Resiliencia estrategia de recuperación

Muñoz, Victoria.
vmpgari@hotmail.com
Universidad Piloto de Colombia

Resumen— La resiliencia en Seguridad Informática podría llegar a considerarse como el indicador más veraz y crudo del Plan de Continuidad del Negocio con que cuenta una organización, para poder recuperarse a situaciones reales de disrupción o desastre, obligando a retomar las operaciones lo más cercano a la normalidad de sus procesos, en un tiempo estimado.

La disrupción y/o el desastre evidencia la ruptura del orden establecido por la organización. La resiliencia permite recuperarse con base en el plan de continuidad definido y adicionalmente adaptarse a los cambios tecnológicos.

La propuesta que se presenta en este documento es seguir los modelos de resiliencia empresarial, adoptarlos y ajustarlos como apoyo estratégico en el plan de recuperación de la organización, desde T.I.

Abstract- The resilience in IT Security could come to be considered as the most truthful and crude indicator of the Business Continuity Plan that an organization has, to be able to recover to real situations of disruption or disaster, forcing them to resume operations as close to the normal of their processes, in an estimated time. Disruption and/or disaster show the breakdown of the order established by the organization. Resilience allows recovery based on the defined continuity plan and additionally adapts to technological changes. The proposal presented in this document is to follow, adopt and adjust business resilience models as strategic support in the organization's recovery plan.

Índice de Términos— Normas, estándares, resiliencia, disrupción, procesos, seguridad, desastre.

Index Terms—Attacks, Normas, estándares, resiliencia, disrupción, procesos, seguridad, disaster.

I. INTRODUCCIÓN

En Colombia la percepción de resiliencia se encuentra en un estado bajo de madurez. Habitualmente las organizaciones desestiman los riesgos o los mitigan de acuerdo al presupuesto designado y en la mayoría de los casos se implementan planes de continuidad del negocio porque la normatividad así lo obliga, pero sin la convicción de lo que representa ser resiliente; es decir, que ante una serie de sucesos que afecten su operación normal, la prestación de servicios y la confianza que genere en sus clientes; la organización esté preparada para reaccionar, recuperarse, buscando la estabilidad, hasta la normalidad de sus procesos para continuar operando.

Las organizaciones usualmente se centran en considerar enfoques para las consecuencias inmediatas de un incidente, pero esto podría variar si se conocieran los modelos de resiliencia existentes y que han tenido éxito en su aplicación.

Es por esto que se plantea la idea de tomar como marco de referencia el método de resiliencia empresarial y homologarlo como método aplicable en los procesos de recuperación del plan de continuidad del negocio, en las T.I.

Al tomar como marco de referencia las características más significativas de las compañías con alta resiliencia empresarial y se aplicara de manera análoga a la resiliencia en el plan de continuidad de negocio desde la T.I., donde además se apartara esa visión obtusa de cualquier medida que deba tomarse, sea calculada únicamente desde lo económico, lo obligatorio por la norma, el costo de la inversión…; abriría la posibilidad de que la organización se comprometa y se proyecte desde la profundidad que sienten las partes interesadas, donde finalmente se refleje entre otras en la reputación de la organización.

Adicionalmente con el compromiso de la alta gerencia, se establecerían políticas basadas en este tipo de ideas, que en consecuencia facilitaría conocer y gestionar los riesgos desde la metodología empresarial; ya con esta información sería posible estimar los costos e incluso con un estudio detallado podría pensarse en la posibilidad de formular y aplicar modelos matemáticos que permitiera, precisar los esfuerzos en cada uno de los recursos de T.I. , prever y aumentar la probabilidad de recuperación de los activos de información, disminuyendo el tiempo para

la normalización de las operaciones, donde T.I, seria factor determinante en la recuperación de la organización, que a su vez permita disminuir el impacto económico y reputacional de la empresa.

