CONTINUIDAD DEL NEGOCIO: LA CLAVE DEL ÉXITO.

Jaimes Arroyo, Jorge Arley
jorgeajarroyo@hotmail.com
Universidad Piloto de Colombia
Bogotá, Colombia

Resumen: *Lo que se pretende con esta revisión es demostrar la importancia que tiene el concepto, la aplicación y el mejoramiento del proceso de continuidad del negocio en una empresa, así como ser una parte fundamental en la implementación de un sistema de seguridad informática.*

Abstract: *The aim of this review is to demonstrate the importance of the concept, implementation and improvement of the process of business continuity in a company as well as being a fundamental part in implementing a security system.*

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

I. INTRODUCCIÓN

Con la evolución de la tecnología, la aparición de los dispositivos inteligentes y aplicaciones móviles, se ha creado una dependencia de las personas hacia la tecnología, "La gente se mantiene conectada sin cesar, en todas partes y en todas las posiciones, en la cama, en los restaurantes o en las salas de espera", señala Remy Oudghiri, director del instituto francés de encuestas Ipsos y autor de un libro sobre la e-dependencia [1].

Toda esta dependencia no solo es a nivel de redes sociales, chats y/o portales de noticias, también la comodidad de realizar transacciones electrónicas (compra, ventas e intercambios) se ha masificado a tal punto que la mayoría de empresas financieras, comercializadoras de servicios e incluso entidades gubernamentales ofrecen la posibilidad de realizar pagos, solicitar y enviar documentos evitando al usuario desplazarse hacia las sucursales a realizar largas y tediosas colas para cumplir con sus obligaciones.

La virtualización de las compañías, ha creado la necesidad que implementar un ambiente seguro, confiable e integral en el cual los usuarios se sientan cómodos al momento de realizar cualquier tipo de transacción electrónica. Las políticas de seguridad hoy en día, es un requisito legal para cualquier entidad que registre datos personales en sus bases de datos para asegurar que el tratamiento que se le está dando a esta información es el adecuado y evitar posibles fraudes, todo esto permite proyectar a la empresa hacia la continuidad del negocio.

La continuidad del negocio, está respaldada por otros elementos de la seguridad informática como la gestión de incidentes, mejora continua; teniendo en cuenta estos conceptos, se va a desarrollar una base teórica de estos elementos y así entender más a fondo su rol en un sistema de seguridad.

II. DESARROLLO DE CONTENIDOS

Como se dijo anteriormente, se va a desarrollar una serie de conceptos necesarios para comprender su función dentro de un sistema de seguridad de la información y su aporte a la continuidad del negocio.

A. Incidentes de seguridad

Un incidente se conoce como el evento no esperado, planeado que puede causar daño, inestabilidad a algo, pero si nos vamos más puntualmente hacia la seguridad informática tenemos, que un incidente es un evento adverso sistema de computadoras o de red de computadoras, que compromete la confidencialidad, integridad, disponibilidad, legalidad o confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento, amenaza de romper los mecanismos de seguridad existentes [2].

Como todo evento inesperado se debe tener métodos, procesos, políticas, contingencias para tratarlos y así evitar un riesgo mayor; la gestión de incidentes tiene como primer objetivo recuperar el servicio afectado a mayor nivel, minimizar en todo impacto negativo en la organización, todo incidente debe ser solucionado rápida y eficientemente de tal manera que no se afecte la continuidad del negocio.

Como todo proceso la gestión de incidentes tiene sus etapas bien definidas, ver Figura No. 1 [3]. Estas deben ser evaluadas, monitoreadas y mejoradas ante la aparición de nuevos eventos.

Fig. 1 Alcance del plan de continuidad del negocio en la cultura de la organización [3].

Durante la buena ejecución de cada una de las etapas se puede asegurar grandes beneficios para la empresa:

Mejorar la productividad de los usuarios, cumplir con los niveles de servicio acordados en el acuerdo de nivel de servicio, mayor control de los procesos y monitorización del servicio, optimización de los recursos disponibles, y principalmente: mejora la satisfacción general de clientes y usuarios [4].

