Ciberresiliencia

DOI: 10.29236/sistemas.n159a7

La integración entre Seguridad de la Información y continuidad de negocio

Resumen
Así como la ambigüedad del concepto de Resiliencia Organizacional, la Ciber Resiliencia se debate en confusiones, por lo que el objetivo del presente escrito es proporcionar con claridad una versión encaminada a entender su importancia y alcance, en términos de Seguridad, Ciber Seguridad, Gestión de Crisis y Continuidad.

En esencia, la clave es la integración del escenario de ciberataque al Programa de Continuidad de Negocio, que suena simple, pero tiene muchas repercusiones, partiendo del Análisis de Riesgos que puede llevar a la interrupción del negocio y finalizando con el impacto operativo, reputacional y financiero, así como la implementación de alternativas tendientes a disponer de una estrategia funcional.

Adicionalmente, es necesaria la revisión de la Gestión de Crisis y del Plan de Comunicaciones, pues los mismos han cambiado debido a factores como el tipo de escenario de interrupción, los actores involucrados, los medios de comunicación (principalmente redes sociales) y las audiencias objetivo.

Palabras claves
Resiliencia, Ciberseguridad, Continuidad, Crisis

Introducción

Comenzando por lo básico, ¿sabían ustedes que la palabra resiliencia viene de latín, *resilio* usada por el ejército romano para describir la táctica de dar pasos hacia atrás o replegarse, para luego avanzar hacia adelante, en el sentido de cambio? Un concepto se trasladó a la física y se refiere a la propiedad de algunos materiales de "volver a su forma original" después de que por alguna razón la han perdido, o a la capacidad de deformarse sin romperse (un buen ejemplo es el bambú).

Este concepto se ha venido usando de diferentes maneras y con connotaciones poco entendibles. En cuanto al nivel de las personas, afirman Torres & Ramírez (2019), en psicología es usual hablar de la "capacidad de los seres humanos para adaptarse positivamente a situaciones adversas, superando el trauma ocasionado por estas".

Sin embargo, puede ir más allá y no limitarse a eventos puntuales, empero es una competencia en las personas que les permiten, por ejemplo, tomar decisiones correctas en la forma de ver la vida diaria y manejar cada una de las situaciones bajo presión y también en situaciones límite o eventos de desastres a la que nos enfrentamos.

En el ámbito de las organizaciones, este concepto es refinado y apunta a conectar la estrategia de negocios con la gestión de riesgos sistémicos, la cual plantea el entorno en el que se mueve; tiene que ver con percibir adecuadamente este entorno (conciencia situacional), con la coherencia en la gestión de riesgos y en la implementación de la estrategia, eliminando el trabajo por silos y enfocándose en una gestión integral. En este punto comenzamos a entender, por qué es necesario incluir el manejo adecuado de los riesgos derivados de los ciberataques, como parte de los riesgos sistémicos más preponderantes en la actualidad, bajo la nueva realidad impuesta por la pandemia del COVID-19, dado el incremento del uso de la tecnología en todos los ámbitos.

Existen varias definiciones del concepto de ciber resiliencia, por ejemplo:

- Instituto Nacional de Ciberseguridad de España - INCIBE (INCIBE, 2021), según el cual la ciber resiliencia es "la capacidad para resistir, proteger y defender el uso del ciberespacio de los atacantes".

