SISTEMA DE GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Wilson Manuel Nieto Parada
Wilsonnieto1603@gmail.com

RESUMEN: El Sistema de Gestión de la Continuidad del Negocio (**SGCN**) se ha convertido en una exigencia para las empresas que compiten el día de hoy en los mercados globalizados, se trata de disminuir y evitar las interrupciones del negocio que tienen un impacto sobre la efectiva ejecución de los procesos críticos de la organización en un momento determinado, teniendo un plan logístico de cómo actuar en estos momentos críticos que afectan a la organización por cualquier tipo de motivo, el plan tiene que abarcar todo el ámbito de la organización para cada proceso de esta, ninguno de sus componentes puede dejar de operar ya que si un elemento del todo dejara de funcionar se paraliza todos los procesos, generando el caos. Cada miembro del sistema tiene que demostrar que es un proveedor confiable. Esto se logra teniendo en cada empresa un **SGCN** que proteja a los procesos esenciales que permiten originar los productos o servicios que desea el cliente, pasando por encima de cualquier adversidad y garantizando la presentación de los servicios en cada momento.

ABSTRACT: Business Continuity Management System or in short, (BCMS), has become a requirement for companies competing today in globalized markets. This management consists in decrease and/or avoids all the disruptions that can affect critical processes of the organization at a given time.
The companies needs a logical plan of how to act in this critical times, the plan must cover every process of the organization, none of it components or processes can´t stop operating because if an element stops then all processes would be paralyzed, creating chaos.
Each member of the system has to demonstrate that it is a reliable supplier. This is achieved by having each company with a BCMS that protects the essential processes that enable the products or services cause the customer wants, passing over any adversity and ensuring the presentation of services at all times.

PALABRAS CLAVES: Contingencia, continuidad, gestión, incidente, disponibilidad y recuperación.

1. INTRODUCCIÓN

El plan de continuidad de negocio abarca todos los sectores de negocio, dado con más énfasis en aquellos donde la disponibilidad de la información es su mayor activo. A partir del 11 de septiembre de 2001, los planes de continuidad de negocio cobraron importancia abarcando con mayor cobertura a compañías del sector financiero y sus asociados, donde hoy en día tiene su mayor aplicación, pero cabe aclarar que no importa el tamaño de la empresa o el sector en el que se desenvuelva, un plan de continuidad puede ser aplicado tanto a empresas grandes, medianas, pequeñas e incluso micro empresas, como a cualquier proceso, después de este trágico evento tomo más fuerza, en todo el mundo el pensar e implementar un plan de continuidad de negocio donde se pondrá demostrar la capacidad estratégica y táctica de una organización para planificar y responder ante incidentes o interrupciones de negocio con el fin de continuar las operaciones a un nivel aceptable de servicio previamente definido. Desde este momento entra a ser parte importante de las compañías el Sistema de Gestión de Continuidad de Negocio (SGCN), el cual consiste en una preparación proactiva de la organización frente a contingencias, mediante el desarrollo de mecanismos para restaurar los procesos claves, protegiendo el servicio al cliente y por ende la reputación de la compañía esto tiene como fin permitir la administración, planificación, seguimiento, control y mejoramiento permanente de la estrategia de continuidad del negocio de la organización para garantizar su operación crítica en caso de una contingencia.
Cuando hablamos de continuidad del negocio nos referimos a la capacidad de sobrevivir a las “cosas malas” que pueden tener un impacto negativo en la empresa: desde un brote de virus informático hasta un brote de virus biológico, y todos los demás peligros entre ambos, como incendios, inundaciones, tornados, huracanes, terremotos, etc. El estándar internacional para la continuidad del negocio, ISO 22301, la define como la “capacidad [de una organización] de continuar la prestación de productos o servicios en los niveles predefinidos aceptables tras incidentes de interrupción de la actividad” [1].

