GESTIÓN DE LA CONTINUIDAD DE NEGOCIO COMO FACTOR DE CONFIANZA EMPRESARIAL DESDE LA PERSPECTIVA DE LA SEGURIDAD INFORMÁTICA

Oviedo Morales, Edwin David
Ing.oviedo1@gmail.com
Universidad Piloto de Colombia

Resumen ----- Actualmente con el auge y apoyo que brindan las nuevas tecnologías a las operaciones empresariales, independientemente del sector en el cual se desarrolle la actividad económica el saber responder oportunamente ante una interrupción o falla es de vital importancia para garantizar y generar la confianza suficiente en el consumidor como para seguir creyendo y confiar en determinada empresa, es aquí donde aparece un concepto muy conocido en el ámbito tecnológico y el cual tiene como objetivo validar y proceder de la manera correcta para evitar las interrupciones en este ámbito de las tecnologías y es la continuidad de negocio(SGCN), apoyada o fundamentada en los conceptos de la seguridad informática.

Abstract ----- Currently with the rise and support offered by new technologies to business operations, regardless of the sector in which economic activity takes place knowing timely response to an interruption or failure it is vital to ensure sufficient and generate consumer confidence to continue to believe and trust in certain company, this is where a concept well known in the technology field and which aims to validate and proceed in the right way to avoid interruptions in this area of technology appears and continuity business (BCMS), supported or based on the concepts of security.

Índice de Términos ---- Continuidad, riesgo, recuperación, disponibilidad,desastre.

I. INTRODUCCIÓN

Toda operación o actividad económica desarrollada por x o y empresa tiene como objetivo el poder ofrecer o brindar a sus clientes accesos a los productos, haciéndolos llegar a sus usuarios mediante televisión, radio, presa e internet.

Basados en la premisa anterior se puede notar que el objetivo de las empresas es llegar a los usuarios o consumidores finales apoyándose en la tecnología, actualmente el medio más efectivo para comunicar una idea o venderse al público es el internet, la cual está apoyada y soportada bajo una infraestructura tecnológica que funciona las 24 horas del día todos los días del año y puede ser consultada y accedida desde cualquier lugar con acceso a internet.

¿Pero qué pasa cuando todo el apoyo tecnológico sobre el cual las empresas u organizaciones que soportan y mantienen las operaciones comerciales fallan? es aquí donde aparece a flote el concepto de Seguridad informática el cual trae consigo los planes de continuidad de negocio, que buscar ante cualquier eventualidad mantener las operaciones de la empresa funcionales y accesibles al público, soportando las actividades del negocio.

Repasando la historia se conoce y se menciona por diferentes medios como el 11 de septiembre del 2001, el día en el cual todos los organismos vieron con importancia la creación y mantenimiento continuo de planes de continuidad de negocio, esto a raíz que muchas de las empresas que funcionaban en las conocidas y desaparecidas torres gemelas, no volvieron a funcionar o abrir sus puertas al público porque toda la información de apoyo al negocio fue consumida por las llamas del atentado terrorista que afecto a los Estados Unidos de América.

No obstante se nota la necesidad a nivel de cualquier organización de tener un plan de continuidad de negocio bien estructurado y controlado para apoyar los objetivos de la organización y ser una base sólida para que la organización continúe funcionando y operando normalmente ante un incidente de seguridad que pueda poner en riesgo su supervivencia en el mercado.
Esta investigación tiene como objetivo mostrar la importancia de la continuidad de negocio como apoyo fundamental para lograr los objetivos empresariales y generar confianza en los usuarios desde la perspectiva de la seguridad informática con

las mejores prácticas de la industria o estándares internacionales.

II. CONCEPTOS RELACIONADOS

En el siguiente apartado se darán a conocer los conceptos relacionados con la continuidad de negocios, los estándares sobre los cuales esta soportada y el apoyo de la seguridad informática para crear estos planes de continuidad.