B. Planes de continuidad del negocio

El Plan de Continuidad del Negocio busca amortiguar en lo posible este riesgo mediante un plan global que permita la pronta recuperación de la operación y de la información, en caso de presentarse algún evento que afecte el flujo normal de las actividades de una organización [5].

Principales objetivos del plan de continuidad [6]:

-Mantenerse en el negocio.

-Proteger la salud de los trabajadores y sus familias.

-Promover la adherencia de los empleados a las recomendaciones de las autoridades durante el período de pandemia.

Un plan de continuidad se compone de varias fases que comienzan con un análisis de los procesos que componen la organización.

Por cada proceso se identifican los impactos potenciales que amenazan la organización, estableciendo un plan que permita continuar con la actividad empresarial en caso de una interrupción.

Beneficios de contar con un plan de continuidad:

-Identifica los diversos eventos que podrían impactar sobre la continuidad de las operaciones y su impacto sobre el negocio.

-Obliga a conocer los tiempos críticos de recuperación para volver a la situación anterior al desastre sin comprometer al negocio.

-Previene o minimiza las pérdidas para el negocio en caso de desastre.

-Clasifica los activos para priorizar su protección en caso de desastre. Aporta una ventaja competitiva frente a la competencia.

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.

Como los planes de contingencias evolucionan junto con la tecnología y su entorno existe el estándar BS 25999-1 que presenta los procesos y principios necesarios para una adecuada gestión de la continuidad del negocio que permita cubrir las necesidades de clientes y organizaciones. La gestión de la continuidad del negocio (Business Continuity Management – BCM) consiste en la mejora proactiva de la resistencia (resilience) de la organización frente a contingencias.

Por otra parte, proporciona mecanismos para restaurar los productos y servicios clave a un nivel aceptable y dentro de un marco temporal limitado, protegiendo la reputación corporativa. El ciclo de vida de la gestión de la continuidad consta de 5 etapas, ver figura No 2. [7].

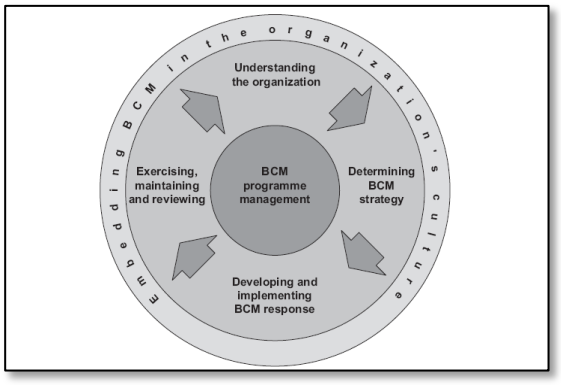

Fig. 2. Incorporación de los planes de continuidad del negocio en la cultura de la organización [7].

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].

C. Informática forense

Junto al modelo de continuidad del negocio y su mejoramiento constante, se debe tener en cuenta la informática forense, que determina las posibles causas, brechas y fallos del sistema de seguridad implementado después que se presenta un incidente de seguridad. Mediante sus procedimientos se identifican, aseguran, extraen, analizan y presentan pruebas generadas y guardadas electrónicamente para que puedan ser aceptadas en un proceso legal.

Las distintas metodologías forenses incluyen la captura segura de datos de diferentes medios digitales y evidencias digitales, sin alterar la información de origen. Gracias a este proceso, la informática forense aparece como una "disciplina auxiliar" de la justicia moderna, para enfrentar los desafíos y técnicas de los intrusos informáticos, así como garante de la verdad utilizando la "evidencia digital"[8].

