea aceptable para lograr los objetivos de la organización?
7. ¿Los objetivos de continuidad de negocio de la organización tienen en cuenta las necesidades y expectativas de las partes interesadas?
8. ¿Los objetivos de continuidad de negocio de la organización son coherentes y están acorde con las regulaciones legales, la gobernanza corporativa, las obligaciones contractuales y las condiciones de operación de licencia?
9. ¿Los objetivos de continuidad de negocio de la organización tienen en cuenta la cadena de suministro de la organización?

10. ¿Son los objetivos de continuidad de negocio de la organización subjetiva u objetivamente medibles?
11. ¿Los objetivos de continuidad de negocio de la organización incluyen los servicios o productos subcontratados y la gestión de contratos?
12. ¿Son los objetivos de continuidad de negocio de la organización supervisados, evaluados y actualizados en su caso?
13. ¿Tiene la organización la capacidad de determinar lo que hay que hacer para lograr sus objetivos de continuidad de negocio?
14. ¿La organización puede determinar qué recursos se necesitan para lograr sus objetivos de continuidad de negocio?
15. ¿Tiene la organización una escala de tiempo para alcanzar sus objetivos de continuidad de negocio?
16. ¿Tiende la organización a definir cómo se evaluarán los resultados de sus objetivos de continuidad de negocio?
17. ¿La organización retiene registros de información documentada sobre sus objetivos de continuidad de negocio?

VI CRITERIO DE HALLAZGO

Las empresas certificadas o en proceso de certificación deberán contar con un grado de cumplimiento superior al 85%, una nota inferior representará un hallazgo de auditoría.

Para las empresas en proceso de autoevaluación no certificadas, el cumplimiento debe ser superior a 75%.

.

Anexo #	13	**Nombre**	Prueba de Cumplimiento: Sección 7
Etapa	Planificación	**Archivo**	BCMS-2014-PC-04 - Seccion 7.docx

Prueba de Cumplimiento: Sección 7

I PROPÓSITO

Realizar una evaluación del contexto de la organización, los marcos regulatorios, las partes interesadas, dimensionamiento del alcance del plan de continuidad, y la utilización de sistemas de continuidad del negocio como elemento habilitador de capacidades ante un incidente disruptivo.

II DESCRIPCIÓN DE LA PRUEBA

La prueba de cumplimiento para la sección 7; Soporte, corresponde a la aplicación de un cuestionario digital por parte del auditor al auditado; quien ofrecerá evidencia suficiente para argumentar y justificar sus respuestas. Una vez procesados los datos la herramienta brindará un grado de cumplimiento, la cual deberá cumplir con los parámetros definidos por la auditoría.

III JUSTIFICACIÓN

El entendimiento de la organización y su contexto permite determinar las actividades, funciones y responsables que permiten que la misma opere. A través de este ejercicio se puede identificar elementos críticos de la empresa y los posibles eventos que le pueden afectar.

El entendimiento de la organización ayuda a la identificación de las partes interesadas así como las expectativas de los mismos con respecto a la empresa. (Drewitt, 2013).

IV PROCEDIMIENTO

Para realizar esta prueba de cumplimiento, se debe convocar al auditado y contestar las siguientes preguntas, este por su parte debe aportar la evidencia suficiente para defender el proceso asociado:

1. ¿La organización ha determinado y proporcionado los recursos necesarios para el establecimiento, la implementación, el mantenimiento y la mejora continua del BCMS?
2. ¿Existe un presupuesto anual dedicado y asignado a los recursos BCMS?
3. ¿Se han asignado los recursos al BCMS?
4. ¿Los recursos incluyen a las personas y a las partes relacionadas con los recursos?
5. ¿Los recursos incluyen la provisión de capacitación, la educación, la sensibilización y el ejercicio?
6. ¿Los recursos incluyen instalaciones que contemplan lugares de trabajo e infraestructura?
7. ¿Los recursos incluyen tecnologías de información y las comunicaciones (TIC), incluyendo aplicaciones que soportan la gestión eficaz y eficiente BCMS?
8. ¿Los recursos y su asignación son revisados periódicamente para asegurar su adecuación y suficiencia?
9. ¿Cuenta la organización con personal encargado de la respuesta de incidentes que tengan la responsabilidad necesaria, la autoridad y competencia para manejar un incidente?

10. ¿La organización ha asignado personal a los equipos de acuerdo a sus competencias y sus capacidades de enfrentar los diferentes aspectos de la respuesta a incidentes?
11. ¿La organización ha nombrado a un equipo de gestión de incidentes y gestión estratégica?
12. ¿La organización ha nombrado a un equipo de comunicaciones y gestión de medios en materia de respuesta a incidentes?
13. ¿La organización ha nombrado a un equipo de gestión de la seguridad y el bienestar en materia de respuesta ante incidentes?
14. ¿La organización ha nombrado a un equipo de gestión de clientes o partes interesadas en relación con la respuesta ante incidentes?
15. ¿La organización ha nombrado a un equipo de rescate y gestión de la seguridad en materia de respuesta en caso de incidentes?
16. ¿La organización ha designado un plan de reanudación de las actividades críticas y los recursos de ayuda al equipo de gestión en materia de respuesta a incidentes?
17. ¿La organización ha nombrado a un equipo de gestión de la reanudación de las TIC para la recuperación en materia de respuesta ante incidentes?
18. ¿La organización ha nombrado a un equipo de gestión de personal en materia de respuesta a incidentes?
19. ¿La organización ha nombrado a un equipo para la seguridad y el bienestar en materia de respuesta en caso de incidentes?
20. ¿La organización asegura que todo el personal o los equipos a los que se les han asignado roles y responsabilidades en los procedimientos, y en especial los acuerdos de continuidad de negocio BCMS, son competentes y capaces de realizar sus funciones?
21. ¿La organización ha determinado la sensibilización, el conocimiento, la comprensión, las habilidades y la experiencia necesaria para cumplir con las funciones y responsabilidades dentro de su BCMS?

22. ¿La organización se ha asegurado de que los individuos y equipos miembros del BCMS son competentes y capaces en cuanto a educación, formación y experiencia?
23. ¿La organización retiene información que evidencie las competencias, formaciones y mejoras de los miembros que participan del BCMS
24. ¿La organización ha establecido un programa de formación para todos los empleados actuales que puedan afectarse o que tienen que lidiar con un incidente perturbador?
25. ¿La organización cuenta con mecanismos para identificar capacidades y requisitos propios del personal que participa con eventos perturbadores?
26. ¿La organización proporciona un programa de desarrollo personal para las personas o los equipos con roles asignados dentro del BCMS que identifica a la formación, la educación, el desarrollo y otro tipo de apoyo necesario para alcanzar las competencias requeridas?
27. ¿Es la formación de continuidad de negocio previsto para los empleados clave directamente involucrada en la planificación, ejecución y gestión de los BCMS y los procedimientos de continuidad de negocio y de acuerdos?
28. ¿El programa de formación de continuidad del negocio es evaluado regularmente para reflejar los cambios y las necesidades dentro de la organización?
29. ¿Son los nuevos desarrollos en la continuidad del negocio y las BCMS incorporados en el programa de formación?
30. ¿Tiende la organización a evaluar la eficacia de la formación recibida en contra de las necesidades y requisitos de formación definidos, con el fin de verificar la conformidad con los requisitos de formación BCMS?
31. ¿La organización ha evaluado la eficacia de las medidas adoptadas para asegurar que las personas y los equipos que participan en la entrega de su BCMS y continuidad del negocio tengan la educación, formación y experiencia apropiadas?

32. ¿Tiene la organización mecanismos de retención de información documental como evidencia de la formación de los individuos y los equipos?
33. ¿La organización ha establecido un programa de concienciación de continuidad de negocio para todos los empleados actuales para promover y crear conciencia del BCMS de la organización?
34. ¿Es la conciencia de continuidad del negocio una parte integral del programa de inducción para todos los nuevos empleados, gerentes y ejecutivos de la organización?
35. ¿Los empleados de la organización son informados de su contribución a la eficacia del BCMS incluyendo los beneficios de un mejor desempeño de continuidad del negocio?
36. ¿Los empleados de la organización son informados de las consecuencias que no se ajustan a los requisitos BCMS de la organización?
37. ¿Son los empleados de la organización conscientes de su propio papel durante un incidente perturbador?
38. ¿El programa de sensibilización de la organización incluye los principales proveedores de información y los distribuidores sobre los procedimientos y mecanismos de continuidad del negocio?
39. ¿Son los empleados de la organización conscientes de su papel y responsabilidad en materia de prevención de incidentes, detección, mitigación, auto-protección, evacuación, respuesta, continuidad y recuperación?
40. ¿La organización ha establecido un proceso para construir, promover, integrar e incorporar una cultura de continuidad del negocio dentro de la organización?
41. ¿Existe un sistema de reconocimiento o recompensas que refuerza los empleados implicados en los BCMS?
42. ¿Son los indicadores de desempeño de la continuidad del negocio comunicados a los empleados.