Continuidad de negocios

La continuidad de negocio se puede ser interpretada como la capacidad de respuesta oportuna y estratégica que debe poseer una organización para responder correctamente ante una interrupción o falla que afecte el normal funcionamiento de las operaciones de la misma y que esta pueda seguir funcionando sin problemas a un nivel aceptable.

El gestionar la continuidad de negocio, hace parte de la gestión de riesgos operacional como se muestra en figura 1, es la alta gerencia quien tiene el compromiso de garantizar que se apliquen y cumplan los planes de continuidad de negocios dentro de la organización.

Fig. 1. Gestión de la continuidad de negocio como parte de la Gestión del riesgo [1].

Los planes de continuidad del negocio no son estáticos, requieren una permanente evolución, un ciclo que les permita mantenerse actualizados y vigentes dependiendo, en gran medida, de los cambios del entorno. El modelo británico BS-5999 planteado por John Sharp presenta algunos pasos para el ciclo de vida del plan de continuidad en los siguientes términos: conocimiento de la organización, determinación de la estrategia de continuidad, desarrollo e implementación de la respuesta de la continuidad del negocio, ejercicios de mantenimiento y revisión, como se muestra en la figura No 2.

Fig. 2. Planes de continuidad de negocio en la organización [2].

Al igual que el modelo *británico BS-5999 planteado por John Sharp* también se expone la norma ISO 22301 dentro de la continuidad de negocios.

Para llegar a organizar planes de continuidad de negocio es indispensable basarse en los mejores estándares de la industria dentro de estos encontramos la **norma ISO 22301** la cual detalla los pasos para crear y mantener una plan de continuidad de negocios que apoye los objetivos de la organización.

Esta norma está basada en el ciclo PHVA, igual como lo hace la norma ISO 27001, con el objetivo de lograr una mejora continua y permanentemente, como se puede apreciar en la siguiente figura 3, correspondiente al ciclo de mejora continua del plan de continuidad de negocios y las partes involucradas en el proceso.

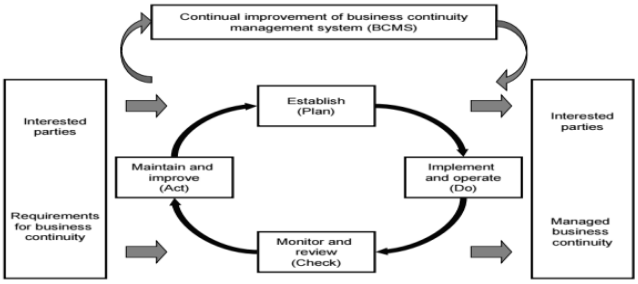

Fig. 3. Ciclo del plan de continuidad de negocios [3].

El ciclo PHVA comprende las siguientes fases, como se aprecia en la figura 4, aplicable no solo al campo de la seguridad informática o tecnologías de TI, si no a cualquier ámbito de la industria.

Plan (Establish)	Establish business continuity policy, objectives, targets, controls, processes and procedures relevant to improving business continuity in order to deliver results that align with the organization's overall policies and objectives.
Do (Implement and operate)	Implement and operate the business continuity policy, controls, processes and procedures.
Check (Monitor and review)	Monitor and review performance against business continuity policy and objectives, report the results to management for review, and determine and authorize actions for remediation and improvement.
Act (Maintain and improve)	Maintain and improve the BCMS by taking corrective action, based on the results of management review and reappraising the scope of the BCMS and business continuity policy and objectives.

Fig.4. Etapas del ciclo PHVA [4].

Las etapas del ciclo PHVA se definen a continuación con el objetivo de dejar claridad en cada uno de los conceptos aplicables al tratamiento del plan de continuidad de negocios, dentro de estas etapas encontramos, las siguientes:

Planificar: En esta etapa se definen los objetivos y cómo lograrlos, esto de acuerdo a políticas organizacionales y necesidades de los clientes. Puede ser de gran utilidad realizar grupos de trabajo, escuchar opiniones de los trabajadores y utilizar herramientas de planificación como por ejemplo: 5W2H en la cual se responden 7 preguntas claves cuyas palabras en inglés inician con W y H:
¿Qué (What)
¿Por qué (Why)
¿Cuándo (When)
¿Dónde (Where)
¿Quién (Who),
¿Cómo (How)
¿Cuánto (How much).
Importante recordar que esta etapa es muy importante y es la que permite el desarrollo de las otras, lo que indica que si no planeamos bien los resultados en las otras 3 etapas no serán confiables.