De acuerdo con el HB: 171 2003 Guidelines for the Management of IT Evidence, la evidencia digital es: "cualquier información, que sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático". En este sentido, la evidencia digital, es un término utilizado de manera amplia para describir "cualquier registro generado por o almacenado en un sistema computacional que puede ser utilizado como evidencia en un proceso legal". La evidencia digital posee, entre otros, los siguientes elementos que la hacen un constante desafío para aquellos que la identifican y analizan en la búsqueda de la verdad [9]:

1. Es volátil
2. Es anónima
3. Es duplicable
4. Es alterable y modificable
5. Es eliminable

Estas características nos advierten sobre la exigente labor que se requiere por parte de los especialistas en temas de informática forense, tanto en procedimientos, como en técnicas y herramientas tecnológicas para obtener, custodiar, revisar, analizar y presentar la evidencia presente en una escena del delito.

Un concepto a tener en cuenta es la cadena de custodia, donde se establecen las responsabilidades y controles de cada una de las personas que manipulen la evidencia, se deberá registrar los datos personales de todos los implicados en el proceso de manipulación de las copias [10]:

- Dónde, cuándo y quién manejo o examinó la evidencia, incluyendo su nombre, su cargo, número de identificación, fechas y horas, etc.

- Quién estuvo custodiando la evidencia, durante cuánto tiempo y dónde se almacenó.

- Cuando se cambie la custodia de la evidencia también deberá documentarse cuándo y cómo se produjo la transferencia y quién la transportó.

Esta cadena de custodia se presenta en toda la metodología de la informática forense, esta se puede ver en la figura No. 3

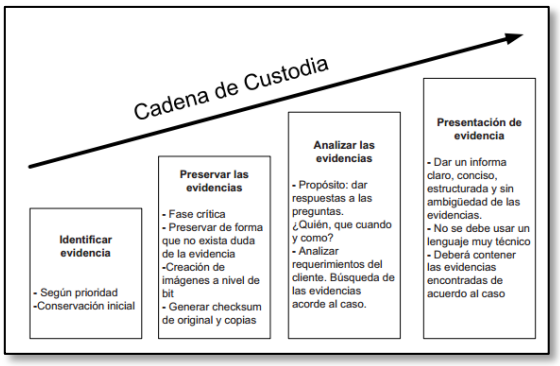

Fig. 3. Metodología de la informática forense [10].

Existen varios usos de la informática forense, muchos de estos usos provienen de la vida diaria, y no tienen que estar directamente relacionados con la informática forense [11]:

Prosecución Criminal: Evidencia incriminatoria puede ser usada para procesar una variedad de crímenes, incluyendo homicidios, fraude financiero, tráfico y venta de drogas, evasión de impuestos o pornografía infantil.

- Litigación Civil: Casos que tratan con fraude, discriminación, acoso, divorcio, pueden ser ayudados por la informática forense.

- Investigación de Seguros: La evidencia encontrada en computadores, puede ayudar a las compañías de seguros a disminuir los costos de los reclamos por accidentes y compensaciones.

- Temas corporativos: Puede ser recolectada información en casos que tratan sobre acoso sexual, robo, mal uso o apropiación de información confidencial o propietaria, o aún de espionaje industrial.

- Mantenimiento de la ley: La informática forense puede ser usada en la búsqueda inicial de órdenes judiciales, así como en la búsqueda de información una vez se tiene la orden judicial para hacer la búsqueda exhaustiva.

Algunos hechos destacados de realizar un análisis forense son [12]:

- Se considera que el 75% de los delitos relacionados con sistemas informáticos se producen desde dentro de una organización (hacker dentro del muro de fuego).

- Durante 1999 el 93% de la información se generó en forma electrónica (fuente: IDC).

La computación forense tiene aplicación en un amplio rango de crímenes incluido pero no limitado a: mal uso de la computadora que conlleve a pérdida de productividad de empleados (uso personal de correo electrónico, uso de internet para actividades personales o entretenimiento). Robo de secretos comerciales e industriales, robo o destrucción de propiedad intelectual, destrucción de archivos judiciales, de auditoría, etc.

