A RESILIENT LOOK AT INFORMATION SYSTEMS IN THE CONTEXT OF CYBER-ATTACKS

UNA MIRADA RESILIENTE A LOS SISTEMAS DE INFORMACIÓN EN EL CONTEXTO DE LOS CIBERATAQUES

MSc. Miguel Hernández Bejarano, MSc. Luis Eduardo Baquero Rey

Fundación Universitaria Los Libertadores
Grupo de Investigación en Ingeniería Aplicada GUIAS
KR 16 63 A 68, Bogotá D.C., Colombia.
Tel.: 57-1-2544750, Ext. 3359
E-mail: {mhernandezb, lebaqueror}@libertadores.edu.co

Abstract: This document is framed in the context of the ongoing research project entitled "*Cybernetic Resilience in Web and Online Applications*", having as a first objective to present the main considerations and contributions of resilience in the security of information systems, especially attention to what is related to computer attacks or cyber attacks. In this sense, a bibliographic review is carried out on the most relevant elements involved in the subject, such as organizations and cybersecurity, the role that resilience to the information systems of organizations should play in terms of cybersecurity against the exposures or vulnerabilities to which it may be exposed; as well as resilience in the face of information security management. Some related standards and good practices are considered, and some final considerations and conclusions are presented.

Keywords: Cyberattacks, resilience, information systems, informatic security.

Resumen: Este documento se enmarca en el contexto del proyecto de investigación en ejecución titulado "*Resiliencia cibernética en aplicaciones web y online*", teniendo como un primer objetivo presentar las principales consideraciones y aportes de la resiliencia en la seguridad de los sistemas de información, en especial atención a lo relacionado con los ataques informáticos o ciberataques. En tal sentido, se realiza una revisión bibliográfica sobre los elementos más relevantes involucrados en la temática, como lo son, las organizaciones y la ciberseguridad, el papel que debiera desempeñar la resiliencia a los sistemas de información de las organizaciones en términos de ciberseguridad frente a las exposiciones o vulnerabilidades a que pueda estar expuesta; así como la resiliencia frente a la gestión de la seguridad de la información. Se consideran algunos estándares y buenas prácticas relacionadas y se presentan algunas consideraciones y conclusiones finales.

Palabras clave: Ciberataques, resiliencia, sistemas de información, seguridad informática.

1. INTRODUCION

En la actualidad, todas las organizaciones (pequeñas, medianas, grandes) se enfrentan a una gran cantidad de riesgos e inseguridades procedentes de diversas fuentes tecnológicas o humanas que se encuentran ligadas o asociadas a amenazas que explotan una amplia tipología de vulnerabilidades, (Yuxia, Qing, Wenzhi, & Bei, 2018) como las que están presentes en las aplicaciones de software, en el hardware (Meltdown y Spectrem), los ataques realizados con ciberarmas (WannaCry, NotPetya). De otra parte, las organizaciones además de implementar

políticas y utilizar tecnologías para la protección de sus sistemas de información, requiere la generación de una conciencia colectiva comprometida con las instituciones ya que los usuarios son el eslabón más débil de la cadena de trabajo, el generar un análisis claro sobre roles, perfiles, usuarios y formas de acceso tanto remoto como físico, hace que este tipo de temas se convierta en una necesidad imprescindible dentro del desarrollo y sobre todo en la generación de controles y acciones que permitan disminuir el riesgo (Akashdeep & Sam, 2018). Estos riesgos y vulnerabilidades han aumentado debido a la conexión de objetos cotidianos a Internet, que en algunos casos no fueron diseñados con esquemas de seguridad.

Además, las empresas de hoy, sin importar su tamaño, cuentan con una gran cantidad de datos que si no se gestionan de la manera correcta pueden ser un punto crítico para el negocio ocasionando un rezago ante el mercado. Una empresa en la actualidad debe ser consciente de la adecuada protección, disponibilidad y uso de sus datos para una óptima toma de decisiones. En el marco del IBM Pro en Bogotá, la compañía resaltó la importancia de diseñar arquitecturas confiables y seguras que a futuro pueden traer una reducción de costos interesantes para las empresas. Se debe tener en cuenta que no todos los datos se pueden almacenar solo en la nube o en servidores, "*almacenar correctamente los datos permite maximizar la posibilidad de utilización, toma de decisiones de negocio y mejorar la calidad de esas decisiones que toman las empresas*" afirmó Mario Gómez, gerente de IBM Systems en Colombia.