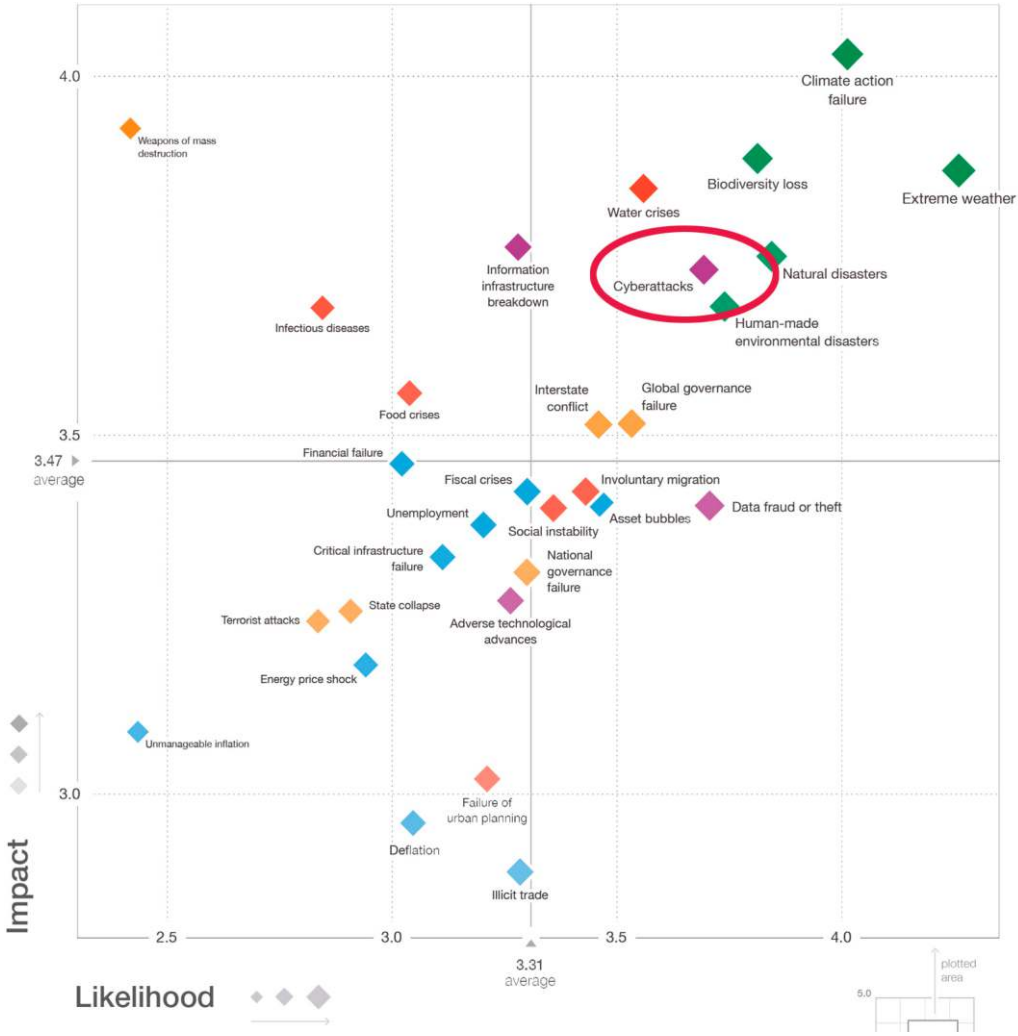
- Disaster Recovery Institute International - DRII (DRII, 2019), afirma que la Resiliencia Cibernética (*Cyber Resilience*) es "la capacidad de una entidad para entregar continuamente el resultado previsto a pesar de los eventos cibernéticos adversos".

• SGSI Blog de ISOTools Excellence (2019), “es la capacidad de las organizaciones de recuperarse de forma rápida de los ciberataques”.

• Así mismo, la habilidad de prepararse, reponerse y recuperarse de un posible incidente cibernético, la ciber resiliencia es una práctica que permite a una organización estar preparada ante posibles ataques, manejar la severidad de estos, y asegurar la continuidad del negocio en caso de que sucedan (The One Brief Aon, 2019).

En varios estudios realizados en los últimos años, el riesgo de ciberataques se ha posicionado como

Figura 1. Paisaje de los riesgos globales 2020



Nota. Matriz de impacto y probabilidad de riesgos. Tomado de Foro Económico Mundial (WEF, 2020).

uno de los de más alto impacto y también en probabilidad de ocurrencia; un ejemplo de esto es el Foro Económico Mundial (WEF, 2020) que califica a los ciberataques dentro del Top 10 de riesgos a nivel Global (Figura 1).

Desde una perspectiva proactiva, ser resiliente implica tomar acciones para desarrollar la capacidad para esa adaptación o incluso transformarse. Por supuesto, para lograrlo el primer paso es innovar, tener conciencia respecto a qué se requiere y contar con los riesgos emergentes que podrían impedir dicho propósito; existen maneras comprobadas que funcionan para manejarlos y sacarles provecho. Cuando se involucra el uso de tecnología de información en las organizaciones en su innovación y operación, también se registra un nuevo ámbito de riesgos, en ocasiones desconocidos y evolucionan más rápido que la capacidad para su entendimiento y manejo.

En este contexto, si una organización quiere ser ciber resiliente, debe empezar por tener personas resilientes en todos los niveles, iniciando con la conciencia de los directivos respecto al entorno global y la actitud, en cuanto a su total convicción para asumirlo. Más allá de las declaraciones vacías de valores corporativos y del cumplimiento de regulaciones, se demanda tomar acciones reales para contar con la capacidad adecuada de protección y respuesta en la recuperación de tecnología, en el instante que sea preciso.