De acuerdo a la guía del texto de PwC: "el marco de resiliencia organizacional engloba todos mecanismos administrativos y gerenciales, que permiten a las organizaciones diseñar e implementar de una forma ordenada, metodológica y adaptada a su realidad, los sistemas de reacción y de protección necesarios"

II. Encuesta sobre Resiliencia Organizacional y Gestión de Riesgos

El documento guía indica el inicio de la metodología desde la encuesta que permita identificar el nivel de madurez de resiliencia y de la gestión de riesgos de una organización.

Muchas organizaciones cuentan ya con un sistema de gestión de riesgos, por lo que la adaptación al nuevo marco de administración generalmente va a partir desde la identificación de aquellas diferencias que tiene la administración actual con respecto al nuevo marco.

Para el propósito del estudio, que tiene como finalidad identificar el nivel de madurez actual en materia de Resiliencia Organizacional y Gestión de Riesgos, se realizó la medición de las fases del proceso de resiliencia establecido por el estándar BS 65000 (conciencia situacional, fijar dirección, brindar coherencia, desarrollar capacidad adaptativa, fortalecer la organización, validar y revisar), y de los 5 componentes definidos por el marco de Gestión de Riesgo Organizacional COSO 2017 (gobierno y cultura, establecimiento de estrategia y objetivos, ejecución, revisión y actualización e información, comunicación y reporte).

Se ha definido una escala de 4 niveles para identificar la madurez del modelo de resiliencia de las organizaciones según aspectos como: formalidad, involucramiento de su personal, grado cultural establecido, y otros aspectos que permiten la efectiva implementación y operación de estos dos importantísimos marcos en las organizaciones modernas.

MEDICIÓN DE LAS FASES DEL PROCESO:

Con el propósito de entender los criterios que permite identificar el nivel de madurez de resiliencia y de la gestión de riesgos de una organización, se describe brevemente las fortalezas de los estándares, que se toman como marco de referencia, para el desarrollo de la medición de las fases del proceso de resiliencia establecido en cada uno de ellos.

BS 65000: Guía para la Resiliencia Organizacional.:

BSI ha publicado la norma **BS 65000**, que pretende ser una Guía para la Resiliencia Organizacional. Esta nueva norma proporciona una visión general de la capacidad de recuperación de una organización, para ello, describe los fundamentos necesarios y explica cómo implementar gradualmente la resiliencia en una organización.

BS 65000 proporciona directrices para lograr una mayor capacidad de adaptación organizativa junto con los beneficios que esto conlleva. También pretende mejorar los sistemas para la gestión de una crisis, así como las prácticas de gestión de la continuidad del negocio mediante la integración de éstos en un programa más amplio denominado "Programa sobre la capacidad de recuperación". Además, **BS 65000** hace referencias a otras actividades como la gestión de riesgos, el denominado "horizon scanning" (Estudios de proyección económica y gestión del cambio.

Algunos de los objetivos y aspectos fundamentales de esta norma **BS 65000** son:

- Permitir la gestión de nivel superior para dibujar una estrategia de resiliencia organizacional que identifique los beneficios y los comportamientos de los organismos resistentes;
- Ofrecer herramientas básicas para la evaluación de las medidas de resiliencia de una organización;
- Contiene un modelo de madurez para la evaluación del desempeño;
- Incluye un test que las organizaciones pueden utilizar para evaluar sus medidas de resiliencia.[i]

- **ISO 22316: 2017 Seguridad y resiliencia - Resiliencia organizacional - Principios y atributos**

La nueva **ISO 22316** proporciona orientación para mejorar la capacidad de recuperación de una empresa. Lo

que hace que mediante principios proporcione atributos y actividades que contribuyen a las empresas más resistentes. Este estándar no puede ser utilizado para certificar una organización. Más bien sirve como un paraguas que cubre una amplia gama de disciplinas de gestión, todos deben ser los suficientemente maduro y capaz de interactuar entre sí de una forma sinérgica.