La Gestión de la Continuidad del Negocio (también llamada BCM, por sus siglas en inglés) es el proceso de lograr mantener la continuidad del negocio después de cualquier incidente y volver a su estado de servicio como debe estar debidamente planeado, este proceso conforma una parte vital de la gestión de seguridad de sistemas de información, este proceso no es sólo para TI sino para todos los procesos de la compañía, aunque la mayoría de las organizaciones de hoy son sumamente dependientes de la tecnología y se han dado cuenta que su mayor activo es la información que puede estar en cualquier lugar de la compañía, desde equipos portátiles, hasta servidores, equipos de escritorio, tabletas y Smartphone, pero queda claro que esta tecnología puede verse afectado por una amplia gama de incidentes potencialmente desastrosos, dañando parcialmente la información o pudiendo ser mucho más grave a tal grado de dañar toda la información, estos incidentes pueden ir desde cortes en el suministro de energía provocados por

tormentas hasta la pérdida de datos causada por equivocaciones de los empleados o por criminales informáticos.

Desde las áreas de TI, estaba claro que las organizaciones iban a necesitar estrategias para prepararse para dichos incidentes, responder a ellos y recuperarse de estos. Por ese motivo, gran parte de los primeros trabajos sobre el manejo de incidentes de interrupción de la actividad provino de la comunidad de TI.

No obstante, con el paso del tiempo, la disciplina de "recuperación ante desastres" evolucionó a "un proceso de gestión holístico" que "identifica amenazas potenciales para la organización y el impacto que de llevarse a cabo su materialización podría ocasionar perdidas en las operaciones corporativas, y que proporciona un marco para crear resistencia corporativa de modo que pueda dar una respuesta eficaz que proteja los intereses de sus grupos de interés, reputación, marcas y actividades de creación de valor fundamentales".

Pero para estar más seguro vemos que El SGCN está fundamentado en la norma ISO 22301, pero hay que tener en cuenta que, aunque tu empresa no necesita tener certificación ISO 22301 para sobrevivir a un desastre, si debe tener a la mano una guía que sería esta norma en la cual se reúnen las mejores prácticas para tener en cuenta a la hora de querer implementar un SGCN, aunque algunas corporaciones desean conseguir esta certificación para mejorar su programa de SGCN y a la vez para ganar más mercado. Las dos empresas deberían partir de una base fundamental para poder consolidar un El Sistema de Gestión de Continuidad de Negocio basándonos en la evolución que han tenido sus estándares como lo muestra la Figura 1.

Figura 1: Evolución de los estándares en continuidad de negocio [7]

2. CONCEPTOS BÁSICOS

ISO 22301:2012 Seguridad Social – Sistema de gestión de continuidad de negocio – Requisitos, proporciona los requisitos para un Sistemas de Gestión de Continuidad de Negocio basado en las mejores prácticas de gestión de continuidad de negocio.

SGCN: Sistema de Gestión de la Continuidad del Negocio

Administración del Plan de Continuidad de Negocios: Es un sistema administrativo integrado, transversal a toda la organización, que permite mantener alineados y vigentes todas las iniciativas, que contiene estrategias, planes de respuesta y demás componentes y actores de la continuidad del negocio. Busca mantener la viabilidad antes, durante y después de una interrupción de cualquier tipo. Abarca las personas, procesos de negocios, tecnología e infraestructura.

Incidente de Trabajo: Es un evento que no es parte de la operación estándar de un servicio y el cual puede causar interrupción o reducción en la calidad del servicio y en la productividad.

Problema de Continuidad de Negocio: Es un evento interno o externo que interrumpe uno o más de los procesos de negocio. El tiempo de la interrupción determina que una situación sea un incidente o un desastre.

Planes de contingencia: Conjunto de acciones y recursos para responder a las fallas e interrupciones específicas de un sistema o proceso.

Plan de Continuidad de Negocio (PCN): Conjunto detallado de acciones que describen los procedimientos, los sistemas y los recursos necesarios para retornar y continuar la operación, en caso de interrupción [2].

Plan de Recuperación de Desastres (DRP): Es la estrategia que se sigue para restablecer los servicios de tecnología (red, servidores, hardware y software) después de haber sufrido una afectación por un incidente o catástrofe de cualquier tipo, el cual atente contra la continuidad del negocio.

Análisis de Impacto del Negocio (BIA): Es la etapa que permite identificar la urgencia de recuperación de cada área, determinando el impacto en caso de interrupción.