Además, es importante tener en cuenta que hay múltiples factores que afectan la capacidad de una organización de ser resiliente, los cuales se pueden entender desde diferentes marcos de Resiliencia Organizacional existentes:

- ICOR - *International Consortium for Organizational Resilience* (ICOR) de EE.UU.
- BSI – *British Standards Institute* del Reino Unido.
- *The Resilience Institute* de EE.UU.

En todos ellos, se evidencia la necesidad de tener en cuenta múltiples disciplinas en la organización, para desarrollar la capacidad de recuperarse mediante la adaptación; además, entender que no es una práctica en sí misma, sino un resultado de hacer las cosas bien en cada uno de esos aspectos.

A continuación, una breve referencia de cada uno de los marcos mencionados (Figura 2).

Para ICOR la Resiliencia Organizacional se obtiene al conjugar las doce disciplinas que plantea, sin un orden específico y con la necesidad de revisar cómo debe ser el desarrollo específico de cada una y la integración con las demás.

En este modelo prima un enfoque holístico, en el que la Resiliencia

Figura 2. Marco de la Resiliencia Organizacional

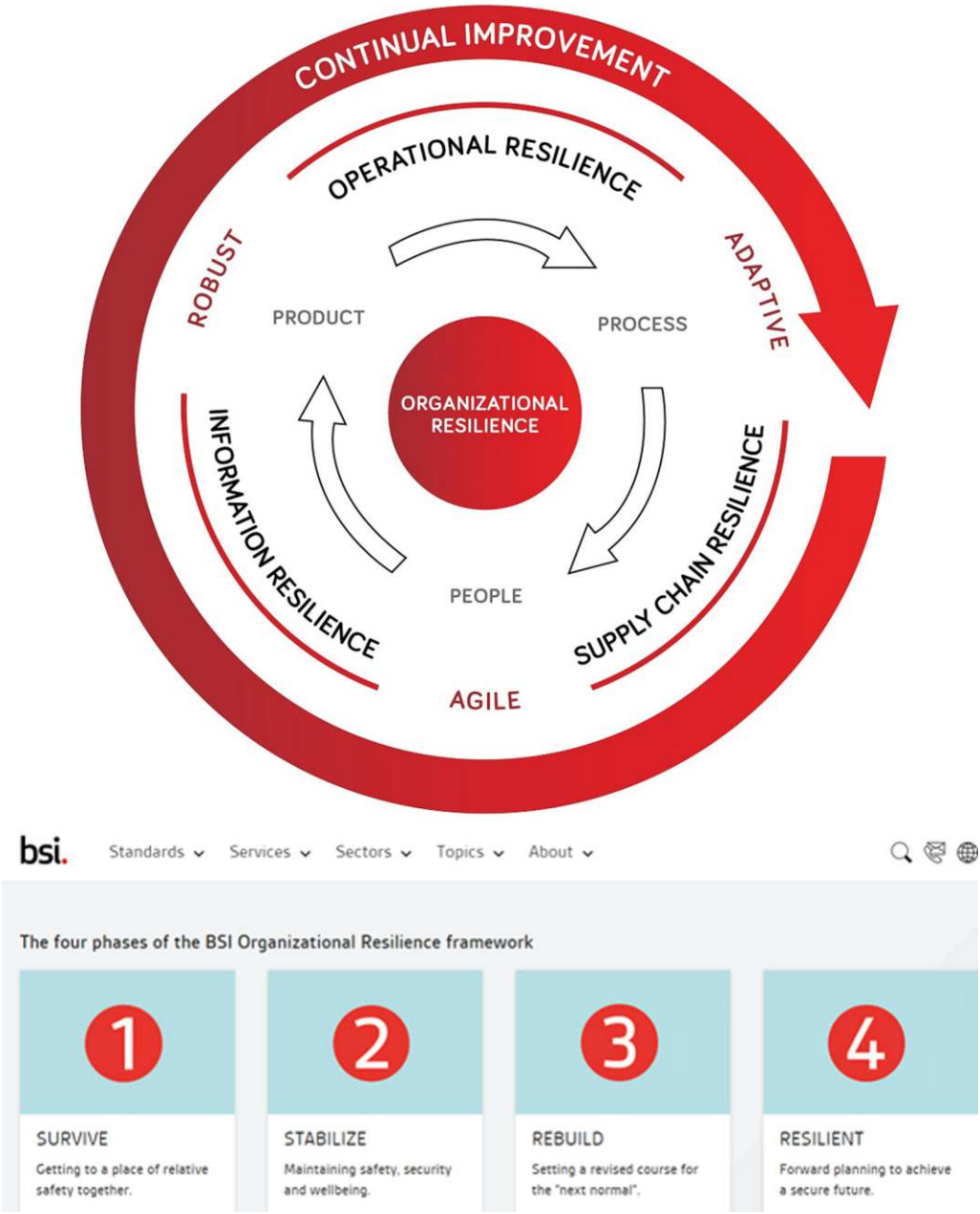
Nota. Marco de la Resiliencia Organizacional. (Tomado de ICOR, 2021, Traducción y adaptación al español iteam).

