La ciberresiliencia ante la inevitabilidad de los ciberataques

DOI: 10.29236/sistemas.n167a7

Resumen
La protección del ciberespacio demanda la participación de procesos durante todas las etapas del desarrollo de un incidente: antes (preparación y prevención), durante (contención y reacción inmediata) y después (continuidad de negocio y adaptabilidad). Lamentablemente la inevitabilidad es una constante, por más mecanismos preventivos: la probabilidad de ser víctima de un ciberataque resulta casi una certeza. La ciberseguridad y la ciberresiliencia son disciplinas dedicadas a la protección del ciberespacio, conceptos que muchas veces se usan como sinónimos, pero que realmente presentan diferencias importantes, sobre todo en su alcance y especialización. Un entendimiento erróneo de estos conceptos puede derivar en una protección parcial y a largo plazo, deficiente. El presente artículo tiene por objetivo describir las similitudes y diferencias de cada una de estas disciplinas, resaltando sus características fundamentales, con la finalidad de que podamos conformar una estrategia de defensa integral y más efectiva ante los escenarios actuales.

Palabras clave
Ciberseguridad, ciberresiliencia, ciberespacio, estándares, marcos de trabajo

Introducción

La historia reciente ha dejado claro que la inevitabilidad es una constante: actualmente ninguna nación ni organización está exenta de sufrir un ciberataque. Lamentablemente, aún con numerosos esfuerzos preventivos que se vierten en regulaciones, estrategias y mejores prácticas para fortalecer la ciberseguridad, siempre existe la posibilidad de ser atacado con éxito. Aunado a esto, se encuentra el factor de la escasez, los recursos humanos y materiales para prevenir y reaccionar en forma inmediata, ante un incidente de esta magnitud siempre son limitados. Adicionalmente, en la actualidad las organizaciones cuentan con centenas de controles de seguridad a los que se debe dar cumplimiento, conforme a las regulaciones y estándares, los cuales se han mostrado insuficientes y no han mitigado de manera eficaz los ciberataques. Como se ha observado, la exigencia puntual e inflexible en su cumplimiento puede conllevar el efecto contrario: en lugar de disminuir el número de ciberataques exitosos, se han incrementado. La causa raíz no es nada sencilla, sino compleja y multidisciplinaria.

Las estadísticas a nivel nacional y mundial muestran un crecimiento sostenido de los ataques informáticos dirigidos hacia diferentes países, originados por adversarios en el ciberespacio, particularmente hacia infraestructuras de redes informáticas y de telecomunicaciones a través de las cuales las personas se comunican e interactúan como lo hacen en el mundo físico, y que son indispensables para la operación de los procesos de los Estados (Mandiant, 2021).

Los ataques de alto impacto originados en el ciberespacio son cada vez más frecuentes, más especializados, más complejos, más silenciosos, más coordinados y, desafortunadamente, inevitables, los cuales incluso están siendo dirigidos a infraestructuras críticas de los países, con amplios efectos multiplicadores que, si bien tienen origen en espacios virtuales, están afectando al mundo físico y viceversa.

Además, la especialización de los ciberataques es cada vez mayor, generando incluso organizaciones de tipo Estado-Nación dedicadas exclusivamente a causar daños por diferentes vías. Ante esta nueva forma de afectación se pueden generar mayores conflictos asimétricos, en los que países de menor poder tradicional pueden causar graves daños a naciones con un mayor poder.

Así pues, ninguna organización está exenta de ser atacada exitosamente en el ciberespacio, por más

medidas preventivas que se procuren. Incluso países con amplios recursos y medidas de ciberseguridad son víctimas de ataques. Por ello, resulta esencial que se sigan suministrando bienes y servicios a pesar de haber sido objeto de un ciberataque. Eso es materia de la ciberresiliencia, el cual es un fenómeno complejo, que requiere la aplicación de capacidades multidisciplinarias, lo cual también lo convierte en ocasiones, hasta en un problema subjetivo, que requiere una profunda interpretación a partir de diversos puntos de vista.