43. ¿Los empleados de la organización entienden plenamente sus funciones, las responsabilidades y autoridades dentro del BCMS?
44. ¿Están las funciones, las responsabilidades de los empleados dentro de la BCMS incluidas dentro de la descripción del trabajo?
45. ¿Están las contribuciones de los empleados a la BCMS reflejadas en sus evaluaciones anuales de desempeño?
46. ¿Están las contribuciones de los empleados a la BCMS reflejados en el sistema de remuneración de rendimiento anual de la organización?
47. ¿Tiende la organización a evaluar regularmente y actualizar su programa de sensibilización de continuidad del negocio?
48. ¿La organización tiende a evaluar regularmente la eficacia del programa de sensibilización de continuidad del negocio?
49. ¿La organización ha establecido e implementado procedimientos para la comunicación interna entre las partes y los empleados involucrados dentro de la organización?
50. ¿La organización ha establecido e implementado procedimientos para la comunicación externa con los clientes, socios, comunidad local y otras partes interesadas, incluidos los medios de comunicación?
51. ¿Ha establecido la organización los procedimientos para recibir, documentar y responder a las comunicaciones de las partes interesadas en la práctica?
52. ¿La organización ha establecido e implementado procedimientos para asegurar la disponibilidad de los medios de comunicación durante un incidente perturbador?
53. ¿La organización ha establecido e implementado procedimientos para las capacidades de comunicación de operación y las pruebas destinadas a ser utilizadas durante la interrupción o comunicaciones normales?
54. ¿La organización mantiene el control sobre la documentación pertinente a los planes de continuidad del negocio, así como la información pertinente de la operación del mismo?

55. ¿El BCMS de la organización incluye la información requerida por la norma ISO 22301 e ISO 22313 documentada?
56. ¿Tiene información documentada de la organización que brinde evidencia sobre la conformidad de los requisitos y el funcionamiento eficaz del BCMS de la organización?
57. ¿Al crear y actualizar la información se asegura la organización la adecuada identificación y descripción, por ejemplo, hora, fecha, autor o número de referencia, único documentado?
58. ¿Al crear y actualizar la información se asegura la organización el formato adecuado (por ejemplo, del idioma, la versión del software, gráficos) y los medios de comunicación (por ejemplo, papel o electrónico) documentados?
59. ¿La organización se asegura de que al crear y actualizar la información del BCMS esta es revisada, aprobada y comunicada a la población interesada?
60. ¿Puede el control del proceso de la información documentada describirse como un sistema de control de documentos complejos en lugar de su enfoque principal y con propósito como se describe en la cláusula 7.5.3 de la norma ISO 22313?
61. ¿La información documentada requerida por el BCMS de la organización es controlada para asegurarse que está disponible y adecuada para su uso, cuando se necesite?
62. ¿La información documentada, que brinda soporte al BCMS, se encuentra correctamente custodiada, con controles suficientes para garantizar su visibilidad, integridad y seguridad?
63. ¿El control de la información documentada por la organización aborda su distribución, acceso, retiro y uso?
64. ¿El control de la información documentada por la organización aborda su almacenamiento y su conservación?
65. ¿La gestión documental integra controles de cambio, manejo de versiones y actualizaciones?
66. ¿El control de la información documentada por la organización garantiza su preservación y su legibilidad?

67. ¿El control de la información documentada de la organización controla la prevención del uso adecuado de la información obsoleta?

VI CRITERIO DE HALLAZGO

Las empresas certificadas o en proceso de certificación deberán contar con un grado de cumplimiento superior al 85%, una nota inferior representará un hallazgo de auditoría.

Para las empresas en proceso de autoevaluación no certificadas, el cumplimiento debe ser superior a 75%.

Anexo #	14	**Nombre**	Prueba de Cumplimiento: Sección 8
Etapa	Planificación	**Archivo**	BCMS-2014-PC-05 - Seccion 8.docx

Prueba de Cumplimiento: Sección 8

I PROPÓSITO

Realizar una evaluación del contexto de la organización, los marcos regulatorios, las partes interesadas, dimensionamiento del alcance del plan de continuidad y la utilización de sistemas de continuidad del negocio como elemento habilitador de capacidades ante un incidente disruptivo.

II DESCRIPCIÓN DE LA PRUEBA

La prueba de cumplimiento para la sección 8; Operación, corresponde a la aplicación de un cuestionario digital por parte del auditor al auditado; este ofrecerá evidencia suficiente para argumentar y justificar sus respuestas. Una vez procesados los datos, la herramienta brindará un grado de cumplimiento la cual deberá cumplir con los parámetros definidos por la auditoría.

III JUSTIFICACIÓN

El entendimiento de la organización y su contexto, permite determinar las actividades, funciones y responsables que permiten que la misma opere. A través

de este ejercicio se puede identificar elementos críticos de la empresa y los posibles eventos que le pueden afectar.

El entendimiento de la organización ayuda a la identificación de las partes interesadas así como las expectativas de los mismos con respecto a la empresa. (Drewitt, 2013).

IV PROCEDIMIENTO

Para realizar esta prueba de cumplimiento, se debe convocar al auditado y contestar las siguientes preguntas, este, por su parte, debe aportar la evidencia suficiente para defender el proceso asociado:

Pregunta

1. ¿La organización cuenta con un proceso de planificación y control documentado de BCMS a nivel operativo, que permite planificar, aplicar, controlar y determinar las acciones necesarias para cumplir con su política de continuidad del negocio?
2. ¿El proceso de planificación contempla el control operativo del mismo, así como la definición de un programa que asegure la continuidad de la organización acorde a los niveles de operación mínimos?
3. ¿La planificación operativa de la organización abarca todos los procesos críticos de la misma y su interrelación?
4. ¿El proceso de planificación operativa de la continuidad del negocio toma en cuenta todos los elementos de la cadena de suministro?
5. ¿Es el proceso de planificación operativa principalmente con actividades priorizadas de la organización y sus dependencias?
6. ¿La planificación operativa cubre completamente el proceso de gestión, desde la respuesta inicial hasta alcanzar un nivel de rendimiento y funcionalidad aceptable para la operación de las funciones críticas?

7. ¿Se integra el proceso de planificación operativa y coordinado con otras partes de la organización, por ejemplo, geográficamente, divisiones, departamentos, funciones de apoyo que pueden ser afectados o involucrados en el proceso de gestión de incidentes, la reanudación del negocio y la recuperación?

8. ¿Se integra el proceso de planificación operativa y coordinada con las autoridades y los servicios pertinentes? Por ejemplo: los reguladores de la industria, los servicios de emergencia y las autoridades locales que pueden estar implicados en la gestión del impacto o en el proceso de reanudación del negocio y recuperación

9. ¿El actual proceso de planificación operativa incluye eventos biológicos de factor humano como las pandemias y otros tipos de eventos relacionados a la industria?

10. ¿El proceso de planificación operativa se vincula con otras áreas del negocio?

11. ¿Es coordinado el proceso de planificación operativa, se integrada con la gestión y la comunicación de crisis corporativa y el proceso de gestión de incidentes de relaciones públicas?

12. ¿Tiene la organización un proceso de procedimiento y evaluación estándar para la realización de un BIA?

13. ¿Es la metodología, proceso, procedimiento y resultados y productos compatibles con la norma ISO 22301 o ISO 22313?

14. ¿El proceso y el procedimiento definen los resultados requeridos de un BIA?

15. ¿Está documentado el proceso del BIA, la metodología y los resultados?

16. ¿Existen directrices y criterios para ayudar a establecer las actividades prioritarias de la organización?

17. ¿La organización utiliza una herramienta de software para llevar a cabo un BIA? Explique la metodología.

18. ¿Determina el BIA la continuidad del negocio y las metas de recuperación?

19. ¿Tiene la organización un proceso estándar y un formato de la plantilla para exponer un informe BIA?
20. ¿Revisa la organización la adecuación del BIA en intervalos planificados o cuando se produzcan cambios fundamentales que afectan a la organización o sus actividades priorizadas y sus dependencias?
21. ¿Existe un proceso para asegurar que el BIA se lleva a cabo como parte de los nuevos acontecimientos y cambios importantes en los sistemas, productos, servicios y abastecimiento?
22. ¿Tiende la organización a retener información documentada como evidencia de sus actividades BIA?
23. ¿La organización ha llevado a cabo un BIA para identificar sus actividades prioritarias?
24. ¿Las actividades prioritarias de la organización para proporcionar productos y servicios han sido identificadas y documentadas?
25. ¿El BIA incluye la cadena de suministro de la organización?
26. ¿El BIA toma en cuenta los procesos críticos que se encuentran tercerizados y su impacto en la organización?
27. ¿El proceso de BIA incluye fechas clave, estaciones, época del año y otros ciclos económicos?
28. ¿Se ha completado un BIA estandarizado por cada unidad de negocio dentro de la organización, al menos una vez en los últimos 12 meses, y ha sido firmados por el gerente de dicha área?
29. ¿La organización tiene conciencia del impacto (financiero y no financiero) de la interrupción de las actividades críticas de la organización?
30. ¿El proceso BIA define los criterios de impacto y evaluación de incidentes de interrupción?
31. ¿Son los impactos y consecuencias resultantes documentados de alguna manera?
32. ¿Son los impactos y consecuencias regularmente revisados y evaluados?
33. ¿Son los impactos y consecuencias utilizados en el proceso de gestión del riesgo operacional ?

34. ¿Se ha analizado y documentado la pérdida e impacto de las TIC, en cuanto a datos y sistemas?

35. ¿Se ha analizado y documentado la pérdida de impacto de los sistemas de telecomunicaciones?

36. ¿La evaluación abarca el impacto legal, contractual, reglamentario y autorización de funcionamiento así como de otros requisitos de operación?

37. ¿El BIA estableció el período máximo tolerable de interrupción para cada actividad crítica del negocio mediante la identificación de la cantidad de tiempo en el que los niveles normales de operación necesitan ser reanudados para cada actividad crítica del negocio?

38. ¿Se ha analizado y documentado el impacto de la pérdida de la cadena de suministros organizacionales?