Dos de estas disciplinas de Gestión de Seguridad de la Información **ISO 27001** y la continuidad de negocio según la norma **ISO 22301**. Estas normas de gestión sirven para aplicar correctamente el enfoque respectivo, y las empresas pueden obtener la certificación de estas dos normas. Resiliencia organizacional amplía el concepto de preparación de las amenazas que podrían desarrollarse lentamente, pero todavía serían fatales para la empresa si no se anticipa de forma correcta. Las normas mencionadas ocupan eventos repentinos, enfoques de resiliencia, política, demográfica, etc.

ISO 22316: 2017 proporciona orientación para mejorar la capacidad de recuperación de la organización para cualquier tamaño o tipo de organización. No es específico de ninguna industria o sector. **ISO 22316: 2017** se puede aplicar a lo largo de la vida de una organización.

ISO 22316: 2017 no promueve la uniformidad en el enfoque en todas las organizaciones, ya que los objetivos específicos y las iniciativas se adaptan a las necesidades de cada organización.

ENFOQUE ESTRUCTURADO

Uno de los grandes valores de **la norma ISO 22316** se basa en el hecho que propone un enfoque estructurado para la capacidad de recuperación. Mientras que las empresas pueden tener más o menos éxito en el camino a la resiliencia.

- **ISO 22301 CONTINUIDAD DEL NEGOCIO**

Desde una perspectiva histórica reciente la norma **ISO 22301** ha sido una conclusión de los esfuerzos del ámbito empresarial internacional por obtener un estándar que ayude a gestionar la Continuidad de un negocio y/o actividades de una organización. Como precedente a este estándar se encuentra con la norma Británica **BS 259999** que actuó como base e impulsora de la actual **ISO 22301** Gestión de la Continuidad del Negocio publicada por la Organización Internacional de estandarización ISO

Las claves para entender la norma **ISO 22301** pasan entender que se trata de:

- Establecer una base común de conocimiento para entender la continuidad del Negocio
- Desarrollar e implantar una política de Continuidad del Negocio en una organización
- Acreditar la conformidad y compromiso de una organización con las mejores prácticas internacionales en Continuidad del Negocio.

EL principal objetivo de esta norma es mantener la continuidad de las actividades de una organización, proteger sus intereses defendiendo los intereses de sus empleados y partes interesadas, mantener la reputación su reputación ante cualquier amenaza o circunstancia adversa. Los principales factores que afectan a la continuidad de negocio son:

- Dependencia creciente de la tecnología.
- Interdependencia de los proveedores.
- Un acto individual puede tener consecuencias planetarias.
- La competencia (feroz) no perdona interrupciones prolongadas o, simplemente, apreciables por los usuarios.
- Cualquier obligación legal o regulación sectorial.

Algunos de los impactos posibles son:

- Pérdida de productividad
- Pérdida de ingresos directa
- Incremento de los costes de proceso
- Incremento en las reclamaciones de clientes
- Retraso en el suministro de productos/servicios
- Daño a la marca y la reputación
- Multas o penalizaciones
- Caída de valor de las acciones

- **COSO (2017)**

El Comité de Organizaciones Patrocinadoras de la Comisión Treadway (The Committee of Sponsoring Organizations of the Treadway Commission (COSO) se ha encargado de publicar el Marco Integrado para la **Administración de Riesgos Empresariales (ERM) COSO ERM 2017** como una actualización de su programa anterior (2004), con la intención de brindar a las empresas un sistema centrado en la Auditoría Interna, que permite identificar, evaluar y manejar los riesgos de la actividad empresarial.

El marco ERM permite darle un manejo adecuado al riesgo, de tal manera que la empresa pueda tomar las decisiones más acertadas para su desarrollo y el cumplimiento de sus metas y objetivos.

La administración del riesgo es un elemento clave en la supervivencia de las empresas en el contexto empresarial moderno. Al hablarse de un contexto nuevo que impone a su vez nuevos elementos asociados al riesgo, es necesario hacer una aproximación a la evolución que han tenido los conceptos y las aplicaciones de la gestión de riesgos empresariales. Una vez se ha establecido este marco conceptual y metodológico actualizado, se procede a la segunda parte, que es el Marco en sí. El Marco ERM está organizado en cinco componentes fáciles que se acomodan a las estructuras operativas y que permiten abordar nuevas estrategias y tomar mejores decisiones relacionadas a la gestión del riesgo.