Concepto general de resiliencia

El Diccionario de la Lengua Española (2020) señala que la palabra **resiliencia** proviene del latín ***resilire*** que significa **volver atrás, volver de un salto, resaltar o rebotar**. Dicho concepto ha sido utilizado en diferentes disciplinas como, por ejemplo, en el uso de materiales, ecología, planeación urbana, por mencionar algunas.

Originalmente, en el entorno de los materiales la resiliencia se refería principalmente a la propiedad de absorber la fuerza exterior que se aplicaba a dicho material y que permitía recuperar su forma después de haber sido doblado o comprimido (Dupont, 2019). Mismo término que después se aplicó con más difusión en las disciplinas de psicología y ecología.

En psicología se emplea para referirse de forma general a la capacidad de una persona para superar circunstancias traumáticas como la muerte de un ser querido, un accidente, etc. Si bien este concepto es ampliamente aceptado hoy en día, aún no se determinan con claridad las circunstancias o actividades que logran regenerar nuevamente a la persona que sufrió un evento traumático (Bork, Henkel, Stirna, & Zdravkovic, 2014).

El uso de este concepto con relación a la atención de desastres en las naciones, ya sea por causas de la naturaleza o humanas, no es nuevo y se puede rastrear su uso desde hace varias décadas. De hecho, la Organización de las Naciones Unidas en 2005 fomentó el concepto de la resiliencia en las naciones para afrontar desastres y reducir los riesgos relacionados (NAP, 2012). Desde entonces, el concepto de resiliencia ha sido utilizado para referenciar a procesos para afrontar eventos adversos en distintas áreas como las tecnológicas, políticas o sociales.

En el espacio físico, las Academias Nacionales en EUA analizaron este concepto desde el punto de vista de desastres a nivel nacional (huracanes, inundaciones, terremotos, actos de terrorismo, enfermedades, etc.) en el cual se enfatizó sobre la importancia de la resiliencia y en que los incidentes se gestionaran desde diferentes áreas, desde los ámbitos local, estatal y federal, así como integrando esfuerzos de la sociedad civil, instituciones priva-

das y gubernamentales (NAP, 2012). En dicho documento se definió resiliencia como "la habilidad para preparar/planear, absorber, recuperar y, sobre todo, **adaptarse** exitosamente a futuros o actuales eventos adversos" (pág. 16).

En ese sentido, esa definición complementa las concepciones que comúnmente se utilizan, las cuales generalmente se centran en las primeras etapas defensivas y reactivas, minimizando las fases de absorción y de adaptación. De la misma forma, resalta la importancia de priorizar la inversión en los elementos de resiliencia con el fin de tomar mejores decisiones para incrementarla, disminuyendo el impacto no inmediato de estos tipos de eventos (NAP, 2012).

En dicho texto se enfatizó en que los desastres no dejarán de suceder y señaló algunas de las causas para ello como, por ejemplo: el crecimiento de la población, migrantes hacia zonas costeras, limitaciones en infraestructura pública, cambio climático, etc.

Los puntos anteriores ponen de manifiesto las siguientes ideas:

1. El evento adverso ocurre en la vida de una persona[1], esto es, **la resiliencia no es preventiva**, no evita un incidente. Se habla de resiliencia como parte de la superación de ese suceso.
2. La esencia de la resiliencia radica en **sobreponerse** ante tal incidente, el cual afectará de forma distinta a cada persona o grupo de ellas. Existen reflexiones que incluso indican que el ente afectado saldrá fortalecido al sobreponerse de dicho evento.
3. La ocurrencia de eventos desafortunados [pe. desastres] **no es opcional**.

Finalmente, Boris Cyrulnik (2014), considerado como padre del concepto en psicología, en su libro "¿Por qué la Resiliencia?" indica que "…lo más difícil de descubrir son las condiciones que permiten iniciar un nuevo desarrollo después del trauma". Lo que pone de manifiesto que es de gran importancia conocer cuáles son los elementos que incrementan la resiliencia *después* del fenómeno traumático.