39. ¿Hay determinación de un Objetivo de Tiempo de Recuperación (RTO) para cada actividad prioritaria?

40. ¿La organización ha establecido el nivel mínimo aceptable de reanudación del negocio o recuperación en términos de funcionalidad y rendimiento para cada actividad priorizada como el de negocios mínimo de continuidad objetivo (MBCO)?

41. ¿La organización ha identificado el plazo máximo de interrupción para cada actividad prioritaria antes de que se convierta en un grave riesgo?

42. ¿Cada objetivo de tiempo de recuperación (RTO) establece el plazo máximo tolerable de interrupción después de lo cual el impacto sería inaceptable?

43. ¿Se han elaborado perfiles de reanudación del negocio para las unidades de producción con tiempos y características semejantes?

44. ¿Ha identificado la organización las dependencias y los recursos necesarios para mantener, restaurar o recuperar cada una de sus actividades prioritarias a un nivel aceptable de funcionalidad y rendimiento (MBCO)?

45. ¿El personal clave que está vinculado a estas actividades se ha identificado y documentado?

46. ¿Identifica el BIA plazos de sustitución y traslado? Por ejemplo; equipo o cargas de trabajo.

47. ¿Hay un tiempo que requieren la sustitución de equipos para actividad la crítica de la planta?

48. ¿Se ha identificado y documentado maquinaria y equipo en estas actividades?

49. ¿Haga que los documentos clave, registros o datos que son críticos para cada actividad prioritaria han identificado y documentado?

50. ¿Hay una lista completa y total de los servicios prioritarios de actividad de telecomunicaciones y los sistemas críticos que los apoyan?

51. ¿Hay una lista completa y completa de TI, las aplicaciones, los datos y los sistemas críticos que los apoyan?

52. ¿Los sistemas de TI, aplicaciones y recuperación de datos se alinean con los requisitos de las actividades prioritarias?

53. ¿Los tiempos de recuperación del sistema de comunicación son alineados con los requisitos de las actividades prioritarias?

54. ¿Hay acuerdos establecidos para reubicar a los locales alternativos o sitio de producción?

55. ¿La organización puede trasladar sus operaciones a otros locales físicos o virtuales sin requerir de un proveedor externo?

56. ¿La organización tiene un procedimiento estandarizado y documentado formalmente así como procedimiento para llevar a cabo la evaluación de riesgos?

57. ¿Tiende la organización a retener información documentada como prueba de su programa y las actividades de evaluación de riesgos?

58. ¿Se cuenta dentro de la organización con documentación suficiente para asignar a un responsable de la gestión del riesgo?

59. ¿Es la metodología, proceso, procedimiento, resultados y productos compatibles con la norma ISO 22301 o ISO 22313?

60. ¿La organización tiene una Política de Gestión del Riesgo Operacional documentada?

61. ¿La organización tiene una estrategia de gestión de riesgos documentada y programada?

62. ¿La alta dirección de la organización ha definido el apetito de riesgo de la organización, es decir, los niveles aceptables de riesgo?

63. ¿La organización tiene un apetito por el riesgo formalmente documentado?

64. ¿La organización utiliza una herramienta de software para llevar a cabo la evaluación de riesgos? (Si es 'sí', facilite detalles)

65. ¿Identifica la evaluación de riesgos de manera sistemática los incidentes de interrupción dentro del contexto organizacional?

66. ¿El proceso de evaluación de riesgos define los tipos de riesgo, su impacto y criterios de evaluación?

67. ¿La organización ha identificado riesgos de interrupción de sus actividades prioritarias y los recursos que apoyan a las mismas?

68. ¿Se distingue en la evaluación del riesgo entre la identificación de riesgos en amenazas específicas e incidentes de interrupción?

69. ¿La gestión del riesgo establece que clase de amenazas deben ser tratadas según su impacto en los procesos críticos del negocio?

70. ¿El proceso de evaluación de riesgo incluye el análisis sistemático, la priorización de los tratamientos de riesgo y sus costos relativos?

71. ¿Son las amenazas, vulnerabilidades, riesgos y los problemas que han sido identificados, documentados en un registro o parte de una base de datos de gestión de riesgos?

72. ¿Los resultados del BIA son entradas primordiales para la gestión del riesgo organizacional y su papel en el contexto de la continuidad del negocio?

73. ¿Es la evaluación de riesgo completada por cada unidad de negocio y la división de apoyo operacional dentro de la organización al menos una vez cada 6 (seis) meses, y firmada por el gerente de negocios asignado?

74. ¿Se ha completado una evaluación de riesgos por cada unidad de negocio y la división de apoyo operacional dentro de la organización al menos una vez en los últimos 6 (seis) meses?

75. ¿Se han identificado y documentado por ejemplo, un edificio / sitio con zonas de alta concentración de riesgo operacional (grupos de riesgo) y / o un

proveedor / prestador de varias actividades de sus recursos de apoyo y / o dependencias prioritarias?

76. ¿El proceso de evaluación de riesgos proporciona una evaluación de riesgos con una presentación estandarizada y comprensible?

77. ¿Las medidas de tratamiento, mitigación de la pérdida y prevención del riesgo necesarias para eliminar, controlar y / o gestionar los riesgos relacionados con interrupciones con respecto a cada actividad priorizada han sido identificadas y puesto en práctica?

78. ¿Se han establecido y documentado niveles de riesgo aceptables para las actividades críticas y sus dependencias?

79. ¿Se han evaluado los tratamientos de riesgo relacionados con amenaza que pueden ser perjudiciales para cada actividad prioritaria de sus recursos de apoyo y dependencias?

80. ¿Están los tratamientos de riesgo acorde con los objetivos de continuidad de negocios de la organización?

81. ¿Están los tratamientos de riesgo acordes con el apetito de riesgo de la organización?

82. ¿Se lleva a cabo revisiones periódicas para prevenir, minimizar o eliminar la exposición de las actividades críticas y sus recursos de apoyo y dependencias a las amenazas e incidentes identificados?

83. ¿Están los proveedores subcontratados preparados para tener capacidad de continuidad del negocio demostrable y eficaz y los arreglos en su lugar?

84. ¿Es la planificación de escenarios empleada como parte de la evaluación del riesgo y del proceso de gestión con respecto a las actividades críticas y la continuidad de las mismas?

85. ¿Se han determinado los niveles de riesgo de los escenarios identificados?

86. ¿Se han identificado los tratamientos de riesgo en relación con los escenarios identificados?

87. ¿Se ha determinado la probabilidad y severidad de los escenarios?

88. ¿Existe un procedimiento documentado de una revisión continua de los escenarios identificados en relación con las actividades prioritarias de la organización y sus dependencias?

89. ¿Hay un procedimiento y un proceso para la revisión permanente de los riesgos de incidentes en el contexto de las interrupciones identificados en relación con las actividades prioritarias de la organización de sus recursos de apoyo y dependencias?

90. ¿Se documenta el proceso de revisión en curso?

91. ¿Están los registros y las bases de datos de gestión de riesgos revisados en intervalos relevantes y acorde a la planificación?

92. ¿El proceso de revisión requiere que la información sea puesta al día y que se haga de manera confidencial?

93. ¿Hay un programa definido y los recursos asignados para la realización de la revisión en curso?

94. ¿Es el BCMS un tema permanente en la agenda de la organización de Riesgo / Comité de Auditoría o la Junta Directiva?

95. ¿Hay un documentado corporativo (Organización) que detalle la Estrategia BCM firmada por la máxima autoridad de la institución?

96. ¿Está la estrategia basada en un enfoque global de la empresa?

97. ¿La estrategia proporciona un conjunto de directrices y normas mínimas o directrices reguladoras o de otra +índole?

98. ¿Son los riesgos asociados, limitaciones y supuestos, elementos fundamentales en relación con la estrategia y su aplicación se establece en la estrategia?

99. ¿Los principios fundamentales de BCM se basan en el riesgo operacional y proporcional al impacto en el negocio?

100. ¿Se revisa y se evalúa la estrategia, al menos una vez cada 12 (doce) meses, para asegurarse de que sigue siendo actual, apropiada (adecuados a los objetivos) y plausible?

101. ¿Existe un proceso de control de cambios documentado para asegurar que la estrategia sigue siendo relevante y actualizada?

102. ¿Está la estrategia basada en reflejar la naturaleza de la organización, la escala y la complejidad de la misma, incluyendo su entorno operativo, perfil de riesgo y el apetito de riesgo?

103. ¿La estrategia proporciona un marco organizacional BCM estandarizado globalmente y estructuralmente?

104. ¿Están los roles clave de BCM claramente definidos y documentados dentro de la estrategia?

105. ¿Se revisa la estrategia y se evalúa, al menos una vez cada 12 (doce) meses, para asegurarse de que sigue siendo relevante y actualizada?

106. ¿Hay estrategia de recuperación(es) para las actividades críticas de la organización de sus recursos de apoyo y dependencias que ha sido firmado por la alta dirección?

107. ¿Se ha asignado la responsabilidad de la estrategia global a alguien específico?

108. ¿Se ha asignado un rol organizacional para garantizar la revisión y evaluación de las estrategias de continuidad de negocio reanudación y recuperación de la organización?

109. ¿Están las funciones clave de continuidad de negocio, responsabilidades y autoridad claramente definidas y establecidas dentro de la estrategia?

110. ¿La estrategia está basada y es consistente con el perfil actual de recuperación asignado por el BIA?

111. ¿La estrategia define cómo la organización se encargará de la reanudación y recuperación de sus actividades priorizadas, sus recursos de soporte y dependencias?