Disponibilidad: La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, igual que los recursos necesarios para su uso [3].

Amenaza: Persona, situación o evento natural del entorno (externo o interno) que es visto como una fuente de peligro, catástrofe o interrupción. Ejemplos: inundación, incendio, robo de datos.

Vulnerabilidad: Es una debilidad que se ejecuta accidental o intencionalmente y puede ser causada por la falta de controles, llegando a permitir que la amenaza ocurra y afecte los intereses de la Institución. Ejemplos: Deficiente control de accesos, poco control de versiones de software, entre otros.

Riesgo: Es la probabilidad de materialización de una amenaza por la existencia de una o varias vulnerabilidades con impactos adversos resultantes para la Entidad.

Frecuencia: Estimación de ocurrencia de un evento en un período de tiempo determinado. Los factores a tener en cuenta para su estimación son la fuente de la amenaza y su capacidad y la naturaleza de la vulnerabilidad.

Impacto: Es el efecto que causa la ocurrencia de un incidente o siniestro. La implicación del riesgo se mide en aspectos económicos, imagen, reputación, disminución de capacidad de respuesta y competitividad, interrupción de las operaciones, consecuencias legales y afectación física a personas. Mide el nivel de degradación de uno de los siguientes elementos de continuidad: Confiabilidad, disponibilidad y recuperación.

3. UN PROGRAMA BÁSICO DE SGCN EN CUATRO PASOS

Desafortunadamente, algunas empresas deben cerrar cuando las alcanza un desastre para el cual no estaban preparadas adecuadamente, es lamentable porque el camino para dicha preparación está bien documentado. Cualquier empresa de

cualquier tamaño puede mejorar las posibilidades de superar un incidente de interrupción de la actividad y quedar en una pieza si sigue ciertas estrategias probadas y de confianza, más allá de que desee obtener la certificación ISO 22301 o no.
A continuación cuatro posibles pasos para que cualquier empresa puede empezar a crear un sistema de gestión de continuidad de negocio basándose en procesos, iniciando si es más fiable por el proceso principal del negocio y replicando así buenas prácticas de este, a un nivel macro sobre los demás procesos:

3.1 Identifica y ordena las amenazas

Crea una lista de los incidentes de interrupción de la actividad que constituyan las amenazas más probables para la empresa, teniendo en cuenta que no debes usar la lista de otro, porque las amenazas varían según la ubicación. Por ejemplo, aquí en Bogotá, hay un grado relativamente alto de sensibilización con respecto a los terremotos y a los atentados terroristas, por lo que muchas organizaciones llevaron a cabo un nivel básico de planificación para prepararse ante desastres teniendo esos eventos en cuenta. ¿Pero qué ocurre donde se encuentra tu empresa? ¿Y qué pasa con la fuga de datos o la interrupción de la infraestructura de TI, que pueden ocurrir en cualquier parte? ¿Qué pasa si un producto químico tóxico provoca que se cierren las instalaciones por varios días? ¿Estás ubicado cerca de una vía ferroviaria? ¿De una autopista importante? ¿Cuánto depende tu empresa de proveedores extranjeros?

En esta etapa, una buena técnica es reunir personas de todos los departamentos en una sesión de intercambio de ideas. El objetivo de la reunión es crear una lista de los posibles escenarios ordenados por probabilidad de ocurrencia y por potencial de causar un impacto negativo, tratar de tener en cuenta todos los factores por mínimos que sean, ya que puedan ayudar a restablecer la continuidad del negocio o viceversa, que nos puedan generar una parálisis en la operación diaria de cualquier proceso o de toda la organización. Ya que si podemos tener todos los escenarios posibles sabremos como actuar en cualquier tipo de adversidad que se llegue a presentar.