Resiliencia en el ciberespacio

Las observaciones realizadas anteriormente son importantes, toda vez que los conceptos y definiciones utilizados comúnmente para denotar la resiliencia en el ciberespacio (o **ciberresiliencia**), difieren en la orientación de procesos clave. Por ejemplo, la muerte de un ser querido no se podrá evitar mediante la resiliencia, ni tampoco este evento impactará de la misma forma a cada persona.

En el mundo del ciberespacio, lo anterior lleva a observar que la ci-

[1] Aunque en este documento se indica una "persona", se puede hablar de familias, grupos o comunidades con características similares.

berresiliencia no es en principio para evitar ciberataques; en caso de que ocurran, será para determinar el grado en que afectarán a las organizaciones y deberán adaptarse ante las **nuevas** condiciones. Es de gran importancia que muchos estudios de ciberresiliencia parecen tener un enfoque preventivo y de reacción inmediata; no obstante, existen otros documentos en los que se resalta la resiliencia como la capacidad para evolucionar, **adaptarse** y alcanzar un nuevo equilibrio. En el primero podría ser una resiliencia total [no pasó nada]; en el segundo, hubo un evento y se derivan **secuelas**, pero se debe seguir adelante. Para el autor de este artículo, esa última es la noción que se debe tener de ciber-resiliencia.

Resulta de suma importancia señalar que un ciberataque, por su naturaleza, no puede ser impedido o mitigado por completo. Como lo indica Dupont: "el paradigma de protección y prevención resulta insuficiente, y la ciberresiliencia tiene que estar entre las estrategias de administración de riesgo… generando una estrategia complementaria" (Dupont, 2019, pág. 1). Esta misma idea la manifiesta Linkov (2013) y agrega que, hay que tener cuidado de no mezclar los términos del análisis de riesgo con ciberresiliencia: el primero requiere de una cuantificación que mide la probabilidad de que un evento conocido ocurra; mientras que el segundo, corresponde al ámbito de eventos inimaginables y por tanto no cuantificables, que ocurren por sorpresa.

Esa última característica resulta de suma importancia, toda vez que la sorpresa implicará un nivel de **improvisación** en la gestión del incidente (Dupont, 2019). No hay nada escrito y, por ende, posiblemente los protocolos de actuación en ese momento sean limitados o en el peor caso inservibles, pues se estará reaccionando a un evento que ni siquiera ha sido planeado. La improvisación es un punto que normalmente es concebido como una parte negativa de la planeación en general [se hacen planes para no improvisar], pero aplicada a la planeación de la resiliencia resulta ser de gran valor. Como lo indica Dupont (2019), al hacer el símil con la música de Jazz (pág. 7): "La resiliencia requiere del arte de combinar espontaneidad e intuición, con disciplina y experiencia".

Una definición propia basada en las que contemplan todas las fases de un ciberincidente podría ser: **ciberresiliencia es la capacidad de anticiparse, soportar y recuperarse, parcial o totalmente, ante un ciber-ataque con el fin de proveer continuamente bienes y servicios hasta adaptarse bajo condiciones diferentes al estado inicial alcanzando un nuevo equilibrio.**

La definición anterior deja en claro que no se está hablando del concepto de **continuidad de negocio**,

el cual precisamente busca regresar a un estado inicial casi idéntico, previo al incidente y por lo general en un tiempo limitado. De ahí que existan muchas métricas al respecto como RTO [*Recovery Time Objective*] para especificar el tiempo que una organización necesita para recuperarse después de sufrir un incidente, RPO [*Recovery Point Objective*] para determinar el tiempo máximo que una organización está dispuesta a perder información o el RTA [*Recovery Time Actual*] que es el tiempo en el que se activa el plan de recuperación de desastres. En este aspecto, la **continuidad de negocio** [BCP por sus siglas en inglés] y el "plan de recuperación ante desastres" [DRP por sus siglas en inglés] representan un concepto diferente a la ciberresiliencia, la cual contempla una fase de adaptación al final que regresará a la organización a un estado diferente al incidente previo, esto es, bajo un nuevo escenario [o equilibrio].