En tal sentido, la información en términos de sistemas es el conjunto de datos, ya procesados y ordenados para su comprensión, que aporta nuevos conocimientos. Es tal la importancia de la información, que, a través de ella, se solucionan problemas, se toman decisiones, se determinan las alternativas convenientes para una situación especial; es decir, que aprovechar la información da la base racional del conocimiento; pero un aspecto de gran importancia es que la información deberá tener un grado de "utilidad" para modificar las interacciones con el entorno, debe ser "vigente" y "confiable" para que preste un servicio adecuado y oportuno.

2. EL PAPEL DE LA RESILIENCIA

En la actualidad la resiliencia es un enfoque emergente que enfatiza la capacidad de una organización para recuperarse rápidamente y adaptarse a eventos adversos. Teóricamente, tal enfoque podría ayudar a muchas organizaciones y sistemas a abordar la incertidumbre y la complejidad inherentes a sus operaciones, y superar mejor las interrupciones o choques que de lo contrario amenazarían con degradar o destruir las operaciones centrales de la organización. En la práctica, sin embargo, falta de consistencia, en cómo se modela aplica y mide la resiliencia, lo cual puede limitar su efectividad para ayudar a las organizaciones en esta tarea. En concordancia con esto La Organización para la Cooperación y el Desarrollo Económicos (OCDE) es una organización que está particularmente interesado en aplicar principios de resiliencia a las amenazas emergentes a la economía y la prosperidad social entre sus estados miembros, implementada a los sistemas de información de las organizaciones.

Por ello, la resiliencia cibernética es cada vez más reconocida como un componente crítico de prácticas de ciberseguridad. Al igual que en otros campos, la resistencia cibernética se refiere a la capacidad del sistema para recuperar o regenerar su rendimiento después de un ciberataque el cual produce una degradación de su rendimiento una empresa ciberresiliente alinea con éxito la gestión de la continuidad y la recuperación de desastres con las operaciones de seguridad de una manera holística.

Por lo tanto, la resiliencia es uno de los factores clave que contribuyen a la preservación de la funcionalidad de los subsistemas de infraestructura crítica, es decir, sectores, subsectores y sus componentes (Rehak David M. J., 2013). Es la capacidad de estos subsistemas para mitigar la intensidad del impacto causado, por un evento externo o interno amenazador, y a fin de reducir la duración de la falla o interrupción (Rehak D., 2017) , la resiliencia es un factor importante que determina la confiabilidad de la infraestructura crítica de los sistemas y puede entenderse como un proceso cíclico basado en la mejora continua del sistema a partir de la prevención , la absorción, la recuperación y la adaptación para la preparación de los sistemas de infraestructura crítica ante emergencias o la capacidad para realizar y mantener sus funciones cuando se ven afectados negativamente por factores internos o externos (Rehak David H. M., 2015). Desde este punto de vista el éxito en el cumplimiento de los servicios que soportan el core del negocio depende de la disponibilidad, productividad y en última instancia de la resiliencia de los activos que soportan los servicios; información como fuente para la toma decisiones, tecnología para soportar la automatización del proceso de la organización, los usuarios para ejecutar y

monitorear el servicio e instalaciones en las cuales se pueda operar el proceso o servicio.

En lo que respecta a resiliencia, la palabra latina resilio significa "rebotar" o "retroceder", y, de hecho, en el lenguaje ordinario de la palabra "resiliencia" es consistente con esta etimología, y la resiliencia es una propiedad deseada o buscada de los sistemas., (Matteo & Valverde, 2019). En este orden de ideas la resiliencia es la capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido (RAE). y Cibernética es la ciencia que estudia las analogías entre los sistemas de control y comunicación de los seres vivos y los de las máquinas (RAE). En este sentido resiliencia cibernética es el termino asociado la capacidad de las organizaciones de recuperarse y adaptarse luego de interrupciones futuras predecibles y desconocidas rápidamente de ataques deliberados; o incidentes que impliquen el uso de las tecnologías de la información y la comunicación, por ende la resiliencia cibernética se puede describir como la capacidad de cualquier organización para prevenir, detectar, responder y recuperarse de los impactos de un ataque con daño mínimo a su reputación y competitividad; una alineación que se busca entre la prevención, la capacidad de detección y la respuesta para mitigar el avance de los ciberataques a nivel de la exposición que tiene la organización dentro del ciberespacio. Dicho concepto es un poco complejo, toda vez que algunos teóricos plantean la resiliencia cibernética como parte del ciberespacio (la empresa inmersa en él), mientras que otros lo plantean al ciberespacio definido dentro de la empresa u organización, haciendo que con ello, una empresa o entidad sea capaz de prevenir, identificar, contener y recuperarse de un gran número de amenazas contra los datos, aplicaciones e infraestructura de TI y en fin sobre esa base de exposición orientada al ciberespacio como (Lee, Bagheri, & Jin, 2016), (Babiceanu & Seker, 2019), (EY PERU LIBRARY, 2017), (Suárez & Peláez, 2018), (ATKINS, 2018), (Symantec, 2014).

