La seguridad informática en el contexto de los planes de continuidad del negocio

Amaya Guzmán, Eduardo Hernán
Universidad Piloto de Colombia
Bogotá, Colombia
ehag1986@gmail.com

Resumen: *la revisión pretende analizar la importancia que tiene dentro de los planes de continuidad del negocio la seguridad informática, que sin pretender ser su componente más importante, si busca demostrar que para que una empresa sobreviva a una contingencia, independiente de su severidad, la garantía de la salvaguarda de su información si es imprescindible en su futuro.*

Abstract: *This review pretends to analyze informatics security importance for business continuity plans, without trying to be the most important aspect, it attempts to demonstrate that if an enterprise is trying to survive a contingency, independently of it severity, the guaranty of safeguarding information is essential for its future.*

Índice de Términos: Gestión de riesgo, plan de continuidad del negocio, salvaguardas, seguridad de la información.

I. INTRODUCCIÓN

Quizá la tragedia del *World Trade Center* en *New York* el 11 de septiembre del 2011, es el mejor referente para que las organizaciones, independiente de su quehacer, implementen planes de continuidad del negocio como estrategia de gestión de riesgos. Este lamentable acontecimiento obligó a cambios en la percepción sobre la protección física, la seguridad informática, las tareas de las personas y las finanzas que debe manejar una empresa para gestionar este tipo de contingencias [1].

La identificación y valoración de acontecimientos que puedan detener el funcionamiento de una empresa, deben estar perfectamente identificados, si se presenta alguna eventualidad debe ser manejada sin demora (gestión de incidentes) y si se materializa un riesgo debe ser asumido, transferido o mitigado de manera inmediata (gestión de riesgos). La gestión de incidentes y de sus riesgos asociados, si es adecuada, evitara sean activados los planes de continuidad del negocio [2].

La continuidad del negocio debe tener en cuenta la valoración del riesgo tecnológico y su efecto sobre los activos informáticos, la valoración de riesgos físicos y su efecto en la producción o en el servicio, la valoración de las tareas desarrolladas por las personas y su redundancia para manejar procesos críticos y la planificación y reserva de los recursos para soportar de manera temporal el funcionamiento empresarial. Este análisis preventivo permitirá identificar los requerimientos mínimos para la continuidad del funcionamiento y el diseño de estrategias de operación y su proceso.

Sin embargo la encuesta sobre planes de continuidad del negocio realizada por AT&T muestra que cuatro (4) de cada diez (10) empresas no consideran como una prioridad la creación de planes de respuesta a incidentes que impidan el

desarrollo normal de operaciones. Del 100% de las empresas que enfrentan un desastre sin tener un plan de continuidad del negocio, el 43% nunca reabre sus puertas, el 51 % sobrevive pero están fuera del mercado por 2 años y solo el 6% logra sobrevivir sin mayores impactos [3].

Esta revisión pretende, dentro de este contexto, demostrar la importancia del manejo de las contingencias de la seguridad informática, como uno de los pilares fundamentales para la continuidad del negocio en todas las instancias que se analizan.

II. DESARROLLO DE CONTENIDOS

A continuación se da un vistazo a los conceptos teóricos y la significancia que para la organización y su supervivencia tienen los términos: plan de continuidad del negocio y sus elementos constitutivos, la seguridad informática y esta en el contexto de la sobrevivencia empresarial en caso de contingencias o desastres.

A. Planes de continuidad del negocio

Se debe entender un plan de continuidad del negocio como la capacidad estratégica, operativa y táctica de la organización para la planeación y respuesta a incidentes e interrupciones del negocio para continuar las operaciones a un nivel predefinido aceptable [4].

La gestión de la continuidad del negocio, hace parte de la gestión del riesgo operacional, es responsabilidad de la alta gerencia y se debe realizar para que la operatividad del negocio continúe de una manera razonable, con el fin de salvaguardar los intereses de sus principales grupos de interés, ante la ocurrencia de eventos que pueden crear una interrupción o inestabilidad en las operaciones de la empresa [5]. No debe ser sólo medidas reactivas sino que se requiere de un proceso de planeación exhaustivo y sistemático en el que se involucre el personal, la tecnología y por supuesto la infraestructura [6].