Organizacional es un resultado de hacer bien las cosas en cada una de las disciplinas y de manera integrada; es decir, teniendo cuidado sobre cómo el desarrollo en cada una de ellas va de la mano con las demás, pues enfocarse en sólo una o algunas, al final no va a permitir la evolución completa como organización. Es necesario balancear los esfuerzos y asignar las responsabilidades de manera adecuada. En este sentido, ser resiliente como organización es una decisión que va absolutamente ligada a la estrategia de negocio establecida. Para finalizar, cabe nombrar que este marco tiene un vínculo a la Resiliencia Comunitaria, es decir, de las ciudades o países, en el que se establecen unos principios y definiciones requeridas para el bienestar de la comunidad a partir de las organizaciones que la conforman (Figura 3).

Para el BSI Group (*British Standards Institution*), la Resiliencia Organizacional se enfoca en dar respuesta operacional a eventos de gran magnitud o crisis, como la Pandemia COVID-19 y para ello establece un antes y un después en las acciones que la organización debe tomar, con un enfoque proactivo en los procesos y en las personas, pero alineado a la estrategia de negocio.

En este caso, el enfoque en lo operacional significa inicialmente definir el manejo a la situación, en ciertos casos dirigir sus esfuerzos a establecer un ambiente seguro para su operación con antelación, cono-

Figura 3. Three essential elements of Organizational Resilience

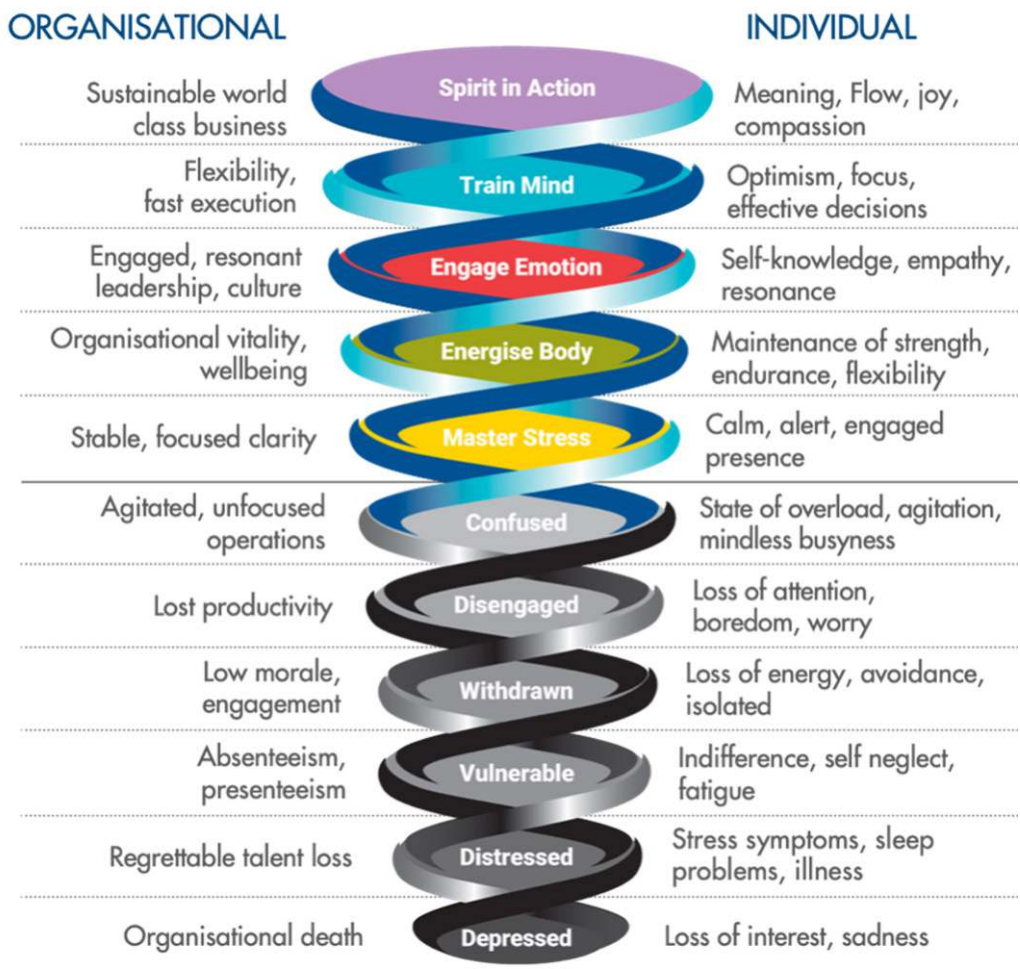


Nota. Three essential elements of Organizational Resilience. (Tomado de BSI)

ciendo su ambiente y su funcionamiento. El siguiente paso, es la estabilización para funcionar con las medidas implementadas anteriormente, ciertas restricciones y cambios que usualmente requieren esfuerzos importantes para asegurar el bienestar de los colaboradores, el manejo de la cadena de suministro y la información.