112. ¿La estrategia de recuperación para las actividades críticas es consistente con los tiempos objetivos de recuperación de las actividades prioritarias?

113. ¿Las estrategias de continuidad del negocio están basadas en vulnerabilidades que puedan afectar la recuperación de las actividades críticas?

114. ¿Las estrategias de continuidad del negocio están balanceadas en una relación costo-beneficio?

115. ¿Las estrategias de continuidad de negocio son modeladas con base en una viabilidad global de implementación?

116. ¿Los resultados de las estrategias de continuidad de negocio han sido identificados y documentados?

117. ¿La organización realiza evaluaciones de las capacidades de continuidad de negocio de sus proveedores como parte del proceso del desarrollo de la estrategia?

118. ¿Está la estrategia basada en concordancia con la evaluación del riesgo actual de las actividades prioritarias de la organización y sus dependencias?

119. ¿Está la estrategia basada en el apetito de riesgo documentado por la organización e incluyendo la aceptación del riesgo residual?

120. ¿La estrategia toma en cuenta las actividades de negocio que no se definen como actividades prioritarias?

121. ¿Determina la estrategia cómo se van a gestionar las relaciones con sus grupos de interés clave y grupos externos que participan en el proceso de reanudación y recuperación?

122. ¿Los recursos que se necesitan para poner en práctica la estrategia han sido homologados junto con un presupuesto suficiente?

123. ¿Se revisa la estrategia y se evalúa, al menos una vez cada 12 (doce) meses, para asegurarse de que sigue siendo actual, apropiada (adecuados a los objetivos) y plausible?

124. ¿Existe un proceso de control de cambios documentado para asegurar que la estrategia sigue siendo relevante y actualizada?

125. ¿La estrategia establece el perfil de reanudación o recuperación crítico para la organización de actividades priorizadas (productos y servicios), sus recursos de apoyo y dependencias?

126. ¿La estrategia establece el nivel aceptable (funcionales y de rendimiento) de la reanudación del negocio o recuperación operacional para las

actividades priorizadas (productos y servicios) sus recursos de apoyo y dependencias?

127. ¿La estrategia ha probado con éxito o invocado, al menos una vez en los últimos 12 meses, para asegurarse de que es apropiada (adecuada para el propósito) y puede alcanzar su fin y los objetivos en los plazos requeridos?

128. ¿Hay una estrategia de recuperación de recursos documentada para las actividades críticas de negocio y sus dependencias que ha sido firmado por la alta dirección?

129. ¿La estrategia tiene los riesgos asociados, limitaciones y supuestos críticos en relación con y su implementación dentro de la estrategia?

130. ¿Se ha asignado a un responsable para la estrategia de recuperación?

131. ¿Se ha asignado un papel organizacional para garantizar la revisión y evaluación de la continuidad del negocio en el contexto de las estrategias de recuperación de los recursos?

132. ¿Están las funciones principales de continuidad de negocio, responsabilidades y autoridad claramente definidas y establecidas dentro de la estrategia?

133. ¿Se ha realizado un análisis de rentabilidad con respecto a la estrategia y sus opciones de recuperación de recursos o soluciones?

134. ¿Existe un proceso de control de cambios documentado para asegurar que la estrategia permanece actual, apropiada (adecuada a los objetivos) y plausible?

135. ¿Está la estrategia relacionada con los requisitos de recuperación de recursos identificados en el actual BIA, en contexto con las actividades críticas de la organización, de su perfil de recuperación, los servicios de apoyo y dependencias?

136. ¿En la estrategia se establecen los objetivos de tiempo de recuperación de las TIC, los objetivos de punto de recuperación de datos y los tiempos de recuperación de otros recursos técnicos necesarios para alcanzar el nivel previsto de aceptabilidad de la (funcionalidad y rendimiento) recuperación de

las actividades priorizadas (productos y servicios) sus recursos de apoyo y dependencias?

137. ¿La estrategia establece los tiempos de recuperación de los recursos no técnicos necesarios para alcanzar el nivel previsto de aceptable (funcionalidad y rendimiento) recuperación de las actividades criticas (productos y servicios) sus recursos de apoyo y dependencias?

138. ¿Se revisa la estrategia y evalúa, al menos una vez cada 12 (doce) meses, para asegurarse de que sigue siendo actual, apropiada (adecuados a los objetivos) y plausible?

139. ¿Se ha revisado la estrategia y se evaluado al menos una vez en los últimos doce (12) meses para asegurarse de que sigue siendo actual, apropiada (adecuados a los objetivos) y plausible?

140. ¿La estrategia se ha probado con éxito o invocado al menos una vez en los últimos 12 meses para asegurarse de que es apropiada (adecuado para el propósito) y puede alcanzar su fin y los objetivos en los plazos requeridos?

141. ¿Se cuenta con los recursos necesarios dentro de las estrategias para abarcar el enfoque de: Personas (22313 ISO: Cláusula 8.3.2.2)?

142. ¿Se cuenta con los recursos necesarios dentro de las estrategias para abarcar el enfoque de: Información y datos (22313 ISO: Cláusula 8.3.2.3)?

143. ¿Se cuenta con los recursos necesarios dentro de las estrategias para abarcar el enfoque de: Los edificios, ambiente de trabajo y servicios asociados (22313 ISO: Cláusula 8.3.2.4)?

144. ¿Se cuenta con los recursos necesarios dentro de las estrategias para abarcar el enfoque de: Instalaciones, equipos y consumibles (22313 ISO: Cláusula 8.3.2.5)?

145. ¿Se cuenta con los recursos necesarios dentro de las estrategias para abarcar el enfoque de: Información y comunicación (TIC) y la tecnología (22313 ISO: Cláusula 8.3.2.6)?

146. ¿Se cuenta con los recursos necesarios dentro de las estrategias para abarcar el enfoque de: Transporte (22313 ISO: Cláusula 8.3.2.7)?

147. ¿Se cuenta con los recursos necesarios dentro de las estrategias para abarcar el enfoque de: Finanzas (22313 ISO: Cláusula 8.3.2.8)?

148. ¿Se cuenta con los recursos necesarios dentro de las estrategias para abarcar el enfoque de: Socios, proveedores y partes interesadas (22313 ISO: Cláusula 8.3.2.9)?

149. ¿Se cuenta con los recursos necesarios dentro de las estrategias para abarcar el enfoque de: Seguridad?

150. ¿Se cuenta con los recursos necesarios dentro de las estrategias para abarcar el enfoque de: Servicios especializados BCM?

151. ¿Se cuenta con los recursos necesarios dentro de las estrategias para abarcar el enfoque de: Salvamento?

152. ¿Tiene cada sitio o construcción de la organización una gestión de emergencias?

153. ¿Cada sitio o construcción de la organización lleva a cabo simulacros regulares del plan de Evacuación o Manejo de Emergencias?

154. ¿Cada sitio o construcción de la organización han registrado una prueba de Plan de Manejo de Emergencia / Evacuación (taladro)?

155. ¿La organización tiene una estructura de gestión de incidentes, procedimientos y mecanismos que proporciona un control total de la respuesta a un incidente de interrupción?

156. ¿El proceso de planificación y el marco de apoyo cuenta con plantillas para proporcionar un enfoque de planificación estandarizado?

157. ¿Ha sido la capacidad de respuesta y el manejo de incidentes de la organización demostrado con éxito a través de la invocación o el ejercicio?

158. ¿Existe un procedimiento o plan para responder y gestionar diferentes tipos de perturbador incidente, por ejemplo, en las empresas o en el

159. ¿La estructura de respuesta a incidentes vela por la seguridad y el bienestar de los afectados?

160. ¿Hay recursos suficientes entrenados, competentes y capaces para apoyar los procedimientos de continuidad de negocio, planes, acuerdos y procedimientos para la gestión de un incidente?

161. ¿Tiene la organización un plan documentado de gestión Corporativa de Crisis (CCMP)?

162. ¿El CCMP establece una estructura operativa, de proceso y respuesta predefinida para la gestión de una crisis corporativa?

163. ¿El CCMP cuenta con propósito, objetivos y alcance definidos claramente establecidos?

164. ¿El plan contiene directrices y criterios respecto de cuales personas tienen la autoridad para invocar cada plan y en qué circunstancias?

165. ¿Está la asignación de un responsable del CCMP documentada y firmada por el responsable del plan de su revisión, actualización y aprobación?

166. ¿Contiene el CCMP detalles para gestionar las consecuencias inmediatas de la crisis en la empresa?

167. ¿Está el CCMP integrado con otros planes de la organización, como la continuidad del negocio, gestión de incidentes y de las comunicaciones, los medios de comunicación y las relaciones públicas?

168. ¿Tiene cada sitio clave un Plan de Manejo de Incidentes?

169. ¿Cada plan establece una estructura operativa, de proceso y respuesta predefinida para la gestión de un incidente?

170. ¿El plan establece el riesgo operacional, limitaciones o suposiciones en relación con cada aplicación o su invocación?

171. ¿El plan cuenta con un propósito, objetivos y alcance definidos y documentados?

172. ¿Cada plan contiene detalles para gestionar la consecuencia inmediata de un incidente de interrupción y la prevención de otros daños de las actividades prioritarias de la organización?

173. ¿Cada plan debe contener persona (s) para gestionar las fases de continuidad del negocio y recuperación de negocio del incidente o interrupción?

174. ¿Está cada plan alineado con otros arreglos de continuidad de negocio externos a la organización?

175. ¿Cada plan contiene material de referencia relevante?

176. ¿Cada plan contiene directrices y criterios respecto de los cuales las personas tienen la autoridad para invocar cada plan y en qué circunstancias?