Como ya se mencionó, los planes de continuidad del negocio hacen parte fundamental de la estrategia organizacional específicamente en lo correspondiente al componente de gestión de riesgos, ya que no deja nada al azar ni a la improvisación. Además aumenta la posibilidad de supervivencia de la compañía [7]. Complementariamente prevé una reducción de costos asociados a la interrupción de actividades que conlleva a mayores gastos, pérdida de ingresos, pérdida de clientes; y si la empresa ejerce como proveedor de productos o servicios, la paralización de su actividad que podría redundar en penalizaciones contractuales.

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 [8] 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. Ver figura No 1

Asimismo John Sharp [8] presenta el alcance que debe ser considerado para implementar los

respuestas del plan de continuidad del negocio que se observa en la figura siguiente. Ver figura No 2.

Fig. 1 Incorporación de los planes de continuidad del negocio en la cultura de la organización [8].

Fig. 2 Alcance del plan de continuidad del negocio en la cultura de la organización [8].

Cuando se realiza un plan de continuidad del negocio se deben identificar los diversos eventos que podrían impactar sobre el futuro de las operaciones, conocer los tiempos de recuperación para volver a la situación anterior, prevenir y minimizar las pérdidas, priorizar los activos para su protección o recuperación, permitir una gestión adecuada de los recursos ante cualquier incidencia, mejorar la imagen y salvaguardar la confianza en la empresa para todos los grupos de intereses afectados, demostrando que existen medidas para garantizar la continuidad de las operaciones [7].

Los componentes de un plan de continuidad del negocio, según Macías, son [7]:

Tabla I
COMPONENTES DE UN PLAN DE CONTINUIDAD DEL NEGOCIO

■ Plan de gestión de la crisis
■ Plan de comunicación
■ Plan de gestión del personal
■ Plan de recuperación de infraestructuras
■ Plan de recuperación del negocio
■ Plan de recuperación de sistemas de información
■ Plan de mantenimiento

Fuente: adaptación con elementos de Macías en herramientas para la gerencia de riesgos y seguros [7].

Gaspar [9] experto en los planes de continuidad del negocio bancario, plantea la estrategia del "banco de tres patas" compuesto por un manual de procedimientos, unas instalaciones alternativas y un duplicado de la información y sistemas básicos de funcionamiento de las compañías en un lugar seguro.

Los objetivos de un plan de continuidad del negocio son [10]:

- Aumentar la probabilidad de continuidad de las funciones críticas de la organización en caso de que un incidente interrumpa las operaciones informáticas en las que se apoyan.
- Proporcionar un enfoque organizado y consolidado para dirigir actividades de respuesta y recuperación ante cualquier incidente o interrupción de trabajo imprevista, evitando confusión y reduciendo la situación de tensión.

- Proporcionar una respuesta rápida y apropiada a cualquier incidente imprevisto, reduciendo así los impactos resultantes de interrupciones a corto plazo.
- Recuperar las funciones críticas del negocio de manera oportuna, aumentando la capacidad de la organización para recuperarlas ante un incidente que haya dejado las instalaciones informáticas dañadas o destruidas.
- Aumentar la probabilidad de continuidad del servicio informático de la organización en caso de que un incidente interrumpa sus operaciones normales.
- Reducir el tiempo de recuperación y como consecuencia, pérdidas económicas directas e inducidas como resultado del desastre.
- Reducir el impacto, tangible o intangible, en las áreas funcionales como consecuencia de una interrupción del servicio informático.
- Realizar la recuperación de las funciones críticas, mediante el desarrollo de los procedimientos necesarios para: reducir la duración de la recuperación, minimizar el costo de la recuperación, evitar la confusión y reducir los riesgos de errores y evitar duplicación de esfuerzos.