Hacer: Es ejecutar lo planeado, en esta etapa es recomendable hacer pruebas pilotos antes de implantar los procesos definidos. En su desarrollo se puede evidenciar los problemas que se tienen en la implementación, se identifican las oportunidades de mejora y su implementación.

Verificar: En esta etapa comprobamos que se hayan
ejecutado los objetivos previstos mediante el seguimiento y medición de los procesos, confirmando que estos estén acorde con las políticas y a toda la planeación inicial.

Actuar: Mediante este paso se realizan las acciones para el mejoramiento del desempeño de los procesos, se corrigen las desviaciones, se estandarizan los cambios, se realiza la formación y capacitación requerida y se define como monitorearlo.

La adopción del ciclo PHVA es de gran ayuda para actuar sobre los procesos y no sobre las personas, pues es frecuente que en las organizaciones se culpen a los trabajadores por los malos resultados cuando en realidad lo que falla es el proceso, de ahí la gran importancia que tiene el compromiso gerencial, pues es en este nivel en donde se deben buscar las estrategias que le permita a las empresas liderar el mercado, ser auto-sostenibles y rentables.

Para la ISO 22301 existen etapas que se deben cumplirse para que el plan de continuidad de negocios se pueda implementar, estas etapas pueden variar de acuerdo al contexto de la organización, las etapas deben tener la siguiente documentación como obligatoria para una empresa:

- Lista de requisitos legales, normativos y de otra índole.
- Alcance del SGCN.
- Política de la continuidad del negocio.
- Objetivos de la continuidad del negocio.
- Evidencia de competencias del personal.
- Registros de comunicación con las partes interesadas.
- Análisis del impacto en el negocio.
- Evaluación de riesgos, incluido un perfil del riesgo.
- Estructura de respuesta a incidentes.
- Planes de continuidad del negocio.
- Procedimientos de recuperación.
- Resultados de acciones preventivas.

- Resultados de supervisión y medición.
- Resultados de la auditoría interna.
- Resultados de la revisión por parte de la dirección.
- Resultados de acciones correctivas.

La norma establece las siguientes clausulas como referente para su implantación:

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.

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.

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.

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.

Cláusula 8: Operación: Después de la planificación del SGCN, la organización debe ponerlo en funcionamiento.

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.

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 [5].

Al igual que la ***ISO 22301***, ***ITIL Foundation*** también tiene un apartado en el cual detalla los pasos para implementar un plan de continuidad de negocios dentro de la organización, el proceso está orientado a mejorar la calidad de los servicios ofrecidos por la organización, estos procesos definen la continuidad de negocios como ***la forma de impedir que una imprevista y grave interrupción de los servicios TI, debido a desastres naturales u otras fuerzas de causa mayor, tenga consecuencias catastróficas para el negocio.***

Dice que la estrategia de la Gestión de la Continuidad del Servicio (ITSCM) debe combinar equilibradamente procedimientos:

Proactivos: que buscan impedir o minimizar las consecuencias de una grave interrupción del servicio.

Reactivos: cuyo propósito es reanudar el servicio tan pronto como sea posible (y recomendable) tras el desastre.

ITIL **hace una comparación entre las ventajas y desventajas de implantar el plan de continuidad de negocios**

Ventajas de una correcta Gestión de la Continuidad del Servicio se resumen en:

- Se gestionan adecuadamente los riesgos.
- Se reduce el periodo de interrupción del servicio por causas de fuerza mayor.
- Se mejora la confianza en la calidad del servicio entre clientes y usuarios.
- Sirve de apoyo al proceso de Gestión de la Continuidad del Negocio (BCM).