177. ¿Tiene cada plan contiene un proceso para retornar una vez un incidente ha terminado?

178. ¿El plan contiene plantillas de formulario estandarizadas?

179. ¿Cada plan, o parte de este, tiene una copia de seguridad o tiene almacenado fuera del sitio para referencia y uso durante un incidente?

180. ¿Los controles financieros, responsabilidades y competencias en materia de gestión de incidentes están establecidos dentro de cada plan?

181. ¿Está cada plan integrado con otros planes, por ejemplo la continuidad de la organización empresarial, la gestión de crisis corporativa y comunicaciones, medios de comunicación y las relaciones públicas?

182. ¿Cada plan contiene un método (registro de incidentes) para el registro de la información vital acerca de la crisis de las empresas, las medidas adoptadas y las decisiones tomadas?

183. ¿Cada plan y sus componentes se ejecutan o se verifican al menos una vez cada 12 meses?

184. ¿El ejercicio de cada plan es coordinado, integrado y vinculado con otras organizaciones y grupos de interés?

185. ¿Es revisado y actualizado cada plan, al menos una vez cada 12 (doce) meses o cuando se producen cambios significativos en la organización o sus actividades críticas, para asegurarse de que sigue siendo actual, apropiado (adecuados a los objetivos) y plausible?

186. ¿Existe un control de versión documental con notificación y gestión de cambio para cada plan?

187. ¿Existe un proceso para proporcionar un plan de acción prioritaria y documentada para implementar los cambios aprobados en el plan dentro de un plazo de tiempo, por ejemplo, mantenimiento posterior acordado, auditoría, no conformidad, informes de pruebas o la invocación de los planes, etc.?

188. ¿El plan contiene un plan de contacto basado en un árbol de llamadas?

189. ¿Cada plan proporciona un proceso claramente definido para examinar las comunicaciones internas y externas, los medios de comunicación y relaciones públicas durante un incidente?

190. ¿Tiene cada plan líneas claramente identificadas de la comunicación?

191. ¿Cada plan contiene detalles de respuesta a través de la organización durante y después de un incidente?

192. ¿Tiene cada plan detalles sobre cómo y bajo qué circunstancia (s) la organización se comunicará con el personal y sus familiares, las principales partes interesadas y contactos de emergencia?

193. ¿Cada plan contiene persona (s) para gestionar el aspecto de comunicaciones de un incidente o interrupción de negocios nominado?

194. ¿Existe un directorio de contactos clave, por ejemplo para los principales y suplentes empleados, proveedores, grupos de interés, los servicios, las autoridades y los reguladores, etc. dentro de cada plan?

195. ¿Se han identificado y proporcionado los recursos necesarios para poner en marcha un centro de gestión de incidentes?

196. ¿Hay recursos suficientes y capacitados disponibles para operar el centro de gestión de incidentes?

197. ¿Los centros de gestión de incidentes de la organización son revisados y actualizados de forma regular?

198. ¿La creación y funcionamiento de los centros de mando de gestión de incidentes de la organización han sido probados o invocado con éxito, y han demostrado ser adecuados (aptos para el propósito) y plausibles?

199. ¿Los centros de gestión de incidentes de la organización han sido probados o invocado, al menos una vez en los últimos doce (12) meses, para asegurar que pueden alcanzar exitosamente los objetivos previstos dentro de los plazos exigidos?

200. ¿Los centros de gestión de incidentes tienen medios primarios y secundarios de comunicación?

201. ¿La gestión de incidentes de la organización incluye el enlace con otras organizaciones, como los servicios de emergencia, proveedores, reguladores y otros actores o partes interesadas que pueden estar implicados en la gestión de un incidente perturbador?

202. ¿Se ha documentado el procedimiento de enlace?

203. ¿Se han identificado las principales funciones u organizaciones que participan en la activación del plan de gestión de incidentes?

204. ¿Los puntos y los detalles de enlace clave se revisan y se actualizan de forma regular?

205. ¿Existe un protocolo de comunicaciones internas y externas documentado para facilitar el proceso de enlace?

206. ¿Los roles y responsabilidades de los involucrados en el plan de respuesta y la gestión inmediata de incidentes se han identificado y documentado?

207. ¿El equipo ha sido ensayado o invocado, al menos una vez en los últimos 12 meses, para asegurarse de que puede lograr sus objetivos dentro de los plazos requeridos con éxito?

208. ¿Es el equipo ensayado al menos una vez cada 12 meses junto con el Plan de Manejo de Incidentes?

209. ¿Los miembros de cada equipo han sido provistos de una memoria de incidentes basado en el plan, que ofrece consejos, instrucciones, orientación y detalles clave de contacto?

210. ¿El personal dentro de cada equipo tiene la responsabilidad necesaria, la autoridad, competencia y capacidad para afrontar su papel en un incidente?

211. ¿Cada equipo tiene procedimientos para regir sus actividades?

212. ¿Cada plan contiene detalles de las tareas y acciones que deben llevarse a cabo?

213. ¿Hay una lista de tareas / acción para la activación del procedimiento de respuesta / plan inmediato / incidente?

214. ¿Hay una lista de tareas / acción para que se tomen las medidas inmediatas?

215. ¿Se ha comunicado la lista de tareas a cada equipo?

216. ¿La lista de acciones de tareas y las personas, roles y equipos responsables son revisados y actualizados con regularidad?

217. ¿Se han ejercitado las listas de acciones de tareas y se han probado para demostrar su eficacia y viabilidad?

218. ¿Hay un ciclo de mantenimiento documentado y financiado del programa para cada plan de gestión de incidentes y sus partes componentes, que busque asegurarse de que sigue siendo apropiado (adecuado para el propósito), plausible y capaz de alcanzar sus objetivos y resultados?

219. ¿La respuesta a incidentes organizacionales y la estructura de la continuidad del negocio apoyan la comunicación interna y externa con las partes interesadas, incluidas las autoridades y los medios de comunicación durante un incidente?

220. ¿La organización tiene documentados los lineamientos generales (estrategia, procesos, procedimientos y el plan) de comunicaciones, medios de comunicación autorizados y las relaciones públicas

221. ¿La estrategia y el plan establecen una estructura operativa, de proceso y respuesta predefinida, para la gestión de las comunicaciones, medios de comunicación y relaciones públicas durante o después de un incidente perjudicial o crisis de las empresas?

222. ¿La estrategia y el responsable del plan están firmados en físico y con nombre de quién es responsable del plan, de su revisión, mantenimiento y efectividad?

223. ¿La estrategia y el plan están aprobados por la dirección?

224. ¿El plan señala a una persona responsable de canalizar la comunicación?

225. ¿El proceso de comunicación de la organización involucra a los miembros del plan de relaciones públicas?

226. ¿Se han notificado a los responsables de los medios de comunicación interna de la organización sus responsabilidades ante un evento de crisis y su relación con el plan de relaciones públicas?

227. ¿La estrategia de comunicación y relaciones públicas abarca la empresa a nivel global?

228. ¿Existen responsables de gestionar redes sociales y medios no convencionales con respecto a la comunicación y respuesta ante eventos críticos?

229. ¿El plan documenta los medios oficiales de comunicación ante una crisis?

230. ¿El plan contiene directrices y criterios respecto de las personas que tienen la autoridad para invocar el plan y en qué circunstancias?

231. ¿El plan contiene un proceso de cierre una vez que el incidente ha terminado?

232. ¿El plan contiene detalles sobre cómo y bajo qué circunstancias la organización se comunicará con el personal y sus familiares, las principales partes interesadas y los contactos de emergencia?

233. ¿El plan contiene un método (registro de incidentes) para el registro de información vital sobre el incidente de interrupción, las medidas adoptadas y las decisiones tomadas?

234. ¿El plan de comunicación se ha ejecutado y validado al menos una vez en los últimos doce meses?

235. ¿El plan está incluido dentro del sistema de notificaciones o árbol de llamadas?

236. ¿El plan contiene instrucciones obligatorias, consejos, proceso, procedimiento o directrices relativas a la coordinación central de comunicaciones y divulgación de la información interna y externa?

237. ¿Tiene la organización una guía o modelo de redacción de una declaración para los medios de comunicación?

238. ¿El plan tiene mensajes estándar 'iniciales' para todos los empleados, contratistas, proveedores y una declaración de retención para los medios de comunicación?

239. ¿La organización ha demostrado procedimientos y capacidad para atender medidas extraordinarias para la emisión de avisos, alertas y comunicación externa con rapidez, especialmente para las partes interesadas con necesidades especiales?

240. ¿El plan tiene un directorio de contactos clave y suplentes, por ejemplo, los medios de comunicación, empleados, proveedores, grupos de interés, servicios tercerizados, proveedores, autoridades y reguladores, etc.?

241. ¿Tiene la organización un proceso para atender las consultas de los clientes, grupos de interés afectados por la crisis, incidente o interrupción del negocio, por ejemplo; una mesa de ayuda?

242. ¿El plan asegura que toda la información de los medios se pone a disposición a través del sitio web de la organización?

243. ¿La organización ha establecido un lugar adecuado para apoyar la coordinación con los medios de comunicación y otros grupos de partes interesadas?

244. ¿Tiene la organización un centro de conferencia de prensa (diferente de las instalaciones de enlace)?

245. ¿La organización ha documentado los planes de continuidad de negocio con respecto a cada una de las actividades críticas y sus dependencias?

246. ¿Cada plan se ajusta a un contenido mínimo estándar basado en las normas ISO 22301 (8.4.4) o 22313 (4.4.4.2)?