B. Seguridad informática

La información, hoy en día, es uno de los activos más relevantes de las organizaciones y por tanto su protección se convierte en una labor primordial. La seguridad informática es la disciplina encargada de asegurar la integridad y privacidad de un sistema informático y el de sus usuarios [11]. El objetivo principal de la seguridad informática es proteger la confidencialidad, la integridad y la disponibilidad de la información:

- **Confidencialidad:** La información debe ser únicamente accesible para aquellos a los que está destinada.
- **Integridad:** La información no debe ser alterada durante la transmisión o en el propio equipo de origen.
- **Disponibilidad:** La información debe poder ser recuperada en el momento en el que se necesite, evitando su pérdida o bloqueo.

Por otra parte, según el informe "El estado de la seguridad de la información 2004" [12] elaborado por PriceWaterhouseCoopers a partir de 8.000 encuestas a responsables TIC de 62 países, la seguridad de la información es una preocupación creciente para las empresas porque afecta directamente a su reputación, su cuenta de beneficios y su desarrollo. Sin embargo, de todo el gasto en tecnologías de la información y la comunicación - TIC, sólo el 11,3% destina recursos a soluciones de seguridad.

Cada vez es mayor la necesidad de conocer y evaluar si el área de tecnologías de la información de la empresa está gestionando adecuadamente los riesgos y está alineada con los objetivos de la misma [7]. La dependencia actual de los sistemas informáticos hace que la gestión de los riesgos derivados sea estratégica, pero constituye un auténtico rompecabezas, por lo que se necesitará de un asesoramiento altamente especializado en áreas como: (Ver figura No 3)

- Análisis de riesgos estratégicos y de los procesos de negocio derivados de los sistemas de información.
- Auditoría informática de sistemas críticos soporte de los procesos de negocio.
- Aseguramiento de redes, sistemas y aplicaciones. *Hacking* ético.
- Adaptación y auditorías del reglamento de seguridad previsto por la ley.
- Auditoría de contratos de *outsourcing*.
- Adecuación del control interno de los sistemas de información a las legislaciones SOX404 y COBIT.
- Diseño, implantación, auditoría y testeo de planes de continuidad de negocio.
- Formación y concienciación.

Un sistema de gestión de la seguridad informática implica que la organización ha estudiado los riesgos a los que está sometida toda su información, ha evaluado qué nivel de riesgo asume, ha implantado controles (no sólo tecnológicos, sino también organizativos y legales) para aquellos riesgos que superan dicho nivel, ha documentado las políticas y procedimientos relacionados y ha entrado en un proceso continuo de revisión y mejora de todo el sistema. La estrategia da así la garantía a la empresa de que los riesgos que afectan a su información son conocidos y gestionados. No se debe olvidar, por tanto, que no hay seguridad total sino seguridad gestionada [11].

En líneas generales, implantar un sistema de seguridad informática comprende las siguientes actividades [13]: Ver figura No 4

1. Identificar los objetivos del negocio.
2. Obtener el patrocinio de la alta dirección.
3. Establecer el alcance (algunos procesos del negocio).
4. Realizar un diagnóstico (*Gap Analysis*).
5. Asignar recursos y capacitar al equipo.
6. Analizar los riesgos de activos de información.
7. Elaborar y ejecutar un plan de tratamiento de riesgos.
8. Establecer la normativa para controlar el riesgo.
9. Monitorizar la implantación del SGSI.
10. Prepararse para la auditoría de certificación.
11. Llevar a cabo auditorías internas periódicas.

Análisis de **riesgos estratégicos y de procesos del negocios** derivados de uso de **sistemas de información**	**Auditoria informática** y de sistemas críticos, soporte de los **procesos de negocio**	Securizacion de **redes, sistemas y aplicaciones** Hacking ético
Auditoria de contratos de outsourcing considerando aspectos legares y del cumplimiento de niveles de servicio, auditorias SAS 70	**Gobierno corporativo en el área de tecnologías de la información**	**Adaptación a la LOPD y realización de las auditorias del reglamento de seguridad** de acuerdo a lo previsto en la ley
Adecuación del control interno de los sistemas de información a la legislación **SOX404 y COBIT**	Diseño, implementación, auditoria y testeo de planes de **continuidad del negocio**	**Formación y concientización**, Seguridad lógica, Programas de ingeniería social cumplimiento LOPD

Fig.3 Planificación estratégica en el desarrollo, gestión y supervisión de los sistemas de información [7].