Posteriormente, en la reconstrucción se induce al cumplimiento de estándares en los ámbitos de Gestión de Riesgo, Ambiental, Continuidad de Negocio, Ocupacional, Calidad y Seguridad de la Información, como prácticas probadas que aportan a esa estabilización de la operación y al funcionamiento en la nueva normalidad. Incluso puede

Figura 4. Resilience Spiral



Nota. Resilience Spiral. (Tomado de The Resilience Institute, 2021)

llevar a cambiar su modelo de negocio e industria, para adaptarse y estar preparado para posibles eventos futuros que requieran de la Resiliencia Organizacional (Figura 4).

Para el *Resilience Institute*, la capacidad resiliente de las organizaciones parte de las personas y crea un paralelo en diferentes niveles de evolución, estableciendo un punto de inflexión entre el deber ser (positivo) y lo no aceptable (negativo), en la medida que se cumple con los 60 factores de resiliencia que están organizados en 11 categorías. La meta es evolucionar y sostener dicha evolución en la medida que se reconoce las debilidades y riesgos y se trabaja para resolverlos.

Esta orientación, viene influenciada desde el desarrollo de lo personal y el potencial del ser humano, para luego extrapolar a las organizaciones y también a las comunidades. Utiliza una herramienta de diagnóstico para establecer un punto de partida y un plan de trabajo, para aprender a vivir y superar los factores que limitan actualmente su desarrollo y para adaptarse a lo necesario para crecer a la resiliencia, sabiendo que no hay soluciones mágicas y que se requiere de esfuerzo para la evolución deseada. Utiliza la figura de la espiral como concepto para avanzar, con base en lo existente, sin olvidar los pasos anteriores, aprendiendo, adaptándose y creciendo. Aceptando que siempre existen retos, aún en la prosperidad y que representan siempre una posibilidad de aprender.

Realizando una comparación de los tres modelos marco de Resiliencia Organizacional, encontramos en resumen que **ICOR** establece una visión global y holística, con diversas disciplinas que conllevan al resultado y se integra con la resiliencia comunitaria. Por otra parte, **BSI** se enfoca en lo operacional y en la organización, protegiendo y adaptando el funcionamiento propio, la cadena de suministro y la información. Por último, el **Resilience Institute** tiene un enfoque más filosófico que permea desde lo personal a las organizaciones y las comunidades, con la noción de crecimiento y evolución.

Los tres marcos tienen en común los conceptos de adaptación y gestión de riesgos, como parte fundamental de la capacidad de ser una organización resiliente, cada cual con diferentes formas para lograrlo.

¿Por qué es importante gestionar la ciber resiliencia?

El aumento de los vectores de ataque que significa la amplia implementación de nuevas Tecnologías de Información, es la principal razón que conlleva la necesidad de gestionar de manera eficaz este importante riesgo, aplicable prácticamente a cualquier tipo de organización; ya no es único en grandes y conocidas corporaciones, más bien se ha encontrado que es asunto de

las pequeñas y medianas empresas, toda vez que son más vulnerables por estar menos protegidas y poseer una menor conciencia de los riesgos en general.

Algunos datos para tener en cuenta:

• Más del 50% de la población mundial, ahora está en línea; aproximadamente un millón más personas se unen a internet cada día. Dos tercios de la humanidad poseen un dispositivo móvil. La cuarta revolución industrial (4IR) de la mano de las nuevas tecnologías atraen grandes beneficios económicos y sociales a gran parte de la población mundial[1].

• Quinta generación (5G) redes, computación cuántica y la Inteligencia artificial están creando oportunidades y a su vez, nuevas amenazas propias en ciberseguridad.

• Ciberataques a la infraestructura crítica, ha sido el enfoque inicial de los delincuentes.

• El robo de datos, permite la manipulación de comportamiento individual y colectivo, liderando a daño físico y psicológico.