247. ¿Está documentado el nombramiento de una persona como responsable del proceso de continuidad en su área crítica?

248. ¿El propósito, objetivos y alcance están definidos y establecidos claramente en el plan?

249. ¿El plan de continuidad del negocio está fundamentado en actividades críticas nominadas por un BIA?

250. ¿La planificación de planes de continuidad del negocio se ejecuta de manera organizada a través de plantillas de trabajo?

251. ¿Están los controles financieros, responsabilidades y autoridad en relación con el proceso de continuidad de negocios establecidos en el plan?

252. ¿Las diferentes secciones dentro de cada plan proporcionan una estructura modular que distintos módulos se pueden suministrar a las personas o equipos en una necesidad de conocimiento?

253. ¿Se mantiene una copia del plan de continuidad del negocio fuera de la organización para poder ser ejecutado en caso de ser invocado?

254. ¿Tiene cada plan un método (registro de incidentes) para el registro de información vital sobre el incidente de interrupción, las medidas adoptadas y las decisiones tomadas?

255. ¿Está cada plan integrado con otros planes de la organización de continuidad del negocio y arreglos por ejemplo ITDR, área de recuperación de trabajo, medios de comunicación y relaciones públicas, gestión de incidentes y crisis de las empresas?

256. ¿Cada plan contiene el RTO y el nivel de reanudación o recuperación en términos de funcionalidad y el rendimiento de cada actividad prioritaria?

257. ¿Cada plan incluye detalles de las dependencias internas y externas?

258. ¿Cada plan detalla sus partes interesadas?

259. ¿Cada plan contiene procedimientos que abordan temas de seguridad documental?

260. ¿Tiene cada plan detalles para gestionar las consecuencias inmediatas de una interrupción del negocio, la prevención de otros daños y la interrupción de las actividades prioritarias?

261. ¿Cada plan identifica los roles y equipos que tienen la antigüedad necesaria, la autoridad, la capacidad, la competencia para controlar y gestionar el incidente y comunicarse con las partes interesadas?

262. ¿Se ha asignado cada rol dentro del plan para un director y un delegado?

263. ¿Tiene cada plan un proceso para ser retirado una vez que el incidente perturbador se acabe?

264. ¿Cada plan de determinar persona (s) para gestionar el aspecto de comunicaciones de una interrupción del negocio nominado?

265. ¿Tiene cada plan detalles de la política de comunicación de la organización y la respuesta durante y después de un incidente perturbador?

266. ¿Existe un directorio de contactos clave, por ejemplo, para los principales y suplentes empleados, proveedores, grupos de interés, los servicios, las autoridades y los reguladores, etc. dentro de cada plan?

267. ¿Tiene cada plan líneas de comunicación claramente identificadas?

268. ¿Cada plan proporciona un proceso claramente definido para examinar las comunicaciones internas y externas, los medios de comunicación y relaciones públicas durante un incidente de la continuidad del negocio?

269. ¿Tiene cada plan detalles sobre cómo y bajo qué circunstancias la organización se comunicará con el personal y sus familiares, las principales partes interesadas y los contactos de emergencia?

270. ¿Tiene cada plan detalles e identifica los sistemas de TIC en que se basa su reanudación y hace referencia a los procedimientos de continuidad de TIC que existen?

271. ¿Las diferentes secciones dentro de cada plan proporcionan una estructura modular sobre distintos módulos que se pueden suministrar a las personas o equipos en una necesidad de conocimiento?

272. ¿Cada plan contiene procedimientos que abordan cuestiones de salvamento de instalaciones, equipos, tecnología, datos e información documentada?

273. ¿Tiene cada plan establecido operaciones o procesos manuales alternos para cerrar cualquier brecha que pueda existir entre los servicios de TI y su reanudación?

274. ¿Los planes son validados y probados cada doce meses?

275. ¿Existe una documentación detallada en el plan para su invocación (activación) y el proceso de escalación que figura en el mismo?

276. ¿Cada plan contiene un proceso para ser retirado una vez que el incidente perturbador se acabe?

277. ¿Hay un ciclo de mantenimiento documentado y financiado para el programa, el plan y sus componentes, para asegurarse de que sigue siendo apropiado (adecuado para el propósito), plausible y capaz de cumplir sus objetivos y los resultados requeridos?

278. ¿Existe un proceso de control de cambios documentado para asegurar que cada plan sigue vigente, adecuado (adecuados a los objetivos) y plausible cuando se producen cambios significativos en la organización o sus actividades empresariales críticos?

279. ¿Existe un control de versiones con registros de notificación y de distribución del cambio formal?

280. ¿Tiene cada plan listas de tareas predefinidas, que incluye tareas obligatorias y discrecionales, junto con las personas, roles y equipos responsables de su realización, y un proceso para el seguimiento dentro de un marco de tiempo asignado?

281. ¿Hay una lista de tareas para la activación de un BCP?

282. ¿Hay una lista de tareas sobre las medidas inmediatas que se deben tomar?

283. ¿La lista de tareas y las personas, roles, equipos responsables son revisados y actualizados con regularidad?

284. ¿Las listas de tareas han sido ejercidas y probadas para demostrar su eficacia y viabilidad?

285. ¿Están los contratos acordados y los niveles de servicio alineados a los objetivos de tiempo de recuperación de las actividades prioritarias?

286. ¿Están los tiempos de invocación y de respuesta de los servicios de BCM claramente definidos y alineados con los objetivos de tiempo de recuperación de las actividades prioritarias?

287. ¿Hay un horario para revisar esos acuerdos, para garantizar que sean pertinentes y actualizados?

288. ¿Los acuerdos de BCM son probados y actualizados con regularidad?

289. ¿Tiene la organización procedimientos de seguridad y de bienestar documentados dentro de cada plan de continuidad del negocio?

290. ¿Cada plan da la debida consideración al bienestar de las personas o equipos afectados o la gestión del incidente?

291. ¿Los procedimientos de seguridad y de bienestar dentro de cada plan incluyen la necesidad de que se preste especial atención a algún grupo con discapacidades u otras necesidades específicas?

292. ¿La organización proporciona guías y asesoramiento confidencial a los empleados afectados por el incidente?

293. ¿Tiene la organización un sistema de seguridad, primeros auxilios o equipos de evacuación a los entrenados, que se puede activar durante un incidente perturbador?

294. ¿La organización tiene un programa documentado de ejercicio, pruebas y proceso para la continuidad del negocio?

295. ¿El programa tiene como fin evaluar el cumplimiento del plan de continuidad?

296. ¿Los programas de ejercicio y prueba ante cada eventualidad cuentan con recursos y metas claros?

297. ¿El programa de ejercicio y pruebas proporciona directrices para la realización de ejercicios y exámenes?

298. ¿El programa de pruebas de la organización evalúa y se actualiza con regularidad?

299. ¿Los programas de prueba y ejecución de simulaciones de suficiencia y cumplimiento ante emergencias abarcan los planes de continuidad del negocio y de recuperación de desastres?

300. ¿La frecuencia de la ejecución de las simulaciones y planes de pruebas es coherente con el modelo, necesidad y tipo de negocio?

301. ¿El programa de pruebas toma en cuenta el tiempo de ejecución y recuperación de todos los elementos críticos ante una activación o simulación?

302. ¿Los programas de pruebas y ejecución abarcan los componentes tecnológicos críticos asociados a los procesos prioritarios, así como los proveedores trascendentales para la continuidad de las operaciones?

303. ¿El programa de ejercicio y pruebas verifica la recuperación de la tecnología, la informática y las telecomunicaciones incluyendo la disponibilidad y reubicación de personal técnico?

304. ¿Los ejercicios de prueba y simulación están acordes con las obligaciones contractuales de la organización?

305. ¿Los componentes humanos, tecnológicos y otros asociados al BCMS son identificados y descritos en el plan de simulación?

306. ¿Son ejercicios basados en escenarios apropiados y realistas?

307. ¿Son los ejercicios y pruebas consistentes con el alcance y los objetivos de continuidad de negocio, planes, procedimientos y arreglos?

308. ¿Es la escala y complejidad de ejercicios y pruebas apropiadas para la organización y sus objetivos de continuidad del negocio?

309. ¿Hay un informe post-ejercicio documentado junto con las recomendaciones producidas después de cada ejercicio o test?

VI CRITERIO DE HALLAZGO

Las empresas certificadas o en proceso de certificación deberán contar con un grado de cumplimiento superior al 85%, una nota inferior representará un hallazgo de auditoría.

Para las empresas en proceso de autoevaluación no certificadas, el cumplimiento debe ser superior a 75%.

Anexo #	15	**Nombre**	Prueba de Cumplimiento: Sección 9
Etapa	Planificación	**Archivo**	BCMS-2014-PC-06 - Seccion 9.docx

Prueba de Cumplimiento: Sección 9

I PROPÓSITO

Realizar una evaluación del contexto de la organización, los marcos regulatorios, las partes interesadas, dimensionamiento del alcance del plan de continuidad y la utilización de sistemas de continuidad del negocio como elemento habilitador de capacidades ante un incidente disruptivo.

II DESCRIPCIÓN DE LA PRUEBA

La prueba de cumplimiento para la sección 9; Evaluación, corresponde a la aplicación de un cuestionario digital por parte del auditor al auditado. quien ofrecerá evidencia suficiente para argumentar y justificar sus respuestas. Una vez procesados los datos, la herramienta brindará un grado de cumplimiento, la cual deberá cumplir con los parámetros definidos por la auditoría.

III JUSTIFICACIÓN

El entendimiento de la organización y su contexto permite determinar las actividades, funciones y responsables que permiten que la misma opere. A través de este ejercicio se puede identificar elementos críticos de la empresa y los posibles eventos que le pueden afectar.