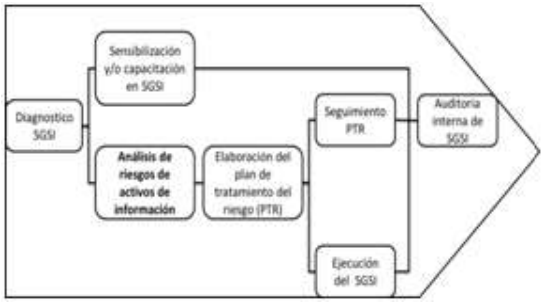

Fig.4 Modelo para implantar un sistema de seguridad de activos de información [13].

C. Acciones de seguridad informática para los planes de continuidad del negocio.

Sólo un 18% de los datos de los usuarios finales están protegidos y el 72% de las empresas se encuentran en alguna de estas tres situaciones [14]:

- No tienen un plan de continuidad de negocio.
- Si lo tienen nunca lo han probado.
- Su plan falló cuando lo probaron.

Lo que demuestra que asegurar el acceso a la información es mucho más que disponer de copias de seguridad, hay que garantizar la existencia de un plan que permita disponer de una infraestructura tal que haga viable el recuperar dicha copia de seguridad en las mismas condiciones que si no hubiera sucedido ningún desastre, garantizando la continuidad de los procesos de la compañía [14].

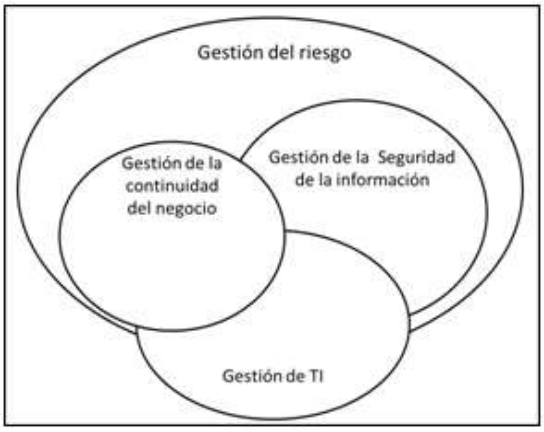

Fig. 5 Guía de desarrollo de un plan de continuidad del negocio para demostrar las relaciones en la gestion de riesgos empresariales [16].

La integración entre los sistemas de gestión de riesgo empresarial se muestra en la figura No 5 en donde se observa sistemas perteneciendo a otros sistemas [15].

En el desarrollo de un plan de continuidad de negocio, en lo referente a la seguridad informática, existen dos preguntas clave:

- ¿Cuáles son los **recursos de información** relacionados con los procesos críticos del negocio de la compañía?
- ¿Cuál es el período de **tiempo de recuperación crítico** para los recursos de información en el cual se debe establecer el procesamiento del negocio antes de que se experimenten pérdidas significativas o aceptables?

Asegurar una buena gestión de la seguridad de la información, toda empresa precisa de una política general de seguridad, que correctamente aplicada, debe concretarse en dos documentos esenciales: "**plan de continuidad del negocio"** y **"el plan de seguridad de la información"** que hace parte del anterior. Estos planes establecen cómo una organización debe recuperarse y restaurar sus funciones críticas que han sido parcial o totalmente interrumpidas después de una contingencia o desastre con énfasis especial en la seguridad de la información [13].

En este apartado debe recogerse el inventario de los recursos tecnológicos que soportan los procesos de la compañía, a fin de identificar aquellos que den soporte directo a los servicios críticos [16].

Según esta autora los tipos de recursos críticos que se deben analizar son:

- ***Hardware,*** identificando cada uno de los elementos *hardware* que soportan los sistemas de información de la compañía.
- ***Software*** base**,** recogiendo todos aquellos componentes de *softwar*e, incluido todos los

asociados al sistema operativo, indispensables para el funcionamiento y optimización del sistema de información de la compañía.