La integración de Seguridad de la Información y Continuidad de Negocio

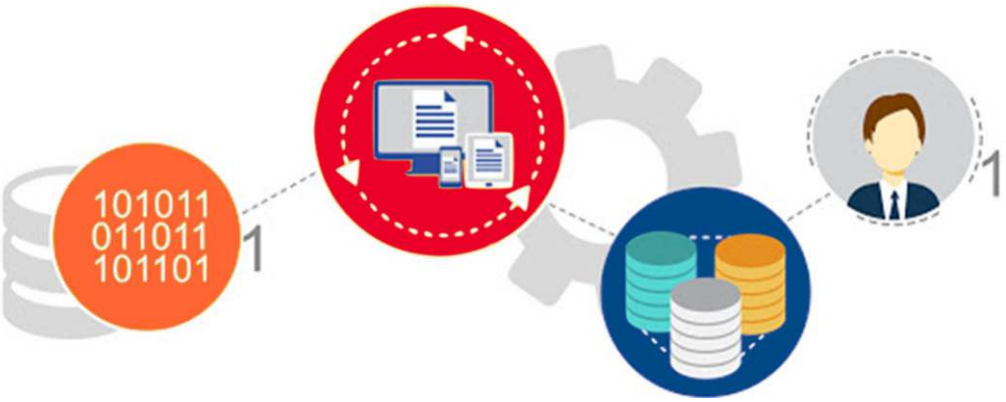
Un enfoque sobre la integración es el que nos brinda el NIST Cyber Resilience Framework 1.1[2], en el que se establece cómo en los pasos ini-

[1] The Global State of Digital 2020 (2020). https://www.hootsuite.com/pages/digital-2020
[2] NIST Cyber Resilience Framework 1.1 https://www.nist.gov/cyberframework/framework

Figura 5. Cyber Resilience Course

Nota. Cyber resilience course. (Tomado de DRII. CRLE 2000 material, 2019)

Figura 6. Identificación de Amenazas



Nota. Identificación de amenazas. (Elaboración propia).

ciales la Seguridad de la Información y Ciber Seguridad son responsables de la protección, y la Continuidad de Negocio es la responsable de la recuperación, combinando manejo de crisis y específicamente la respuesta del DRP para la infraestructura de tecnología. Ambas disciplinas son responsables en conjunto de la gestión de incidentes (Figura 5).

Lo primero, es identificar correctamente las ciberamenazas del entorno en el que opera la organización. Es un proceso estructurado que consulta diferentes fuentes para identificar y proveer información sobre amenazas cibernéticas y sus tendencias (Figura 6).

Este proceso suele llamarse Ciber Inteligencia[3], puesto que es un término acuñado a partir de las estructuras gubernamentales; consta de varias etapas que serán revisadas más adelante y sus salidas vendrán determinadas por la naturaleza de la amenaza, si es conocida o no, activando otros procesos que forman parte de la gestión de ciberseguridad (Figura 7).

La planificación de la gestión de ciberamenazas incluye:

- Definir qué fuentes van a ser incorporadas a la investigación.
- Establecer las responsabilidades que tendrá el equipo.
- Establecer el método y las herramientas de identificación de amenazas.
- Conocer la frecuencia en que se realizarán las investigaciones y se presentarán los resultados.

[3] Ciber Inteligencia: Se define como la adquisición y el análisis de información para identificar, rastrear y predecir las capacidades, intenciones y actividades cibernéticas que apoye la toma de decisiones. ASOSEC – Asociación Colombiana de Seguridad. Recuperado de https://asosec.co/ciberinteligencia/

La recolección de datos tiene como objetivo obtener la información en bruto, establecer los atributos de la información y contar con un repositorio de los datos.

El análisis de los datos consiste en la aplicación de diversas técnicas para poder convertir los datos en información. El resultado final del análisis de ciberamenazas deberá determinar qué acciones realizar con ella.

La conclusión de este proceso es la difusión a la organización de los hallazgos, para:

- Alineación de los equipos.
- Fortalecimiento de controles o desarrollo de nuevos.
- Preparación preventiva de los usuarios.
- Llamado a la acción.

Es decir, tomar medidas que realmente fortalezcan la capacidad de protección de la organización, mediante una gestión adecuada de los incidentes que sean amenazas de ciberataques. No obstante, puede ser insuficiente y es por ello que se necesita una capacidad de recuperación, desde la Continuidad de Negocio, esto implica una integración, la cual se aprecia en la figura 8.