3. LA RESILIENCIA Y LOS SISTEMAS DE INFORMACIÓN

La necesidad de tener sistemas de información dentro de cualquier organización o entidad hace que la resiliencia de dichos sistemas sea una prioridad, tal como lo define (ISO 22316, 2017) y (Sharma & Kaul, 2018), más aún cuando en el mundo de tecnologías de información (TI), la infraestructura es una prioridad para poder proveer todos los servicios de TI. Partiendo desde los mismos servidores, sistemas de comunicaciones o de seguridad, sistemas de bases de datos, sistemas de conectividad alámbrica e inalámbrica, son algunas de las aristas que se deben tener presentes para poder tener claridad en un procedimiento de continuidad de negocio a partir de la tecnología, con fin de proveer y mantener una continuidad operacional, a pesar de las fallas que se puedan presentar a nivel físico como lógico. Dentro de toda esta gama de problemas se tienen problemas por sobrecarga en sistemas eléctricos y de alta potencia, fallas en el centro de datos (datacenter), problemas de saturación de canales de comunicación, tráfico malicioso en la organización, amenazas avanzadas a nivel de software, exfiltración de información confidencial, ataques de secuestro digital de información (ransomware), virus, suplantación, denegación de servicios y un largo etcétera que cada día crece más con la necesidad de los delincuentes para poder hurtar o hacer daños a la información como lo define (Alguliyev, Imamverdiyev, & Su, 2018), (Accenture, 2018) y (Tarao & Okamoto, 2016).

Cuando se empieza a trabajar con la unión de estos dos mundos, los sistemas de información y la resiliencia, lo primero que se debe adelantar es una análisis de brecha que permita medir cada componente en aspectos como rendimiento, ancho de banda, conexiones concurrentes, disponibilidad, latencia, paquetes perdidos, módulos de seguridad activos, tiempo de respuesta de equipos de soporte, etc., como lo define (British Standars International, 2014), de tal manera que se pueda evaluar en tiempo real, qué tan fuertes son los controles asumidos a nivel de tecnologías de seguridad y políticas de seguridad implementadas dentro de la organización o entidad y de esa manera definir las capacidades de la infraestructura de TI, de las personas a cargo de cada uno de los subsistemas de TI y/o de los mismos proveedores, en el momento de prestar algún tipo de servicio con el cual se cuenta para poder salir adelante y cumplir con los RTO y RPO definidos dentro de la etapa de análisis en concordancia entre la norma (ISO 22316, 2017) y la aplicación (ROMERO, 2014).

De esta manera, esta primera etapa del proceso de adopción de la resiliencia se torna como un punto crítico, al momento de empezar a mirarse introspectivamente y empezar a reconocer que existe dependencias grandes en las organizaciones, ya sea públicas o privadas en las distintas tecnologías de la información para desarrollar las actividades cotidianas y que muchas veces no se tiene claridad frente a los servicios, infraestructura, conocimientos y necesidades de la misma entidad y de sus

usuarios, como lo evidenció (Ding, Han, Xiang, Ge, & Zhang, 2018).

Así mismo, las aplicaciones y los ambientes en los que se ejecutan los sistemas de información son cada vez más complejos, diversos y cargados de muchos tecnicismos, donde empiezan a coexistir una gran cantidad de conceptos nuevos, nuevos servicios y nuevas tecnologías, que son la base de la arquitectura empresarial a nivel de TI y que cada uno de dichos ítems sostiene algún tipo de procedimiento u operación frente a la generación de valor de la entidad u organización como se evidencia en (Babiceanu & Seker, 2019) y (ATKINS, 2018).