3.2 Realiza un análisis del impacto en la empresa

Necesitas determinar qué partes de tu empresa son las más críticas para funcionalidad de tu organización. Una manera es comenzar detallando las funciones, los procesos, los empleados, los lugares y los sistemas que son críticos para el funcionamiento de la organización. De esto se puede ocupar el líder del proyecto de SGCN; para ello, deberá entrevistar a los empleados de cada departamento y luego elaborar una tabla de resultados que enumeren las funciones y las personas principales y las secundarias, después deberás determinar la cantidad de **"**días de supervivencia" de la empresa para cada función. ¿Cuánto puede resistir la empresa sin que una función en particular provoque un impacto grave?, luego ordenarás el impacto de cada función en caso de que no esté disponible. Por ejemplo, Michael Miora [4], experto en recuperación ante desastres, sugiere utilizar una escala de 1 a 4, donde 1 = impacto crítico en las actividades operativas o pérdida fiscal, y 4 = sin impacto a corto plazo. Si luego se multiplica el Impacto por los "días de supervivencia", se puede ver cuáles son las funciones más críticas. Al principio de la tabla quedarán las funciones con un impacto mayor y con sólo un día de supervivencia, de igual manera se genera un listado de las personas que son dueñas del proceso o al función y se tratara de determinar en caso de no estar esta persona quien sería la más capacitada para suplirla en el momento de poner en marcha el plan de continuidad de negocio. [4]

3.3 Crea un plan de respuesta y recuperación

En esta etapa deberás catalogar datos clave sobre los bienes involucrados en la realización de las funciones críticas, incluyendo sistemas de TI, personal, instalaciones, proveedores y clientes. Deberás incluir números de serie de los equipos, acuerdos de licencia, alquileres, garantías, detalles de contactos, etc. Necesitarás determinar "a quién llamar" en cada categoría de incidente y crear un árbol de números telefónicos para que se hagan las llamadas correctas en el orden correcto. También necesitas una lista de "quién puede decir qué cosa" para controlar la interacción con los medios durante un incidente (considera quedarte con una estrategia de "sólo el Director ejecutivo" si se trata de un incidente delicado).
Deberán quedar documentados todos los acuerdos vigentes para mudar las operaciones a ubicaciones e instalaciones de TI temporales, de ser necesario. No te olvides de documentar el proceso de notificación para los miembros de la empresa en su totalidad y el procedimiento de asesoramiento para clientes.
Los pasos para recuperar las operaciones principales deberían ordenarse en una secuencia donde queden explícitas las interdependencias funcionales. Cuando el plan esté listo, asegúrate de capacitar a los gerentes sobre los detalles relevantes para cada departamento, así como la importancia del plan general para sobrevivir a un incidente, ten en cuenta que desde que ocurre el incidente se tiene un cronograma para poder restablecer la continuidad del negocio pero alternamente tiene que haber un plan logístico de la misma manera como se planeó el de respuesta o (DRP) plan de recuperación de desastres para poder volver a dejar a la organización en el mismo punto, al ser ejecutado el plan de continuidad de negocio recuerda son dos planes que tienes que tener en cuenta de esto depende la supervivencia y continuidad de tu organización. [4]

3.4 Prueba el plan y refina el análisis

La mayoría de los expertos en BCM recomiendan probar el plan al menos una vez al año**,** con ejercicios, análisis paso a paso o simulaciones. La prueba te permite sacar el mayor provecho a lo que invertiste en la creación del plan, y no sólo te permite encontrar fallas y dar cuenta de los cambios corporativos con el transcurso del tiempo, sino que también te ayudan a contemplar aspectos de fiabilidad en la conmutación a los sistemas de copia de seguridad que nos garanticen la continuidad de los trabajos críticos causa una buena impresión en la gerencia.
No cabe duda de que estos cuatro pasos significan un enorme trabajo, pero es una tarea que las empresas ignoran bajo su propio riesgo. Si el proyecto parece demasiado desalentador para aplicar a la empresa completa, considera comenzar por unos pocos departamentos o una sola oficina, si hay varias. Todo lo

que vayas aprendiendo en el proceso se podrá aplicar en mayor escala a medida que progreses. Evita a toda costa pensar que las cosas malas no suceden, porque sí lo hacen. Sólo tienes que estar preparado, y no pretendas pensar que cuando ocurra algo no será tan malo, porque podría serlo.