El entendimiento de la organización ayuda a la identificación de las partes interesadas, así como las expectativas de los mismos con respecto a la empresa(Drewitt, 2013).

IV PROCEDIMIENTO

Para realizar esta prueba de cumplimiento, se debe convocar al auditado y contestar las siguientes preguntas, este, por su parte, debe aportar la evidencia suficiente para defender el proceso asociado:

Pregunta

1. ¿La organización evalúa el rendimiento de los planes de continuidad del negocio?
2. ¿Tiende la organización a mantener un programa de evaluación del desempeño BCMS por el que las evaluaciones temáticas y otras se llevan a cabo a intervalos planificados?
3. ¿Cubre el programa de evaluación del desempeño todo el ámbito de la organización en el contexto del BCMS?
4. ¿El proceso de evaluación de desempeño proporcionan los métodos y metodologías para el seguimiento sistemático, la medición, el análisis y la evaluación?
5. ¿El programa y los procedimientos de evaluación de la organización especifican los recursos competentes y cualificados deberán realizar evaluaciones de desempeño?

6. ¿El procedimiento de control y evaluación del desempeño tiene un conjunto de métricas de rendimiento / mediciones cuantitativas?
7. ¿Son evaluaciones influenciadas por las necesidades de las partes interesadas?
8. ¿Se vincula el conjunto de métricas de rendimiento / mediciones tanto al BCMS y sus resultados?
9. ¿El conjunto de métricas se alinean a las prácticas de gestión, indicadores operativos y económicos?
10. Los procesos de evaluación del desempeño cuentan con mecanismos de seguimiento y cumplimiento de los hallazgos identificados
11. ¿la evaluación del desempeño toma la forma de auditorías internas o externas?
12. Los procesos de evaluación del desempeño están diseñados para favorecer y fortalecer la continuidad del negocio de las funciones críticas?
13. ¿Los procedimientos de seguimiento y evaluación del desempeño incluyen medidas proactivas de desempeño que monitorean el cumplimiento de la BCMS con la legislación aplicable, regulación, autorización de funcionamiento y los requisitos contractuales?
14. ¿Los procedimientos de seguimiento y evaluación del desempeño incluyen medidas reactivas de desempeño para monitorear los incidentes (incluyendo cuasi accidentes y las falsas alarmas) y otras evidencias históricas de desempeño deficiente BCMS?
15. ¿Las actividades realizadas a través la activación, las pruebas, los informes post-incidente, exámenes de la gestión, auditorías, evaluaciones de madurez y otros tipos verificadas por el proceso de evaluación del desempeño?
16. ¿Tiene la organización evaluar periódicamente el cumplimiento de las obligaciones legales, reglamentarios y contractuales aplicables y buenas prácticas de la industria?
17. ¿Se documenta los planes de evaluación del desempeño y sus informes de operación?

18. ¿El informe incluye la identificación de no conformidades y recomienda medidas correctivas?
19. ¿Aborda el informe de evaluación las oportunidades para la mejora continua de la idoneidad, adecuación y eficacia del BCMS?
20. ¿Son las recomendaciones resultantes de la evaluación priorizadas y realizadas dentro de un plazo de tiempo acordado?
21. ¿Tiene la organización a retener información documentada como la evidencia de su programa de evaluación de desempeño y resultados / productos?
22. ¿Tiene la organización evaluaciones de desempeño conducta de sus procedimientos de continuidad de negocio, los medios y capacidades con el fin de verificar su continua aptitud, idoneidad y eficacia?
23. ¿Tiene la organización realizar sus evaluaciones de desempeño de sus procedimientos y mecanismos de continuidad de negocio a intervalos planificados, como parte de su programa global de evaluación BCMS?
24. ¿Las evaluaciones abordan la posible necesidad de cambios en las políticas, objetivos, estrategias y otros elementos de los procedimientos de continuidad de negocio y acuerdos que incluyen la mejora continua?
25. ¿Son las evaluaciones influenciadas por las necesidades de las partes interesadas?
26. ¿Son las evaluaciones realizadas a través del ejercicio, las pruebas, los informes post-incidente, exámenes de la gestión, auditorías, evaluaciones de madurez y otros tipos de evaluación de desempeño?
27. ¿Los ejecutores de las evaluaciones tienen criterio suficiente para interpretar y recomendar en el informe?
28. ¿Cada evaluación verifica el cumplimiento y la conformidad de sus procedimientos y mecanismos de continuidad de negocio con su propia política y objetivos de la continuidad del negocio?
29. ¿Usa la organización autoevaluaciones, auditorías internas o externas para evaluar sus procedimientos y mecanismos de continuidad de negocio?

30. ¿Están involucrados las partes interesadas o actores en la evaluación de los procedimientos y mecanismos de continuidad de negocios de la organización?
31. ¿Verifica la evaluación que todos los productos y servicios clave y sus actividades y recursos de apoyo se han identificado e incluido en la estrategia de continuidad del negocio de la organización?
32. ¿La evaluación verifica la competencia y capacidad de las personas, roles ejecutores de la gestión, mando, control y coordinación de la respuesta organizacional de incidentes perturbadores o crisis de las empresas?
33. ¿Verifica la evaluación que el mantenimiento de la continuidad del negocio organización y el ejercicio de los programas de pruebas se han implementado de manera efectiva?
34. ¿Verifica la evaluación que las estrategias y procedimientos de continuidad de negocios de la organización incorporan mejoras identificadas durante los incidentes y ejercicios y mediante el programa de mantenimiento?
35. ¿Verifica la evaluación que la organización cuenta con un programa permanente de capacitación y sensibilización de continuidad del negocio?
36. ¿La evaluación verificará que los procedimientos de control de cambios y sus procesos están en su sitio y funcionan de manera efectiva?
37. ¿Cada evaluación verifica los procedimientos de continuidad de negocio y que los arreglos están en cumplimiento con los requisitos legales, reglamentarios, contractuales y de licencias de funcionamiento y de la industria de buenas prácticas?
38. ¿Tiende la organización a retener información documentada en relación con todas las evaluaciones de sus procedimientos y mecanismos de continuidad de negocio y sus resultados, conclusiones y salidas como evidencia de la evaluación?
39. ¿Tiene la organización un programa de mantenimiento claramente definido y documentado para sus BCMS, incluyendo sus procedimientos de continuidad de negocio y arreglos en particular?

40. ¿Está la responsabilidad de la gestión y mantenimiento de los procedimientos de las organizaciones de continuidad del negocio o arreglos claramente documentado?
41. ¿El propósito de los planes de mantenimiento es mantener actualizado, idóneo y eficiente los planes de continuidad de la organización?
42. ¿Tiende la organización a retener información documentada en relación con su programa de mantenimiento que incluye los resultados, conclusiones, salidas como evidencia del mantenimiento continuo?
43. ¿Cubre el programa de mantenimiento de la organización todo el ámbito de BCMS de la organización?
44. ¿El programa de mantenimiento organizacional garantiza y verifica que están capacitadas, son competentes y capaces las personas clave que van a poner en práctica la estrategia de continuidad del negocio y los procedimientos?
45. ¿El programa de mantenimiento organización proporciona la verificación de la planificación y control del BCM operacional?
46. ¿Los cambios en las leyes, reglamentos, contratos de licencias y normas son incorporadas en el BCMS?
47. ¿Se documentan los planes de acción correctivos?
48. ¿Los planes de acción correctivos resultantes de la evaluación post-ejercicio o revisión- auditoría son prioridad y se ejecutarán dentro de un plazo acordado?
49. ¿Hay un proceso documentado para comunicar, en el momento oportuno, cualquier inadecuación clave o incumplimiento o no conformidades a altos directivos o comités pertinentes?
50. ¿Las medidas adoptadas para garantizar que los cambios y sus implicaciones para los sistemas de continuidad de negocio, procedimientos y disposiciones existentes son comprendidas por los grupos de interés internos o externos relevantes o por las partes interesadas?

51. ¿La organización realiza auditorías internas a intervalos planificados para proporcionar información sobre si los BCMS se aplican y mantienen de manera efectiva?
52. ¿Tiende la organización a mantener un programa de auditoría BCMS, así como auditorías temáticas asociadas a la continuidad a llevar a cabo en intervalos planificados?
53. ¿El programa y los procedimientos de auditoría especifican los recursos competentes y calificados que deberán emplearse durante la ejecución?
54. ¿Cubre el programa de auditoría interna de la organización todo el ámbito de BCMS?
55. ¿El programa de auditoría y los procedimientos cubren el alcance, frecuencia, las metodologías, las responsabilidades y los requisitos para llevar a cabo auditorías e informar los resultados?
56. ¿Verifica la auditoría interna que el BCMS se ajusta a los requisitos de la organización?
57. ¿El proceso de auditoría BCMS tiene en cuenta los resultados de auditorías anteriores?
58. ¿Verifica el proceso de auditoría y valida que el BCMS está logrando sus objetivos y se ajusta a sus disposiciones planificadas?
59. ¿El proceso de auditoría identifica oportunidades de mejora?
60. ¿Hay un informe de auditoría formal publicado después de cada auditoría?
61. ¿Son los resultados de la auditoría y los resultados utilizados para corregir las no conformidades específicas?
62. Son los resultados y las conclusiones de las auditorías informados a la alta dirección, directivos y comités pertinentes?
63. ¿Tiende la organización a retener información documentada como evidencia de la aplicación de los resultados de la auditoría del programa de auditoría, los hallazgos, recomendaciones, productos y cualquier acción tomada?
64. ¿El programa de revisión especifica un informe que deberá presentarse después de cada revisión de la gestión?