Tras toda esta generación de valor por medio de la adopción de sistemas de TI, viene un análisis que desde las normas de seguridad obligan a adelantarlo y es la gestión de riesgos, como lo plantea (ISO 22316, 2017), toda vez que cada Sistema de Información, cada tecnología, cada servicio basado en TI trae numerosos riesgos y una gran variedad de vectores de ataque (amenazas), a los que la mayoría de las organizaciones se encuentran expuestos y que por lo general, no se tiene claridad del nivel de exposición y menos un control específico para cada uno de ellos y a partir de todo este análisis se puede observar que los puntos de falla comunes pueden estar orientados hacia la infraestructura expuesta, pero que al final del análisis uno de los ítems más complejos y de mayor falla son los usuarios, pues es la masa crítica más disímil, con diferentes tipos de conceptos y completamente susceptibles a un innumerable cantidad de problemas que no solo para la ejecución de vulnerabilidades se pueden adoptar sino que se convierten en piezas claves al momento de adelantar procesos de resiliencia.

Hay que tener en cuenta que los sistemas de información actualmente, al permear todos los procedimientos de una entidad u organización, han alcanzado límites insospechados, a tal punto que el nivel de sistematización de plantas completas por medio de robots, PLC, internet de las cosas y muchas tecnologías adicionales como el SCADA, sistemas de TV, control y calidad, son formas de asumir posturas frente a la tecnología pero también de asumir riesgos frente a la misma como lo expone (Wei, De Aguiar, Collar, & Otto, 2015).

Por tanto y bajo las necesidades claras de tener en las manos el futuro de una empresa, al momento de adelantar los procesos de resiliencia, muchas entidades gubernamentales y privadas han definido ciertas metodologías que han ayudado a generar modelos de trabajo para adoptar en el resto de las organizaciones y de esa manera poder definir un marco de trabajo preciso para poder estandarizar dicho proceso de adopción y buenas prácticas.

4. LA RESILIENCIA Y LA GESTIÓN DE LA SEGURIDAD

La resiliencia organizacional parte de una gestión proactiva de la seguridad como lo define (Symantec, 2014), (Asia Pacific Economic Cooperation, 2017) y (Strigini, 2012), lo cual involucra a todos los niveles jerárquicos de la entidad u organización y en ese sentido se plantean cuatro ítems específicos que se deben tener en cuenta para poder generar la resiliencia que se requiere, a saber:

• APRENDER: La organización debe estar en la capacidad de aprender, no solo de los eventos propios sino de los ajenos, buscando comprender los problemas, qué pasó, por qué pasó y sobre todo, tener la actitud para utilizar todo ese aprendizaje en pro de la organización o el sistema.

• RESPONDER: Si bien es cierto, el aprendizaje está orientado hacia la evaluación del pasado y verificación del presente, la respuesta puntualiza las condiciones actuales (usuales o irregulares) que se van a definir con el fin de poder adelantar acciones de manera efectiva, flexibilizando los protocolos o procedimientos, para que la recuperación se dé, de la mejor manera.

• MONITOREAR: El ítem anterior sobre la respuesta es la probabilidad a la cual, se le apunta nunca llegar, de ahí que hay una necesidad de adelantar acciones que permitan evitar al máximo, cualquier tipo de acción que direccione hacia la respuesta y el monitoreo de ciertas variables, las cuales van a determinar la toma de acciones previas que eviten llegar a dicho estado; en ese sentido, el monitoreo va a permitir pronosticar, adelantar y gestionar el desarrollo de eventos que involucren problemas de pérdida de capacidad operativa, en ese sentido se hace necesario definir y priorizar las amenazas, ubicarlas en el corto, mediano y largo plazo y a partir de todo ese análisis, revisar los modelos de riesgo que la organización está tomando y sobre todo como se hace dichos controles.

• ANTICIPARSE: Toda organización debe estar en la posibilidad de prever posibles riesgos, anticiparse a las amenazas y conocer sus vulnerabilidades y solo a partir de dicha prevención se puede obtener una planeación plausiblemente clara y precisa que oriente a la organización hacia una resiliencia efectiva y a aprovechar las oportunidades en el mediano y largo plazo.

En este sentido, se pueden observar estas cuatro etapas diagramadas en el siguiente gráfico:

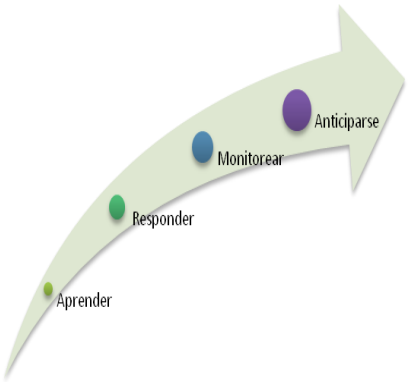

Fig. 1. Gestión proactiva de una organización

Desde la perspectiva de que resiliencia es la capacidad de proteger y sostener la operación de una organización, apoyando el cumplimiento de sus objetivos competitivos y misionales con la presencia y gestión del riesgo, se pueden identificar 3 elementos fundamentales para identificar el nivel de resiliencia, según lo define (ATKINS, 2018):

- Hay resistencia frente a la destrucción,
- Se forja un comportamiento vital positivo pese a las circunstancias difíciles.
- Se regresa a un estado normal en un tiempo razonable.