Las ***desventajas*** a la hora de implementar la Gestión de la Continuidad del Servicio se resumen en:

- Puede haber resistencia a realizar inversiones cuya rentabilidad no es inmediata.
- No se presupuestan correctamente los costes asociados.
- No se asignan los recursos suficientes.
- No existe el compromiso suficiente con el proceso dentro de la organización y las tareas y actividades correspondientes se demoran perpetuamente para hacer frente a "actividades más urgentes".
- No se realiza un correcto análisis de riesgos y se obvian amenazas y vulnerabilidades reales.
- El personal no está familiarizado con las acciones y procedimientos a tomar en caso de interrupción grave de los servicios.
- Falta de coordinación con la BCM.

Las principales actividades de la Gestión de la Continuidad de los Servicios TI se resumen en ITIL son:

- Establecer las políticas y alcance de la ITSCM.
- Evaluar el impacto en el negocio de una interrupción de los servicios TI.
- Analizar y prever los riesgos a los que está expuesto la infraestructura TI.
- Establecer las estrategias de continuidad del servicio TI.
- Adoptar medidas proactivas de prevención del riesgo.
- Desarrollar los planes de contingencia.
- Poner a prueba dichos planes.
- Formar al personal sobre los procedimientos necesarios para la pronta recuperación del servicio.
- Revisar periódicamente los planes para adaptarlos a las necesidades reales del negocio.

El proceso de gestión de continuidad de negocios de ITIL se detalla en la siguiente imagen.

Fig.5. Proceso de la gestión de continuidad del servicio [6].

Política y Alcance

El primer paso necesario para desarrollar una Gestión de la Continuidad del Servicio coherente es establecer claramente sus objetivos generales, su alcance y el compromiso de la organización TI: su política.

La gestión de la empresa debe demostrar su implicación con el proceso desde un primer momento pues la implantación de la ITSCM puede resultar compleja y costosa sin la contrapartida de un retorno obvio a la inversión.

Es imprescindible establecer el alcance de la ITSCM en función de:

- Los planes generales de Continuidad del Negocio.
- Los servicios TI estratégicos.
- Los estándares de calidad adoptados.
- El histórico de interrupciones graves de los servicios TI.
- Las expectativas de negocio.
- La disponibilidad de recursos.

La Gestión de la Continuidad del Servicio está abocada al fracaso sino se destina una cantidad de recursos suficientes, tanto en el plano humano como de equipamiento (software y hardware). Su dimensión depende de su alcance y sería absurdo y contraproducente instaurar una política demasiado ambiciosa que no dispusiera de los recursos correspondientes.

Una importante parte del esfuerzo debe destinarse a la formación del personal. Éste debe interiorizar su papel en momentos de crisis y conocer perfectamente las tareas que se espera desempeñe: una emergencia no es el mejor momento para

estudiar documentación y manuales.

Análisis de Impacto

Una correcta Gestión de la Continuidad del Servicio requiere en primer lugar determinar el impacto que una interrupción de los servicios TI pueden tener en el negocio.

En la actualidad casi todas las empresas, grandes y pequeñas, dependen en mayor o menor medida de los servicios informáticos, por lo que cabe esperar que un "apagón" de los servicios TI afecte a prácticamente todos los aspectos del negocio. Sin embargo, es evidente que hay servicios TI estratégicos de cuya continuidad puede depender la supervivencia del negocio y otros que "simplemente" aumentan la productividad de la fuerza comercial y de trabajo.

Cuanto mayor sea el impacto asociado a la interrupción de un determinado servicio mayor habrá de ser el esfuerzo realizado en actividades de prevención. En aquellos casos en que la "solución puede esperar" se puede optar exclusivamente por planes de recuperación.