COSO (2017) establece que la nueva actualización, a diferencia de la versión pasada (2004), presenta las siguientes fortalezas: **Primero**, proporciona una comprensión más amplia y clara de lo que significa la gestión del riesgo y su papel clave en la implementación de estrategias. **Segundo**, permite establecer objetivos de rendimiento basados en la alineación entre el rendimiento y la gestión del riesgo empresarial para el beneficio de la empresa. **Tercero**, da pautas relacionadas con la gobernanza y la supervisión aplicables para cualquier empresa. **Cuarto**, hace un reconocimiento del nuevo contexto planteado por la globalización de la economía y la necesidad de adaptación a los mismos.

Quinto, se presentan nuevas perspectivas para entender y analizar el riesgo como la manera más efectiva de adaptarse a la complejidad del mundo de los negocios. **Sexto**, es una fuente suficiente y completa para responder a las expectativas de los administradores y todos los interesados en ampliar su entendimiento sobre la gestión de riesgos. **Séptimo**, es compatible con la evolución y el uso de las TIC, así como su aplicabilidad en el manejo de datos y en la toma de decisiones. Y **Octavo**, establece definiciones básicas y principios que deben tenerse en cuenta en todos los niveles de gestión del riesgo y así poder establecer estrategias más acertadas.

- **ESCALA DE NIVEL DE MADUREZ**

Con la aplicación de las metodologías propias de la empresa **PWC** tomada -como modelo- y de las propuestas por **BS 65000** (conciencia situacional, fijar dirección, brindar coherencia, desarrollar capacidad adaptativa, fortalecer la organización, validar y revisar), y de los 5 componentes definidos por el marco de Gestión de Riesgo Organizacional **COSO 2017** (gobierno y cultura, establecimiento de estrategia y objetivos, ejecución, revisión y actualización e información, comunicación y reporte), se establece la escala de nivel de madurez del modelo de resiliencia de las organizaciones según aspectos como: formalidad, involucramiento de su personal, grado cultural establecido, y otros aspectos que permiten la efectiva implementación y operación de estas dos importantísimos marcos en las organizaciones modernas.

III. RESILIENCIA ORGANIZACIONAL Y GESTIÓN DE RIESGOS

Tal como se presentó esta propuesta y con base en las experiencias y resultados obtenidos en el desarrollo y aplicación de esta metodología; que inicia con la encuesta que determina el nivel de madurez del modelo de resiliencia, Este nuevo marco cuenta con una serie de novedades orientadas a engranar la gestión de riesgos desde la estrategia hasta la operación, y además a hacer una implementación y gestión más adaptada a la realidad de la organización mediante la aplicación de una estructura de componentes y principios.

Muchas organizaciones cuentan ya con un sistema de gestión de riesgos, por lo que la adaptación a este nuevo marco de administración generalmente va a partir desde la identificación de aquellas diferencias que tiene la administración actual con respecto al nuevo marco; el propósito es seguir éstos modelos de resiliencia

empresarial, adoptarlos y ajustarlos como apoyo estratégico en el plan de recuperación de la organización, desde T.I., teniendo en cuenta que el mayor activo de una empresa es la información y la tecnología que se utiliza para registrar, modificar, actualizar, archivar, datos relevantes y críticos que representa muchas veces el core de la empresa.

Partiendo desde este punto, acorde a la metodología propuesta, una vez encontrado el nivel de madurez del modelo de resiliencia desde las T.I., se continúe con determinar las diferencias que se presenta entre la administración y gestión actual versus el nuevo marco; de esta manera se podrá definir las actividades orientadas a la adaptación del modelo de resiliencia para T.I.