Diferencia entre ciberseguridad y ciberresiliencia

En este punto resulta de suma importancia revisar dos términos relacionados con la protección del ciberespacio: ciberseguridad y ciberresiliencia. Las definiciones simples de estos conceptos pueden apoyar en la identificación de la diferencia fundamental: mientras la ciberseguridad se enfoca a la protección general del ciberespacio [pre y reacción inmediata], la ciberresiliencia se enfoca en dicha protección, pero en un nivel adaptativo [post y mediano-lago plazo]. Este último nivel es la parte diferenciadora entre ambos conceptos.

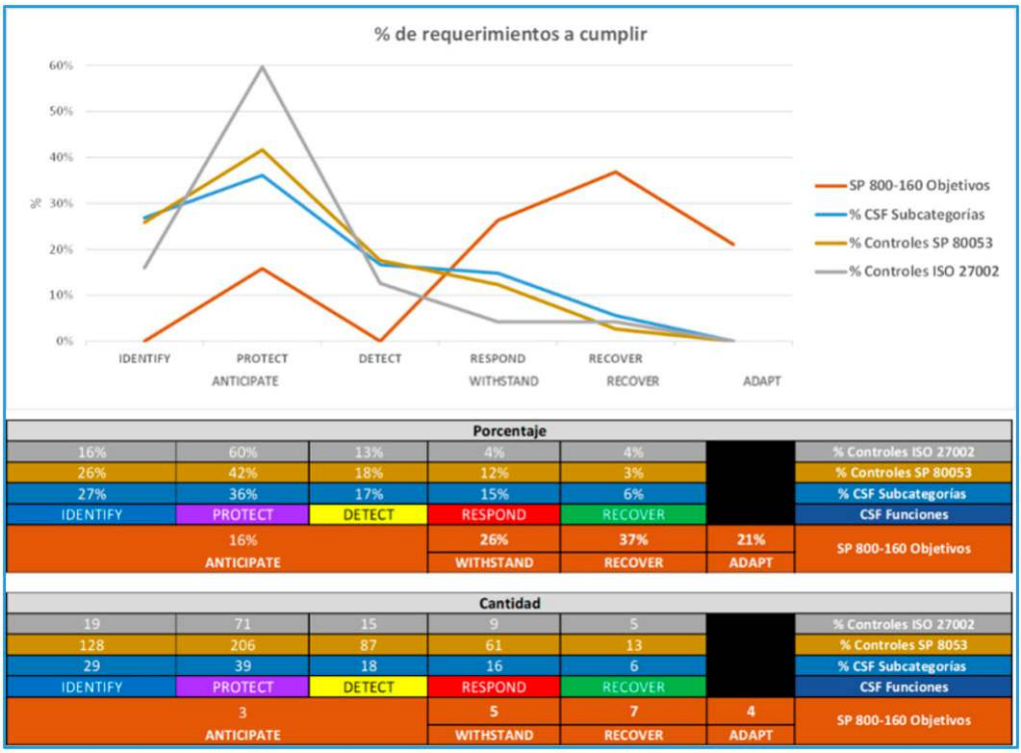
Como parte de este artículo se revisaron algunos estándares que demuestran exactamente este comportamiento:

Figura 1
Fases que cubren los estándares

La gráfica 1 fue elaborada con base en 4 estándares de amplio uso en organizaciones de países en todo el mundo:

- ISO 27002 [*International Organization for Standarization*]
- NIST 800-53 [*National Institute of Standards and Technology, Security and Privacy Controls for Information Systems and Organizations*]
- NIST CSF [*National Institute of Standards and Technology, CyberSecurity Framework*]
- NIST SP 800-160 [*National Institute of Standards and Technology, Developing Cyber Resilient Systems*]

Los primeros tres estándares están enfocados en la ciberseguridad, mientras que el último NIST SP 800-160 es el único que se especializa en ciberresiliencia. Como se aprecia en la gráfica anterior, esos primeros tres estándares tienen un porcentaje amplio de cobertura de las primeras 3 fases **sin cubrir la fase de adaptación**. Si bien el NIST SP 800-160 tiene controles