Si no cuentas con la infraestructura para tener un centro de respuesta alterno puedes ser muy activo y mirar con que equipos y recursos mínimos podemos poner a funcionar cada proceso de esta manera sabrás como actuar y tendrás un total control de lo mínimo que necesitas para continuar sabiendo que lo más importante para que funcione el proceso es la información y la persona que la conoce y la maneja, ya que tienes que tener un respaldo de la información de cada proceso en un lugar alterno que debes decidirlo con tu gerente el cual debe tener pleno conocimiento de cómo actuar en dicho evento.

Ten en cuenta de hacer pruebas al activo más crítico de cualquier empresa la información, trata de realizar restauración de backups con frecuencia para mirar si al restaurar de esta información la restaura desde el punto deseado de no ser así desde que punto, con todos los privilegios y que es fácil de consultar por los usuarios sin generar ningún retraso adicional, por que como suele suceder no nos queda tiempo para hacer este tipo de pruebas y a la hora de necesitarlo vamos a ver que la información, o no esta o está incompleta que al restaurar no carga los perfiles, permisos y datos necesarios para ser accedida y por ende no se podrá poner en marcha el plan de continuidad de negocio, las pruebas también te dan un conocimiento de cómo actuar y como actual la gente en este tipo de casos ya que en un desastre todos los seres humanos actuamos de formas diferentes a veces la persona más adecuada no es la que tenga mayor poder si no la que sea más crítica para dirigir y organizar en un momento determinado.[4]

4. MEJORA CONTINUA DEL PLAN DE SGCN

Ciclo PHVA para la implementación de la mejora continua y la integración con el sistema de SGCN Figura 2

Figura 2: Mejora continua del sistema de gestión de la continuidad del negocio [5]

La preocupación por la continuidad del negocio es sin duda uno de los puntos principales en las iniciativas estratégicas de las empresas del sector de las tecnologías de la Información, que valoran más que nadie, los gravísimos inconvenientes, tanto económicos como empresariales que se podrían causar debido a un tiempo de inactividad.[6] por esto la mejora continua va de la mano con el plan de continuidad de negocio ya que todo parte de una base pero se tiene que ir retroalimentando de cada prueba de cada cambio que se valla realizando en los procesos de la organización ya que de este ciclo de vida depende la supervivencia de nuestra organización.

5. IMPORTANCIA DE LA NORMA ISO 22301:2012

La norma es particularmente importante en aquellas organizaciones que trabajan en entornos de altos riesgos donde la habilidad de continuar trabajando es de suma importancia para los negocios, clientes y partes interesadas – esto incluye las empresas de servicios públicos, financieras, de telecomunicaciones, de transportes y el sector público, a norma permitirá: Establecer, implementar, mantener y mejorar su Sistema de Gestión de Continuidad de Negocio, Cumplir con los requisitos de la política de continuidad de negocio y dar a las partes interesadas confianza en su conformidad y compromiso con las buenas prácticas reconocidas internacionalmente. La norma internacional ISO 22301 tiene como finalidad responder a las posibles apariciones de incidentes que pueden darse en las organizaciones. Para dar respuestas a los incidentes de una manera eficaz debemos de: Asegurar la ejecución de forma idónea de las actuaciones, a través de, la comunicación de los puntos frágiles de la seguridad de la información para que podamos estar preparados ante incidentes. Comunicación de los puntos débiles de la seguridad a los terceros, a los empresarios, entre otros. Evaluar los riesgos de seguridad en la información mediante los instrumentos adecuados. Garantizar la aplicación a través de la gestión de los incidentes de la seguridad que hablan sobre la información y mejora constante. Dar respuesta estructurada, eficaz y rápida, a través de la asignación de los procesos de gestión y responsabilidades.