Los servicios TI han de ser analizados por la ITSCM en función de diversos parámetros:

- Consecuencias de la interrupción del servicio en el negocio:
- Pérdida de rentabilidad.
- Pérdida de cuota de mercado.
- Mala imagen de marca.
- Otros efectos secundarios.
- Cuánto se puede esperar a restaurar el servicio sin que tenga un alto impacto en los procesos de negocio.
- Compromisos adquiridos a través de los SLAs.
- Dependiendo de estos factores se buscará un balance entre las actividades de prevención y recuperación teniendo en cuenta sus respectivos costes financieros.

Evaluación de Riesgos

Sin conocer cuáles son los riesgos reales a los que se enfrenta la infraestructura TI es imposible realizar una política de prevención y recuperación ante desastre mínimamente eficaz.

La Gestión de la Continuidad del Servicio debe enumerar y evaluar, dependiendo de su probabilidad e impacto, los diferentes riesgos factores de riesgo. Para ello la ITSCM debe:

Conocer en profundidad la infraestructura TI y cuáles son los elementos de configuración involucrados en la prestación de cada servicio, especialmente los servicios TI críticos y estratégicos.

Analizar las posibles amenazas y estimar su probabilidad.

Detectar los puntos más vulnerables de la infraestructura TI, tal como lo muestra la figura 6.

Fig.6. Riesgos asociados a los servicios de TI [7]

Estrategias de Continuidad

La continuidad de los servicios TI puede conseguirse bien mediante medidas preventivas, que eviten la interrupción de los servicios, o medidas reactivas, que recuperen unos niveles aceptables de servicio en el menor tiempo posible.

Es responsabilidad de la Gestión de la Continuidad del Servicio diseñar actividades de prevención y recuperación que ofrezcan las garantías necesarias a unos costes razonables.

Actividades preventivas

Las medidas preventivas requieren un detallado análisis previo de riesgos y vulnerabilidades. Algunos de ellos serán de carácter general: incendios, desastres naturales, etcétera, mientras que otros tendrán un carácter estrictamente informático: fallo de sistemas de almacenamiento, ataques de hackers, virus informáticos, etcétera.

La adecuada prevención de los riesgos de carácter general depende de una estrecha colaboración con la Gestión de la Continuidad del Negocio (BCM) y requieren medidas que implican a la infraestructura "física" de la organización.

La prevención de riesgos y vulnerabilidades "lógicas" o de hardware requiere especial atención de la ITSCM. En este aspecto es esencial la estrecha colaboración con la Gestión de la Seguridad.

Los sistemas de protección habituales son los de "Fortaleza" que ofrecen protección perimetral a la infraestructura TI. Aunque imprescindibles no se hallan exentos de sus propias dificultades pues aumentan la complejidad de la infraestructura TI y pueden ser a su vez fuente de nuevas vulnerabilidades.

Actividades de recuperación

Siempre será necesario poner en marcha procedimientos de recuperación.

En líneas generales existen tres opciones de recuperación del servicio:

Cold standby: que requiere un emplazamiento alternativo en el que podamos reproducir en pocos días nuestro entorno de producción y servicio. Esta opción es la adecuada si los planes de recuperación estiman que la organización puede mantener sus niveles de servicio durante este periodo sin el apoyo de la infraestructura TI.

***Warm standby*:** que requiere un emplazamiento alternativo con sistemas activos diseñados para recuperar los servicios críticos en un plazo de entre 24 y 72 horas.

Hot standby: que requiere un emplazamiento alternativo con una replicación continua de datos y con todos los sistemas activos preparados para la inmediata sustitución de la estructura de producción. Ésta es evidentemente la opción más costosa y debe emplearse sólo en el caso de que la interrupción del servicio TI tuviera inmediatas repercusiones comerciales.

Organización y Planificación

Una vez determinado el alcance de la ITSCM, analizados los riesgos y vulnerabilidades y definidas unas estrategias de prevención y recuperación es necesario asignar y organizar los recursos necesarios. Con ese objetivo la Gestión de la Continuidad del Servicio debe elaborar una serie de documentos entre los que se incluyen:

- Plan de prevención de riesgos.
- Plan de gestión de emergencias.
- Plan de recuperación.