- ***Software* de aplicaciones,** inventariando las aplicaciones de gestión que son utilizadas en la empresa.
- **Sistemas de infraestructura,** considerando aquellos elementos o componentes que sin disponer de una tecnología enfocada propiamente al tratamiento de la información sí son requeridos para garantizan la operatividad del servicio**.**

De gran importancia en esta relación de los planes de continuidad del negocio y la seguridad informática es el gobierno de seguridad de la información que consiste en el liderazgo, estructura organizacional y el proceso para proteger la información. El gobierno de seguridad de la información es un subconjunto del gobierno corporativo de la organización que provee dirección estratégica, garantiza los objetivos establecidos, gestiona los riesgos de forma apropiada, usa los recursos organizacionales responsablemente y monitorea el éxito o falla del programa de seguridad de la organización [17].

III. CONCLUSIONES

1. Si bien gestionar los riesgos empresariales no es garantía de control para todas las eventualidades que puedan suceder, si permite prevenir muchos acontecimientos que podrían poner en riesgo la continuidad del negocio.
2. El plan de continuidad del negocio es una estrategia de gestión de riesgos que permite la prevención de contingencias y la provisión de estrategias y recursos que permitan la sobrevivencia de la empresa.
3. La seguridad informática, que hace parte fundamental de los planes de continuidad del negocio, es un componente fundamental para que el negocio rápidamente pueda renacer ya que restituye quizá el activo más valioso de las empresas.
4. Implementar la cultura de la previsión, de la prevención y del riesgo, no es una tarea fácil en las empresas, puesto que requiere inversiones de dinero importantes y dadas las crisis y contingencias del mercado muchos gestores las consideran poco costo-efectivas.

IV. REFERENCIAS

[1] Thibodeau P. Computerworld: como cambio el 11 de septiembre a los centros de datos. Computerworld. 2011 Septiembre; http://www.computerworldmexico.mx/articulos/18239.htm?goback=.gde_128300_member_162326734.

[2] Ramírez A, Gestión de riesgos tecnológicos basada en ISO 31000. e ISO 27005 y su aporte a la continuidad de negocios. Ingeniería, Vol. 16, No. 2, pág. 56-66.; Vol. 16(No 2 pág. 56-66.).

[3] Beltran S. Consideraciones de diseño de planes de continuidad de la operación en redes de telecomunicaciones IPN MIT. 2010.

[4] International Organization for Standardization ―2, inventor;

International organization for standardization, ―ISO/IEC 27001, Information Technology–Security Techniques-Information Security Management Systems.. 2007 Suiza.

[5] Superintendencia de banca SyAdFdP. Superintendencia de Banca, Seguros y asociación Circular Nº G-139-2009 gestión de la continuidad del negocio. Lima. Perú; 2009.

[6] Institution BS. Guide to business continuity management. Londres, Reino Unido:; 2003.

[7] Macias M. Herramiantas para la gerencia de riesgos y seguros. Rev Riesgos y Seguros Nº 107—2010.

[8] Sharp J. The route map to Business Continuity Management – Meeting the requirements of BS 25999. British Standards Institution. 2008. Londres Rei no Unido.

[9] Gaspar J. Un banco de tres patas. Bolsa actualidad. 2008.

[10] Gaspar J. El plan de continuidad del negocio - Guía práctica para su elaboración Barcelona: Diaz de Santos; 2006.

[11] Deloitte & Touche, S.A. Riesgos de tecnología de información, retos para la auditoría. ; 2003.

[12] PriceWaterhouseCoopers. El estado de la seguridad de la información. ; 2004.

[13] Sotelo M, Torres JRJ. Un proceso practico de analisis de riesgos de activos de información. Universidad Nacional Mayor de San Marcos. 2010.

[14] Balleste M. www.firstconference.org. [Online].; 2013 cited 2914 Noviembre 21.

[15] Kosutic D. Conceptos báshttp://www.iso27001standard.com/index.php?option=com_content&view=article&id=421:sto-je-iso-22301&catid=9. [Online].; Conceptos básicos sobre ISO 22301 cited 2014.

[16] del Pino l. Guía de desarrollo de un palan de continuidad del negocio. Universidad Politécnica de Madrid, Tesis de Magister; 2007.

[17] ISACA. Guidance for Boards of Directors and Executive Management. ; 2010.