A partir de esto según lo plantea (EY PERU LIBRARY, 2017) y (Hua, Chen, & Luo, 2018), toda organización puede estar sujeta a riesgos generados por condiciones particulares de negocio o de tecnología que conlleva a definir dos ramas de trabajo plenamente definidas, una, orientada al negocio o misionalidad denominada Resiliencia de Negocio o RNE y la otra de frente a la parte tecnológica llamada Resiliencia de Tecnologías de Información (RTI), como se muestra en la siguiente gráfica:

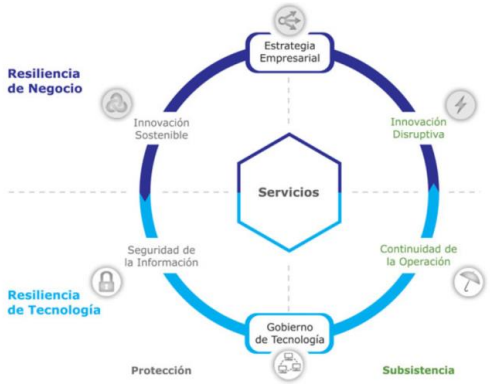

Fig. 2. Tipos de Resiliencia. (ESET, 2017) y (Asia Pacific Economic Cooperation, 2017)

Por lo que es importante la identificación de la infraestructura crítica de la organización, las partes involucradas (desde la alta gerencia y demás recurso humano), el establecer una documentación de roles y responsabilidades, la construcción de mecanismos de coordinación y colaboración, la elaboración de un marco de referencia para la administración del riesgo, así como el establecimiento de métricas.

5. ALGUNOS ESTÁNDARES Y BUENAS PRÁCTICAS

5.1 La norma ISO 22316

En el año 2017, la ISO entrega una de las normas que trata de dar un norte frente a la unificación de conceptos, que es la ISO 22316 de 2017 (ISO 22316, 2017), buscando generar unos principios y atributos para que las organizaciones puedan elegir la norma que más le acomode y de la misma manera, tengan claridad en las necesidades del estándar.

Cabe resaltar que este estándar no puede ser utilizado para certificar una organización y está construido como un paraguas que cubre una amplia gama de disciplinas de gestión, que juntas, con la suficiente madurez y capacidad dentro de una empresa o entidad, y con una buena capacidad de interacción y sinergia, hacen que dicha organización pueda alcanzar metas a largo plazo de una manera organizada y resiliente. Por esta razón, en esta norma se empieza a hablar de "Resiliencia organizacional" ampliando el concepto hacia la preparación que toda organización debe tener, frente a las amenazas que podrían desarrollarse lentamente, que aún no son fatales, pero que si no se anticipa de forma correcta pueden afectar de manera notoria a la organización, según lo explica (ISO 22316, 2017).

Esta norma propone un enfoque estructurado para poder alcanzar la capacidad de recuperación que se busca dentro de una organización, definiendo las acciones que se deben adelantar para poder encontrar un nivel óptimo de resiliencia. Por esta razon, se rige por dos principios como base fundamental de su funcionamiento, los cuales permiten consolidar una postura frente al tema, los cuales son:

- La sinergia de toda la entidad o empresa es la principal fortaleza para resiliencia empresarial y de los sistemas de información, según (ISO 22316, 2017). Bajo esta perspectiva, el comportamiento de todos y cada uno de los miembros de una empresa o entidad deben contribuir a la resiliencia y cualquier comportamiento pasivo o contraproducente debe ser evitado o controlado. En pocas palabras, lo que plantea la norma es que "la unidad hace la

fuerza" buscando que la fuerza de trabajo debe consistir en un grupo de personas con características altamente resilientes por si solas, lo que hace que se aumentar el nivel de resiliencia desde abajo hacia arriba. La lógica para definir este principio conlleva a la necesidad de trabajar en un acoplamiento dentro de la fuerza de trabajo obligando a que el sistema sea resiliente en la mayor base de exposición y donde la gerencia solamente dirige lo ya ganado.