Porcentaje						
16%	60%	13%	4%	4%		% Controles ISO 27002
26%	42%	18%	12%	3%		% Controles SP 80053
27%	36%	17%	15%	6%		% CSF Subcategorías
IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER		CSF Funciones
16% ANTICIPATE			26% WITHSTAND	37% RECOVER	21% ADAPT	SP 800-160 Objetivos

Cantidad						
19	71	15	9	5		% Controles ISO 27002
128	206	87	61	13		% Controles SP 8053
29	39	18	16	6		% CSF Subcategorías
IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER		CSF Funciones
3 ANTICIPATE			5 WITHSTAND	7 RECOVER	4 ADAPT	SP 800-160 Objetivos

Figura 1
Fuente: Elaboración propia basada en (Ureña Cuate, 2021)

para la ciberseguridad, es el único que tiene objetivos de protección que contemplan fase de adaptación.

Resulta oportuno señalar que la figura anterior **no** desea expresar que los marcos de trabajo o estándares enfocados a ciberseguridad sean menores o deficientes en cuanto a la protección ante amenazas del ciberespacio, sino que los enfoques difieren en su alcance y finalmente resultan complementarios.

Para finalizar, Cano (2020) indicó con claridad que, no solo es cuestión de seguir prácticas comunes de continuidad de negocio y recuperación para enfrentar un ciberataque de alto nivel, diseñado de forma particular para irrumpir en una organización vital. Si bien eso es esencial en todo programa de seguridad, se deben incorporar estrategias de resiliencia de forma complementaria.

Interrelaciones en ciberresiliencia

La ciberresiliencia es un componente organizacional, un elemento que coadyuva al correcto funcionamiento de las organizaciones. Además, resulta importante seña-

lar que este componente está interrelacionado con otras áreas que tienen un propósito complementario como se muestra en la figura:

Figura 2
Relaciones de la ciberresiliencia

La gráfica 2 permite identificar la interrelación entre varias disciplinas que se relacionan para alcanzar una resiliencia organizacional sin importar que un riesgo provenga del mundo físico o del lógico, y este gráfico envolvería a las demás áreas. Asimismo, se puede observar lo siguiente:

- La continuidad del negocio está más enfocada en la disponibilidad de los procesos y abarca un mayor número de actividades organizacionales [no solamente los que tienen contacto directo con el ciberespacio].
- La gestión de riesgos también atiende diferentes amenazas hasta que se concrete un incidente, entonces un riesgo deja de serlo para convertirse en incidente.
- La ciberseguridad está acotada al espacio virtual del ciberespacio, y como se vio, su alcance es menor que la ciberresiliencia, aunque comparten estrategias y controles en las primeras etapas.