Supervisión de la Continuidad

Una vez establecidas las políticas, estrategias y planes de prevención y recuperación, es indispensable que éstos no queden en papel y que la organización TI esté preparada para su correcta implementación.

Ello depende de dos factores clave: la correcta formación del personal involucrado y la continua monitorización y evaluación de los planes para su adecuación a las necesidades reales del negocio.

Formación

Es inútil disponer de unos completos planes de prevención y recuperación si las personas que eventualmente deben llevarlos a cabo no están familiarizadas con los mismos.

Es indispensable que la ITSCM:

- Dé a conocer al conjunto de la organización TI los planes de prevención y recuperación.
- Ofrezca formación específica sobre los diferentes procedimientos de prevención y recuperación.
- Realice periódicamente simulacros para diferentes tipos de desastres con el fin de asegurar la capacitación del personal involucrado.
- Facilite el acceso permanente a toda la información necesaria, por ejemplo, a través de la Intranet o portal B2E de la empresa.

Control del proceso

La Gestión de la Continuidad del Servicio debe elaborar periódicamente informes sobre su gestión que incluyan información relevante para el resto de la organización TI.

Estos informes deben incluir:

- Análisis sobre nuevos riesgos y evaluación de su impacto.
- Evaluación de los simulacros de desastre realizados.
- Actividades de prevención y recuperación realizadas.
- Costes asociados a los planes de prevención y recuperación.
- Preparación y capacitación del personal TI respecto a los planes y procedimientos de prevención y recuperación [8].

Los pasos descritos anteriormente fueron tomados de ITIL Foundation, versión online [9].

III. IMPORTANCIA DE LA CONTINUIDAD DEL NEGOCIO DENTRO DE LAS ORGANIZACIONES.

Los negocios actualmente funcionan basados en la tecnología ante un incidente de unas pocas horas de duración puede tener un impacto muy fuerte para la organización y especialmente para su imagen en el mercado, el tener un programa de Continuidad del Negocio bien desarrollado ayuda a:

- La protección de vidas humanas
- Reducción de la confusión y toma de decisiones efectivas en los momentos de crisis
- Reducción de la dependencia de personal específico
- Reducción de la pérdida de datos, información y clientes
- Facilita la recuperación oportuna de los procesos críticos del negocio
- Mantiene la imagen pública y la reputación de la empresa.
- Disminuye las pérdidas económicas por interrupción prolongada de los procesos vitales

IV. CONCLUSIONES

- El saber planificar una gestión adecuada de los riesgos de TI no permite garantizar que ocurran sucesos que estén por fuera del alcance del plan de continuidad del negocio.

- El plan de continuidad del negocio hace parte de la gestión de riesgos permitiendo creación de estrategias para la continuidad de los servicios ofrecidos por la organización.

- El desarrollo de planes de continuidad debe estar basado y organizado utilizando alguna de las mejores prácticas de la industria como ISO 22301 o ITIL Foundation.

V. REFERENCIAS

[1] http://advisera.com/27001academy/es/que-es-iso-22301/
[2] Sharp J. The route map to Business Continuity Management – Meeting the requirements of BS 25999. British Standards Institution. 2008. Londres Reino Unido.
[3] Continuidad de negocios ISO 22301-2012
[4] Continuidad de negocios ISO 22301-2012
[5] Continuidad de negocios ISO 22301-2012
[6] Proceso gestión continuidad de negocios, ITIL Foundation, http://itilv3.osiatis.es/diseno_servicios_TI/gestion_continuidad_servicios_ti.php
[7] Evaluación de riesgos, ITIL Foundation, http://itilv3.osiatis.es/diseno_servicios_TI/gestion_continuidad_servicios_ti/evaluacion_riesgos.php.
[8] Continuidad de negocios, ITIL Foundation, http://itilv3.osiatis.es/diseno_servicios_TI/gestion_continuidad_servicios_ti.php.
[9] ITIL Foundation, version online, http://itilv3.osiatis.es/.