Tomando como marco de referencia, el documento donde El British Standard Institution publica su marco metodológico en Resiliencia Organizacional **BS 65000**, que proporciona una guía para lograr una mayor resiliencia organizacional, los beneficios de hacerlo, e integra las prácticas de administración de crisis y gestión de la continuidad del negocio, y otras como la gestión de riesgos y la gestión de cambios, pero limitándola a las áreas de T.I.**,** se podrá hacer seguimiento y monitoreo en construir resiliencia ante las nuevas realidades y tendencias globales, como avances tecnológicos, cambios demográficos, cambios climáticos, cambios en el poder económico y la urbanización acelerada a nivel global, resulta fundamental para las organizaciones, las cuales deben trabajar en el fortalecimiento de sus atributos para abordar las diversas situaciones y salir victoriosas.

En 2017, el International Organization for Standardization (ISO) publicó el estándar **ISO 22316:2017** sobre Seguridad y Resiliencia Organizacional, que incluye los principios base para mejorar la capacidad de recuperación de una organización con base en unos atributos, así como las actividades que orientan a su utilización, evaluación y mejora.

- **RESILIENCIA ORGANIZACIONAL Y GESTION DE RIESGOS.**

En septiembre de 2017, COSO publica la versión actualizada del Marco de Gestión de Riesgo Organizacional, definiéndola como "la cultura, capacidades y prácticas que se encuentran integradas con el conjunto de estrategias y su ejecución", con el propósito
de gestionar el riesgo en la creación, preservación y realización de valor.

IV. RESILIENCIA ORGANIZACIONAL

- **CONCIENCIA SITUACIONAL**

Busca identificar lo que tiene más valor en la organización, las características del entorno externo e interno, los riesgos y oportunidades de la situación actual, las interdependencias y las lecciones aprendidas de experiencias pasadas propias y de terceros.

En el proceso para construir resiliencia organizacional, la conciencia situacional representa la base para definir y aplicar acciones y asegurar que éstas sean las apropiadas.

- **FIJAR DIRECCIÓN**

Se establecen valores, lineamientos y estructuras, roles y responsabilidades que ayudan a la organización a ser más resiliente. El lograr mejorar el nivel de madurez en resiliencia debe ser uno de los objetivos de la organización.

- **BRINDAR COHERENCIA**

La identificación de los riesgos y la retroalimentación de información importante a todas las áreas forma parte de la cultura de la organización. Con la aplicación de disciplinas operacionales las organizaciones logran responder, anticipar y mitigar los riesgos, de forma coordinada entre las áreas y con terceros.

- **CAPACIDAD ADAPTIVA**

Se refiere a la posibilidad que tiene la organización de mantener su desempeño ante diferentes situaciones, modificando si es necesario los planes, estructuras o procesos inicialmente establecidos con acciones rápidas y flexibles. Reestructurar los planes oportunamente es la clave para que la organización tenga la capacidad de responder a eventos emergentes

- **FORTALECER LA ORGANIZACIÓN PARA EL CASO PUNTUAL EL ÁREA DE T.I.**

Para fortalecer la organización la resiliencia debe formar parte de la cultura de la organización, por lo que ésta es medida y resultan comunes las prácticas para prevenir, simular eventos, proteger, adaptarse y recuperarse valiéndose del aprendizaje sobre las experiencias vividas y la colaboración entre sus diferentes unidades.

Establecer un sistema de medición de los niveles de resiliencia con indicadores permitiría realizar un seguimiento sobre su nivel de madurez.

- **VALIDAR Y REVISAR.**

Consiste en realizar pruebas sobre la capacidad de resiliencia de la organización bajo diferentes escenarios. Adicionalmente, se deben efectuar evaluaciones por parte de terceros sobre las acciones de resiliencia para verificar la capacidad de respuesta, con el objetivo de realizar mejoras a favor de la resiliencia.

Realizar pruebas sobre las acciones de resiliencia, ejercitar periódicamente las capacidades de resiliencia y corregir para mejorar, es primordial para aumentar la resiliencia organizacional

V. ACCIONES SUGERIDAS PARA ESCALAR AL PRÓXIMO NIVEL DE MADUREZ

Reforzar la cultura de resiliencia, así como la colaboración constante y la coherencia entre las diferentes áreas y con otras organizaciones.