La evidencia informática es frágil por definición y puede fácilmente ser alterada o modificada y así perder autenticidad frente a una corte. Se deben

por lo tanto establecer rígidas normas de preservación y cadena de custodia de la misma.

Como complemento de todo lo dicho anteriormente se debe tener en cuenta, la importancia de la seguridad informática en la continuidad del negocio, esta radica en asegurar el acceso a la información pero esto 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.

La continuidad del Negocio en muchas ocasiones viene provocada por factores externos a la propia compañía, desastres naturales o provocados por el hombre, incendios, terremotos, huracanes, etc., sobre los cuales la empresa no puede actuar pero si puede de alguna manera, planificar cómo reaccionar ante estas situaciones adversas para poder continuar ofreciendo a sus clientes el servicio comprometido [13].

III. CONCLUSIONES

- El plan de continuidad del negocio permite mantener a través de diferentes estrategias los niveles y la calidad del servicio que se ofrece evitando que se tengan pérdidas de dinero, imagen y usuarios.
- Con el estándar BS 25999-1 se puede tener una guía muy completa para realizar un buen proceso de implementación y ejecución de continuidad del negocio, basado en buenas practicas, principios y procedimientos.
- La informática forense permite obtener hallazgos de los incidentes presentados en la empresa que ayudan a complementar, cambiar y mejorar los procesos implementados para asegurar la continuidad del negocio, y también para evitar futuros incidentes críticos.

- La continuidad del negocio se basa en la preservación de los principios básicos de la seguridad informática que son: disponibilidad, confiabilidad e integridad de la información.

IV. REFERENCIAS

[1] AFP: Dependencia a las nuevas tecnologías. una enfermedad que puede curarse; http://www.eltiempo.com/archivo/documento/CMS-12898544.

[2] Unidistrital:Seguridad de la informacion.https://portalws.udistrital.edu.co/CIT/documentos/NORMATIVIDAD/politica_seguridad/archivos/Politica_para_Seguridad_Informacion_Version_0.0.1.0.pdf

[3] Ing. Joaquín Louzao ,Gerardo Geis, Gabriel Silva. Gestión de Incidentes - Análisis Forense. ftp://public.dhe.ibm.com/la/documents/imc/la/uy/news/events/networking12/files/15_IBM_-_Gestion_de_Incidentes_ _Analisis_Forense_-_Joaquin_Louzao_Gerardo_Geis_Gabriel_Si

lva.pdf

[4] OSIATIS S.A.ITIL.Gestión de Servicios TI. http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_incidentes/introduccion_objetivos_gestion_de_incidentes/introduccion_objetivos_gestion_de_incidentes.php

[5] Colegio de Contadores Públicos de México A.C. La importancia de implementar un Plan de Continuidad de Negocios (1ra parte); http://www.dineroenimagen.com/2013-07-01/22403

[6] Soyenterpreneur.com.que es un plan de continuidad del negocio? www.soyentrepreneur.com/que-es-un-plan-de-continuidad-de-negocio.html

[7] Sergi Blanco-Cuaresma. BS 25999-1: Gestión de la Continuidad del Negocio.www.marblestation.com/?p=650.

[8] Altonivel. ¿Qué es la Informática Forense? http://www.altonivel.com.mx/7102-que-es-la-informatica-forense.html

[9] Jeimy J. Cano, Ph.D, CFE Introducción a la informática forense. http://www.acis.org.co/fileadmin/Revista_96/dos.pdf

[10] Universidad Politecnica Salesiana Ecuador. dspace.ups.edu.ec/bitstream/123456789/546/4/CAPITULO3.pdf

[11] Giovanni Zuccardi, Juan David Gutiérrez. Informática Forense. http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf

[12] Marcos.Informatica Forense. http://sinsaju.blogspot.com/

[13] Consillium's webblog. Más allá de la Seguridad Informática. Los Planes de Continuidad de Negocio. https://consiliumblog.wordpress.com/2009/01/26/mas-alla-de-la-seguridad-informatica-los-planes-de-continuidad-de-negocio/