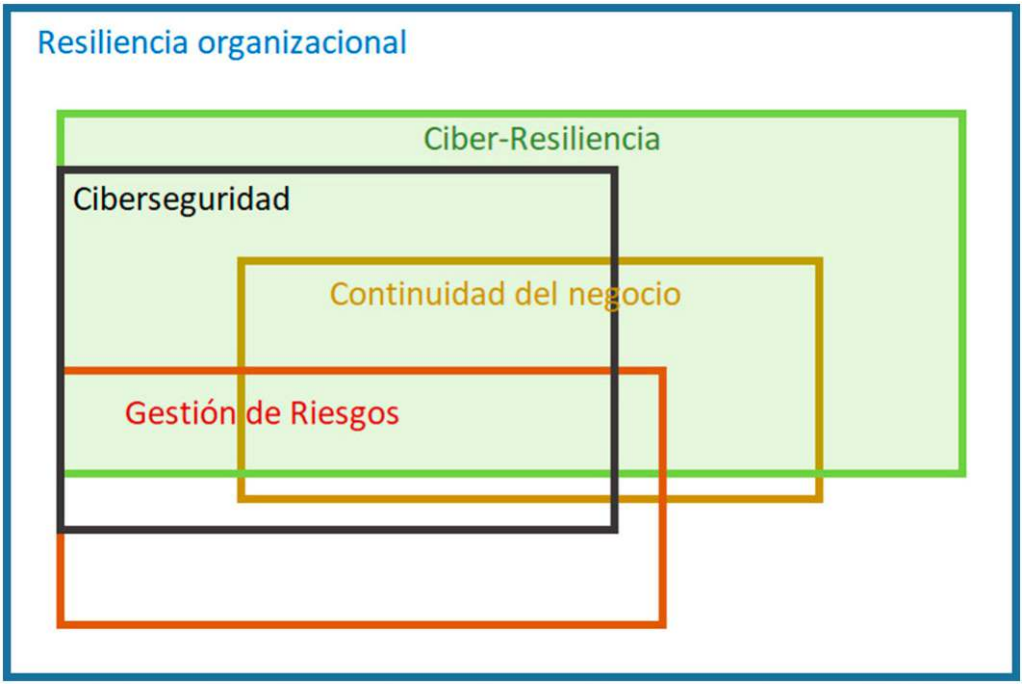


Figura 2
Elaboración Propia basada en (Vargas Pedroza, 2019)

Conclusiones

La ciberresiliencia es un término que requiere de un análisis profundo para identificar con más claridad sus componentes y relaciones. A través de este artículo se resaltó que la fase **adaptativa** es la que hace la principal diferencia con otros conceptos relacionados en el ciberespacio, y que generalmente se confunden ocasionando una aplicación incompleta del término. Dada la magnitud de algunos ciberataques, es posible que las actividades de adaptación no sean por completo claras o no hayan sido publicadas todavía: ¿en qué se han modificado los procesos involucrados?, ¿qué es ahora diferente de lo que se hacía?, ¿cuánto cambio?, ¿cuánto mejorará la protección integral del ciberespacio? En fin, son preguntas que aún están en investigación por lo que tenemos mucha tarea por hacer en este entorno virtual.

Referencias

Bork, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2014). Cyber Resilience- fundamentals for a definition. Suecia.

Cano, J. (2020). ¿Por qué los ciberataques son inevitables?: Prácticas y capacidades claves de la ciberseguridad empresarial. En V. Gauthier-Umaña, R. Méndez-Romero, & D. Suárez, *Voces diversas y disruptivas en tiempos de Revolución 4.0* (págs. 223-248). Bogotá: Universidad del Rosario. doi:10.2307/j.ctv123x566.14

Cyrulnik, B., & Anaut, M. (2014). *¿Por qué la resiliencia?* (A. Diez, Trad.) Barcelona, España: Gedisa.

Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. *Journal of Cybersecurity*, 1-17. doi:10.1093/cybsec/tyz013

Linkov, I., Eisenberg, D. A., Bates, M. E., Chang, D., Covertino, M., Allen, J. H., . . . Seager, T. P. (2013). Measurable Resilience for Actionable Policy. (A. Publications, Ed.) *Environmental Science & Technology*, 108-110.

Mandiant. (2021). *M-Trends.* Obtenido de https://www.mandiant.com/resources/m-trends-2021

NAP. (2012). *Disaster Resilience. A National Imperative.* Washington DC, USA: The National Academies Press.

Real Academia Española. (2020). *Real Academia Española*. Obtenido de https://www.rae.es/

Ureña Cuate, M. (1 de Octubre de 2021). Curso de Ciber-resiliencia organizacional. CDMX, México.

Vargas Pedroza, G. (Marzo de 2019). El estado del arte para enfrentar los ciberataques y el cibercrimen organizado. *Gerencia. Noticias, Análisis e Información*. Obtenido de http://www.emb.cl/gerencia/articulo.mvc?xid=4647&ni=ciber-resilencia-el-estado-del-arte-para-enfrentar-los-ciberataques-y-el-cibercrimen-organizado

Arturo García Hernández
Estudioso de la ciberseguridad con más de 25 años de experiencia. Obtuvo el grado de Doctor en Defensa y Seguridad Nacional con mención honorífica en la Universidad Naval de México, especializándose en la ciberresiliencia de las infraestructuras críticas. Cuenta con varias certificaciones profesionales de reconocimiento internacional como DSE, CISM y CISSP. Labora en Banco Central de México como Gerente de Seguridad en Tecnologías de la Información.