Formalizar las estructuras, procesos y reportes entre otros, orientados a la gestión de la resiliencia organizacional.

Establecer roles y responsabilidades a todos los niveles para mejorar el nivel de madurez de resiliencia.

Divulgar a todos los niveles de la organización los hallazgos sobre eventos que generan riesgos y oportunidades, así como construir y divulgar las lecciones aprendidas.

Efectuar pruebas sobre los procesos que fortalecen la resiliencia, y aplicar mejoras a las debilidades identificadas.

Emplear indicadores de medición para evaluar la resiliencia de forma periódica y hacer seguimiento de los planes de acción

Conclusiones

Una organización resiliente será aquella en la que sus procesos continúen operativos en cualquier circunstancia, con un grado de eficacia que tal vez no alcance el cien por cien del rendimiento deseable, pero que sí permita mantener la vida de la organización.

La gestión de riesgos, como disciplina operacional, se caracteriza por aumentar la gama de oportunidades, mejorar el desempeño, reducir sorpresas negativas, anticiparse a los cambios, mejorar la administración de recursos y mejorar la resiliencia organizacional.

Existirán grados en la capacidad de resiliencia de un organismo. Cuanto más traumática sea la crisis que es capaz de superar dicho organismo podemos hablar que es mayor su capacidad de resiliencia.

Desafío global

El camino de la resiliencia no es aquel que lleva a un destino cierto.

De hecho, una de las premisas para ser resiliente involucra reconocer que hay que cambiar el destino, y por ello es que la resiliencia está asociada con la manera de actuar más que con resultados específicos a obtener. En principio porque es una condición que requiere, al igual que un atleta, de procesos de mejora y entrenamiento constantes. Luego porque además de la ruta, las estrategias deben ser ajustadas en cada ocasión que sean requeridas para cumplir con los objetivos. La resiliencia organizacional debe ser entonces una manera de hacer negocios.

Más que nunca entonces, la gestión integral de riesgos y la resiliencia organizacional deberán tomar relevancia en la discusión de la directiva y en la visión estratégica del negocio. Deberán impregnarse en el ADN de la organización, y pasar a ser elementos de discusión necesaria en cada actividad, independientemente de su importancia relativa para la organización.

VI. REFERENCIAS

[1] Resiliencia en la Seguridad Informática, [en Línea], http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2904/00002215.pdf?sequence=1&isAllowed=y
[2] Continuidad_negocio_resiliencia [En Línea] http://qualitaslearning.com/w/c/t/D9VLBCF7/continuidad_negocio_resiliencia.html
[3] Disrupción [Fernando Bayón - en Línea] https://www.eoi.es/blogs/fernandobayon/2014/02/24/disrupcion/
[4] Resiliencia organizacional y gestión de Riesgos- Descubriendo el nivel de madurez y tomando las primeras medidas. PWC [En Línea]- Texto Guía tomado por las experiencias consignadas- https://www.pwc.com/ve/es/publicaciones/assets/PublicacionesNew/Estudios/1ra_Encuesta_Resiliencia_Riesgos_2018.pdf
[5] BS 65000: Guía para la Resiliencia Organizacional, [en Línea], http://normaiso22301.com/bs-65000-guia-para-la-resiliencia-organizacional/.

[6] ¿Qué hay de nuevo respecto a la gestión de riesgos? – COSO ERM 2017, [en Línea], https://www.incp.org.co/nuevo-respecto-la-gestion-riesgos-coso-erm-2017/
[7] ISO 22316:2017 Security and resilience -- Organizational resilience -- Principles and atributes, [en Línea], https://www.iso.org/standard/50053.html

[i] Consulta: http://normaiso22301.com/bs-65000-guia-para-la-resiliencia-organizacional/

Autor Elsa Victoria Muñoz Pérez
Ingeniera de Sistemas,
Estudiante de la Especialización en Seguridad Informática.
Actualmente trabajo en: Procuraduría General de la Nación.