65. ¿Posterior a la revisión se elaboran informes?
66. ¿Son las recomendaciones resultantes de los comentarios seguidas y actualizadas en los sistemas de BCM, procedimientos y arreglos?
67. ¿El informe incluye la identificación de no conformidades y recomienda medidas correctivas?
68. ¿Hay una lista de distribución acordada por el informe sobre la gestión?

VI CRITERIO DE HALLAZGO

Las empresas certificadas o en proceso de certificación deberán contar con un grado de cumplimiento superior al 85%, una nota inferior representará un hallazgo de auditoría.

Para las empresas en proceso de autoevaluación no certificadas, el cumplimiento debe ser superior a 75%.

Anexo #	16	**Nombre**	Prueba de Cumplimiento: Sección 8
Etapa	Planificación	**Archivo**	BCMS-2014-PC-07 - Seccion 10.docx

Prueba de Cumplimiento: Sección 10

I PROPÓSITO

Realizar una evaluación del contexto de la organización, los marcos regulatorios, las partes interesadas, dimensionamiento del alcance del plan de continuidad y la utilización de sistemas de continuidad del negocio como elemento habilitador de capacidades ante un incidente disruptivo.

II DESCRIPCIÓN DE LA PRUEBA

La prueba de cumplimiento para la sección 9; Evaluación, corresponde a la aplicación de un cuestionario digital por parte del auditor al auditado; quien ofrecerá evidencia suficiente para argumentar y justificar sus respuestas. Una vez procesados los datos, la herramienta brindará un grado de cumplimiento, la cual deberá cumplir con los parámetros definidos por la auditoría.

III JUSTIFICACIÓN

El entendimiento de la organización y su contexto, permite determinar las actividades, funciones y responsables que permiten que la misma opere. A través de este ejercicio se puede identificar elementos críticos de la empresa y los posibles eventos que le pueden afectar.

El entendimiento de la organización ayuda a la identificación de las partes interesadas así como las expectativas de los mismos con respecto a la empresa. (Drewitt, 2013).

IV PROCEDIMIENTO

Para realizar esta prueba de cumplimiento se debe convocar al auditado y contestar las siguientes preguntas, este por su parte debe aportar la evidencia suficiente para defender el proceso asociado:

Pregunta

1. Cuando la organización identifica una no conformidad, ¿cómo reacciona en cuanto a tomar medidas para controlar, corregir y hacer frente a las consecuencias?
2. ¿La identificación de una no conformidad representa un proceso de seguimiento y validación?
3. Cuando la organización identifica una no conformidad. ¿se determinan e implementan las acciones correctivas necesarias?
4. ¿La organización revisa la eficacia de las medidas correctivas adoptadas y realiza cambios en el BCMS y procedimientos de continuidad de negocio, en particular, si es necesario?
5. ¿Tiende la organización a retener información documentada como evidencia de la naturaleza de las no conformidades, acciones posteriores tomadas y los resultados de la acción correctiva?
6. ¿Tiende la organización a mejorar continuamente la idoneidad, adecuación o eficacia de las BCMS?

7. ¿La organización utiliza el proceso de las BCMS como el liderazgo, la planificación y la evaluación del desempeño para lograr una mejora?
8. ¿Tiene la organización a retener información documentada como evidencia de la mejora continua de sus procedimientos de continuidad BCMS y de negocios en particular?

VI CRITERIO DE HALLAZGO

Las empresas certificadas o en proceso de certificación deberán contar con un grado de cumplimiento superior al 85%, una nota inferior representará un hallazgo de auditoría.

Para las empresas en proceso de autoevaluación no certificadas, el cumplimiento debe ser superior a 75%.

Anexo #	17	**Nombre**	OFICIO DE COMUNICACIÓN DE INICIO DE AUDITORÍA
Etapa	Ejecución	**Archivo**	BCMS-2014-E1 - Notificacion de Inici

CONSECUTIVO

X *de* ***XXX*** *del* ***20XX***

Señor

NOMBRE COORDINADOR DEL PROCESO

Coordinador del BCMS

ASUNTO:	***Comunicación sobre inicio de estudio de auditoría de ISO 22301 sobre el BCMS y dependencias asociadas.***

La Gerencia General, con fundamento en su Plan Estratégico del 2014, efectuará un estudio de cumplimiento sobre los componentes asociados al plan de gestión para la continuidad del negocio a lo largo de todas dependencias asociadas al alcance de los mismos.

Dicho lo anterior, favor girar las instrucciones al personal y a los miembros asociados al proceso en estudio para que la ejecución de la evaluación sea profesional, fluida, sistemática, suficiente y eficaz, acorde con lo requerido por la alta gerencia.

El estudio está a cargo de. ***NOMBRE DEL AUDITOR LIDER****, miembro del equipo de auditoría y el suscrito, por lo que en caso de tener alguna duda podría contactarnos a los teléfonos* ***NNNNNNNN*** *y* ***NNNNNNNN****, respectivamente.*

Respetuosamente

Lic. _____

LIDER DEL EQUIPO DE AUDITORÍA

ENTIDAD ENCARGADA

Anexo #	18	**Nombre**	Formulario de Aceptación de Ejecución de prueba de control
Etapa	Ejecución	**Archivo**	 BCMS-2014-E2-For mulario de Entrevist

Formulario de Aceptación de Ejecución de prueba de control

En LUGAR DONDE SE ESTA EJECUTANDO LA PRUEBA, a las HH; MM del DD-MM-YYYY, se efectúa prueba de cumplimiento CODIGO DE LA PRUEBA a NOMBRE DEL AUDITADO, quien se hace acompañar de NOMBRE DEL SEGUNDO AUDITADO y el señor NOMBRE DEL AUDITOR en calidad de ejecutor de la auditoría y NOMBRE DE ASISTENTE DE AUDITORÍA en el rol de soporte a la auditoría.

El auditado ha sido notificado y él ha aceptado la ejecución de la prueba con las siguientes características:

I PROPÓSITO

Realizar una evaluación del contexto de la organización, los marcos regulatorios, las partes interesadas, dimensionamiento del alcance del plan de continuidad, y la utilización de sistemas de continuidad del negocio como elemento habilitador de capacidades ante un incidente disruptivo.

II DESCRIPCIÓN DE LA PRUEBA

La prueba de cumplimiento para la sección de la normativa ISO 22301,corresponde a la aplicación de un cuestionario digital por parte del auditor al auditado; quien ofrecerá evidencia suficiente para argumentar y justificar sus respuestas. Una vez procesados los datos, la herramienta brindará un grado de cumplimiento la cual deberá cumplir con los parámetros definidos por la auditoría.

III JUSTIFICACIÓN

El entendimiento de la organización y su contexto permite determinar las actividades, funciones y responsables que permiten que la misma opere. A través de este ejercicio se puede identificar elementos críticos de la empresa y los posibles eventos que le pueden afectar.

El entendimiento de la organización ayuda a la identificación de las partes interesadas, así como las expectativas de los mismos con respecto a la empresa(Drewitt, 2013).

VI CRITERIO DE HALLAZGO

Las empresas certificadas o en proceso de certificación deberán contar con un grado de cumplimiento superior al 85%, una nota inferior representará un hallazgo de auditoría.

Para las empresas en proceso de autoevaluación no certificadas, el cumplimiento debe ser superior a 75%.

Registro de firmas			
Auditor	Auditado	Asistente	Asistente Auditoría

Anexo #	19	**Nombre**	Cedula para Registro de Hallazgos
Etapa	Ejecución	**Archivo**	BCMS-2014-E3 - Cedula de Hallazgo.

CEDULA PARA REGISTRO DE HALLAZGO

Código	BCMS-2014-E-H-**XX**	Visibilidad	_ Pub _Priv _Lim
ID Prueba	BCMS-2014-P-PC- XX	Pregunta	
Nombre		Auditor	

I DATOS GENERALES

II DESCRIPCION DE HALLAZGO

Condición	
Criterio	
Causa	
Efecto	
Recomendación	

III SOPORTE DOCUMENTAL

ID	Descripción	Tipo	Observaciones

IV REGISTRO DE FIRMAS

Auditor	Asistente	Auditado (Opcional)

Anexo #	20	**Nombre**	INDICE DE HALLAZGOS
Etapa	Ejecución	**Archivo**	BCMS-2014-E4 - Indice de Hallazgos.

INDICE DE HALLAZGOS

ID Hallazgo detectado	ID Prueba Asociada	Descripción	Sección

Anexo #	21	**Nombre**	BCMS-2014-C1-Informe Final
Etapa	Comunicación	**Archivo**	BCMS-2014-E4 - Indice de Hallazgos.

22 de febrero de 2015

Señor
NOMBRE DEL SOLICITANTE
PUESTO DEL SOLICITANTE
NOMBRE EMPRESA

Estimado señor:

Adjunto para su conocimiento, el informe del estudio de la evaluación realizada al proceso "Sistema para la gestión de la continuidad del Negocio", en el cual se presentan los resultados obtenidos de la evaluación, la razonabilidad y eficacia de los controles internos establecidos por la institución para gestionar dicho proceso.

Con la finalidad de analizar y discutir el informe y considerar las observaciones de la Administración Activa en la emisión del informe final y las sugerencias de mejora operativas en el proceso producto de la evaluación, se les convoca a reunión el próximo DD de MM de YYYY, a las HH:MM p.m. en esta Auditoría.

Atentamente,

Alberto González Villalobos
Auditor Líder