5.1 Clausulas claves de la norma ISO 22301 para tenerlas como referente:

- **Cláusula 4:** Contexto de la organización: Determinar temas internos y externos que son relevantes para el propósito de la organización y que afectan su habilidad de alcanzar los resultados esperados de su SGCN. [1]

- **Cláusula 5:** Liderazgo: La alta dirección debe demostrar un compromiso continuo con el SGCN. A través de su liderazgo y acciones, la dirección puede crear un ambiente en el cual distintos miembros del personal estén completamente involucrados y el sistema de gestión pueda funcionar de manera eficaz en sinergia con los objetivos de la organización. [1]

- **Cláusula 6:** Planificación: Esta es una etapa crítica en la que se establecen objetivos estratégicos y principios para la orientación del SGCN en su totalidad. [1]

- Cláusula 7: Soporte: La gestión diaria de un SGCN, se basa en el uso de recursos apropiados para cada actividad. Estos recursos incluyen personal competente en base a formaciones y servicios de soporte, toma de conciencia y comunicación pertinentes (y demostrables), esto debe ser apoyado por información documentada adecuadamente gestionada. [1]

- **Cláusula 8:** Operación: Después de la planificación del SGCN, la organización debe ponerlo en funcionamiento. [1]

- **Cláusula 9:** Evaluación del desempeño: Una vez que el SGCN se ha implementado, la norma ISO 22301 requiere permanente seguimiento del sistema, así como revisiones periódicas para mejorar su operación, e implementar auditorías internas es la mejor práctica. [1]

- **Cláusula 10:** Mejora: La mejora continua se basa en EL PHVA que se debe implementar de la mano con el SGCN, para aumentar la eficacia (cumplir objetivos) y la eficiencia (proporción costo/beneficio óptimo) de los procesos y controles de seguridad para brindar más beneficios a la organización y a sus partes interesadas. [1]

6. CONCLUSIONES

El estándar ISO 22301:2012 engloba las distintas Metodologías y buenas prácticas en continuidad del Negocio generadas en los últimos casi 20 años, por ende es la guía a la cual cualquier empresa sin importar el tamaño o el capital a la cual pueden a acudir para poder implementar en su compañía un sistema de gestión de continuidad del negocio basándose siempre en buenas practicas.

El sistema de gestión de continuidad del negocio después de la catástrofe del 9 11 del 2001 que de evidenciado que es parte fundamental para cualquier compañía en el proceso de mejora continua para poder garantizar a su usuario que pase a cualquier incidente siempre se le va poder prestar el servicio por el cual está acudiendo a la empresa y de esta manera poder mantener la organización en un crecimiento sustancial en la prestación de los servicios.

Con estos simple pasos podemos asegurar que cualquier empresa que quiera implementar un sistema de gestión de continuidad del negocio no necesita ser enorme, lo único que necesita es poder implementarla correctamente, con esto disminuirá la posibilidad de ocurrencia de un incidente y, en caso de producirse, la organización estará preparada para responder en forma adecuada y, de esa forma, reducir drásticamente el daño potencial de ese incidente.

Debemos mirar que para cualquier compañía el activo más valioso es la información por ende tenemos que manejar su seguridad y disponibilidad para el momento en ocurra un incidente tener la seguridad de que la información es veraz y que no está siendo afectada por el incidente y así poder seguir prestando un servicio de alta calidad a nuestros clientes garantizando que la información es la misma con la que ellos cuentan.

7. REFERENCIAS

[1] El estándar internacional para la continuidad del negocio, ISO 22301, ISO 22301. Societal Security - Business Continuity Management Systems-Requirements 2012.
Sharp, John. The Route Map to Business Continuity management meeting the requirements. British Standards Institute, United Kingdom.
[2] Concepto tomado del Capítulo XXIII – Reglas relativas a la administración del riesgo operativo – de la Circular Básica Contable de la Superfinanciera.
[3] Concepto tomado del Capítulo XII – Requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios- Título I de la Circular Básica Jurídica de la Superfinanciera.
[4] Traducción y adaptación del post de Stephen Cobb en We Live Security.Alexander, Alberto. Diseño y Gestión de un Sistema de Gestión de
[5] Imagen 2 Copyright 2012 All rights reserved. Bureau Veritas Certification
[6]Fuente: Revista ISO Focus+, Edición junio 2012
Traducción al español: Secretaría Ejecutiva de COPANT
http://www.bsigroup.es/
[7] http://www.gestion.com.do/pdf/018/018-nuevo-estandar-internacional.pdf