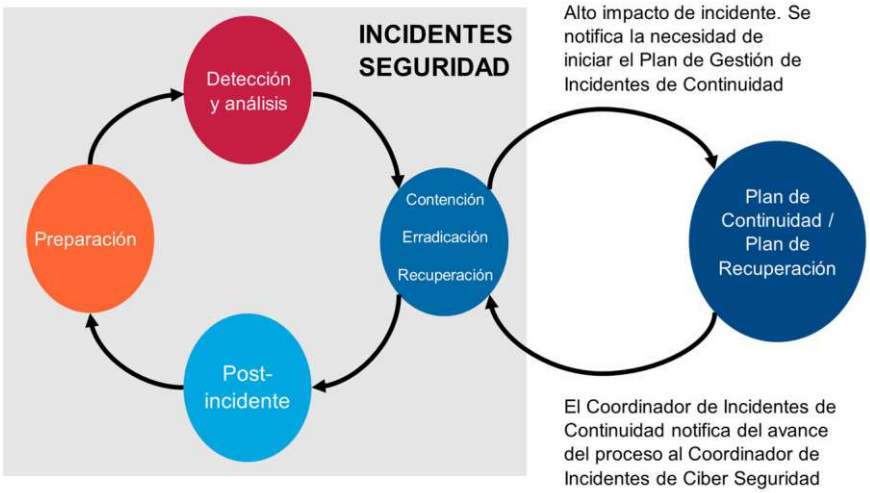
Recuperación de tecnología y lo que se requiere hoy

Desde que comenzó la disciplina de *Disaster Recovery*, en los tiem-

Figura 7. Modelo de gestión de Ciber amenazas

Nota. Modelo de gestión de Ciber amenazas. (Elaboración propia).

Figura 8. Integración del proceso de atención de incidentes de seguridad con el proceso de continuidad de negocio y recuperación ante desastres



Nota. Integración del proceso de atención de incidentes de seguridad con el proceso de continuidad de negocio y recuperación ante desastres. (Elaboración propia).

pos de los primeros mainframes, la dependencia de un solo sitio de cómputo concentrando todo el procesamiento y el riesgo de perderlo, la estrategia siempre fue crear una capacidad redundante, para recuperar los datos y el procesamiento en otro sitio similar, equivalente o algunas veces superior.

Lo clásico es establecer lo más claro posible qué es lo más crítico para el negocio (entendiendo negocio, como la razón de ser de la organización, no sólo para empresas comerciales) usualmente, mediante un Análisis de Impacto al Negocio (BIA por sus siglas en inglés, *Business Impact Analysis*), para definir los procesos críticos y todos los recursos que requieren para una recuperación adecuada, así como los tiempos en que deberían estar de nuevo operativos; uno de los recursos más importantes ha sido la tecnología, las aplicaciones y cómo funcionan para la operación del negocio y qué tantos datos se deben conservar. También se identifican los riesgos del sitio de cómputo y de los sitios donde funciona el negocio. Con estos insumos se diseña una Estrategia de Continuidad, dentro de la cual la recuperación de la tecnología de información es una parte crucial, a la que se le conoce como DRP (por sus siglas en inglés, *Disaster Recovery Plan*). Al final se documentan los planes (procedimientos para las diferentes

áreas de TI) y se hacen ejercicios incluyendo pruebas, para asegurarse de que todo ello funciona.

Han evolucionado diferentes tecnologías para realizar estas tareas, replicar más rápido y de manera eficiente e incluso hasta lo que se conoce como Disponibilidad Continua (*Continuos Availability* por sus siglas en inglés), que permite tiempos de recuperación cercanos a cero.

Inicialmente el DRP consistía en tener un centro de datos alterno, pero ante el escenario de ciberataque eso no es suficiente, simplemente porque el daño causado al centro de datos principal se replicaría tan rápido como sea la eficacia de la estrategia implementada, que puede ser en segundos o en minutos, por lo cual no es una defensa apropiada, toda vez que el resultado sería tener en corto tiempo dos o más centros de datos atacados y probablemente inservibles.

Es por esto, que se requiere implementar otras estrategias y nuevas tecnologías, tampoco procedimientos y trabajo en conjunto con las áreas responsables de seguridad de la información, y otros departamentos de TI. Algunos ejemplos son:

- Air GAP y Bóveda segura (vault), que en esencia establece una conexión aislada y controlada, física y lógicamente, para evitar que el ataque se replique, pero no los datos más esenciales del DRP que se guardan de manera segura cada vez que se activa y asegura la conexión.

- Regreso en el tiempo, a múltiples puntos de recuperación hacia atrás, lo que se logra a partir de tecnologías de virtualización e hiperconvergencia.

Conclusiones

Atender esta nueva realidad de ciberataques aumentados, que evolucionan muy rápido y son difíciles de manejar, requiere de un enfoque diferente, en el que se combinan varias disciplinas, siendo las principales la Seguridad de la Información y la Continuidad de Negocio.

Cabe considerar que no se debe realizar de manera independiente, por el contrario, implica trabajo en conjunto con el objetivo en común de gestionar este riesgo de la mejor manera para la organización.

La integración de las disciplinas es la clave, primero con trabajo preventivo, implementando las soluciones tecnológicas y procedimientos que obstaculicen la realización de los ataques (Seguridad de la Información), sin creer que se es completamente infalible; también es necesario implementar las soluciones para tratar el riesgo del ciberataque una vez se presenta, para poder restaurar los datos y el procesamiento desde fuentes seguras y aisladas.

En paralelo, activando la gestión de crisis para este caso tan especial, que tiene tanto potencial de dañar la reputación, por negligencia (permitir que suceda el ataque a los datos propios o de los clientes) o por mala actuación una vez sucede. En este sentido, es preciso revisar el Plan de Manejo de Crisis y el Plan de Comunicaciones, para hacerlos más asertivos, toda vez que requieren una atención más rápida que otros escenarios y exigen la capacidad de ajuste, cambio y toma del rumbo a la misma velocidad de los acontecimientos del ataque cibernético, que puede ser caprichoso de acuerdo con lo que el atacante pueda decidir durante o desde antes, muchas veces dejan acciones del código malicioso para más adelante contar con una reserva en su actuación y así tomar ventaja.

Desde la perspectiva de Continuidad de Negocio es necesario revisar el proceso y cómo interactúa en el Comité de Crisis con el área de Seguridad de la Información/Ciberseguridad, según sea el caso, para la adaptación de la Estrategia y Planes de Continuidad antes de que ocurra el evento, y para la toma de decisiones y la activación necesaria, una vez el incidente existe o tiene el potencial de convertirse en una crisis.

En conclusión, la Ciber Resiliencia es la capacidad de recuperarse ante eventos de ciberataque, impidiendo o minimizando sus efectos desde la Seguridad de la Información y también estableciendo un Estrategia de Recuperación de Tecnología (DRP) adecuada integrada a la Continuidad de Negocio y la Gestión de Crisis.

Referencias

DRII (2019). CRLE 2000 Cyber Resilience for the Business Continuity Professional. Course Instituto Nacional de Ciberseguridad de España (INCIBE). (3 de marzo de 2021).
¿Qué es la ciber resiliencia y cómo influye en la seguridad? [Mensaje en un blog].
https://agenciab12.com/noticia/que-es-ciberresiliencia-como-influye-seguridad

Foro Económico Mundial - WEF (2020). The Global Risks Report 2020. (N.15). Recuperado de
https://es.weforum.org/reports/the-global-risks-report-2020

Organizational Resilience Framework BSI. (2021). Three essential elements of Organizational Resilience.
https://www.bsigroup.com/en-GB/our-services/Organizational-Resilience/Three-essential-elements-of-Organizational-Resilience/ y https://www.bsigroup.com/ en-GB/our-services/Organizational-Resilience/bsi-organizational-resilience-framework/

ICOR (2021). Organizational Resilience Framework. Traducción y adaptación al español iteam.
https://www.build-resilience.org/organizational-resilience-framework.php

The Resilience Institute (2021). Resilience Spiral. https://resiliencei.com/resources/resilience-spiral/

SGSI Blog de ISOTools Excellence (2019). ¿Qué es la ciber resiliencia? [Mensaje en un blog]. https://www.pmg-ssi.com/2019/10/que-es-la-ciber-resiliencia/

The Global State of Digital 2020 (2020). https://www.hootsuite.com/pages/digital-2020

The One Brief Aon. (2019) La Resiliencia Cibernética: ¿Qué hacer en caso de un posible ataque? https://theonebrief.com/latam/post/la-resiliencia-cibernetica-que-hacer-en-caso-de-un-posible-ataque/

Torres, J. C. & Ramírez, N. (2019). Resiliencia ¿Organizacional? LinkedIn. iteam Ltda. https://www.linkedin.com/pulse/resiliencia-organizacional-norman-ramirez/

Norman A. Ramírez S. MBCP, CRMP, CCRP e Instructor (DRII), MBCI (BCI) & Auditor Líder ISO22301 (ICOR). *Posee amplia experiencia como emprendedor en su rol de Gerente General de iteam y como especialista Consultor Senior de Resiliencia Organizacional, Continuidad de Negocio y Riesgos Empresariales. Graduado de la Universidad de los Andes (Bogotá, Colombia), Ingeniero Industrial (1998) y Especialista en Sistemas de Información en la Organización - ESIO (2002).*