• El segundo principio, según la norma citada, pone de frente a los diferentes tipos de habilidades, las cuales son muy importantes, ya que las nuevas amenazas, los desafíos y las oportunidades pueden proceder de diferentes áreas dentro de la empresa y para poder resolverlos se deben trabajar desde diferentes perspectivas.

De la misma manera como define estos principios, también plantea dos atributos sobre los cuales deben generarse otros, que van a ayudar a la empresa o entidad a conseguir los objetivos propuestos, teniendo en cuenta que los expuestos son solamente una primera aproximación, pues de ellos se deben desprender una gama de atributos adicionales, que van a apoyar el camino hacia la resiliencia mejorada en concordancia con (Asia Pacific Economic Cooperation, 2017), (British Standars International, 2014), (International Organization for Standardization, 2018) y (Lee, Bagheri, & Jin, 2016). Estos son:

• La comprensión del contexto de la empresa. Para contribuir a la resiliencia es necesario conocer la organización, no sólo como parte de la gestión de los riesgos, sino también dentro de la identificación de oportunidades.

• Mejora continua. Todos y cada uno de los integrantes de una organización deben pensar en la forma de mejorar continuamente, coadyuvando el crecimiento de la entidad o empresa en el alcance de metas a nivel de servicios internos y externos, buscando que de alguna manera esto revierta en la posibilidad de la empresa se pueda reponer a algún tipo de problemática adversa.

Una vez se tiene definido los dos ítems iniciales, es necesario empezar a trabajar en las personas que van a adelantar cada una de ellas y que sin las cuales es muy difícil lograr algún tipo de avance (Suárez & Peláez, 2018) y (Hua, Chen, & Luo, 2018). De esta manera, la norma define algunas ocupaciones u objetivos que deben cumplir dichas obligaciones, las cuales deben estar alineados a objetivos específicos, que aportan a la construcción de la misionalidad de la organización.

Algunas de las consideraciones que se definen dentro de la norma (ISO 22316, 2017) para la construcción de las ocupaciones son:

• Objetivos individuales alineados con los objetivos de la empresa de tal manera que cada individuo sepa lo que adelanta y como aporta a la construcción de la organización.
• Tener claro el propósito de la empresa, de tal manera que las labores de cada persona sean claras, precisas y orientadas a variables medibles.
• Dar seguimiento a las ideas innovadoras, las cuales pueden ayudar a cumplir de mejor manera la misionalidad de la organización.
• Si bien es cierto hay actividades que pueden ser nuevas y que van a requerir recursos, no se debe dejar de pensar en las actividades en curso y que hacen parte del flujo normal de la entidad o empresa.

Bajo esta perspectiva, la norma define ciertas necesidades para ser gestionadas desde sistemas integrados que obligan a generar, no solo administración de consideraciones propias de cada empresa sino a generalizar algunas, que, en el sentido estricto, toda entidad o empresa debería tener o por lo menos adelantar el trabajo para poder conseguirlas. En ese sentido, dichas disciplinas de gestión no son de obligatorio cumplimiento, pero se sugieren como una labor proactiva de una organización como lo define (Colbaugh & Glass, 2011). Dichas Disciplinas son:

• Gestión ambiental
• Gestión de las instalaciones
• Control financiero
• La gestión de salud y seguridad
• Gestión de la calidad
• Gestión de riesgos

5.2 La ISO 22301

Es una norma internacional de gestión de continuidad de negocio, especifica los requisitos para implementar, mantener y mejorar un sistema de gestión para proteger, reducir la probabilidad de ocurrencia, prepararse, responder y recuperarse de las interrupciones cuando surjan, proporciona una base de entendimiento, desarrollo e implantación de continuidad de negocio dentro de la organización (ISO, 2019).

5.3 La ISO 27001

El estándar ISO/IEC 20000, es el estándar ISO/IEC 20000, de gestión de la calidad de los servicios TI (Tecnologías de la Información) (ISO, s.f.). La Asociación Española de Normalización y Certificación (AENOR, 2016) expresa que la norma ISO 27001 detalla los requisitos de un Sistema de Gestión de la

Seguridad de la Información (SGSI). Provee un marco común para la elaboración de las normas de seguridad de cualquier organización, estableciendo un método de gestión confiable para la seguridad. Esta norma es la base del proceso de auditoría y certificación de los sistemas de seguridad de información de las organizaciones.

Los Sistemas de Gestión de Seguridad de la Información (SGSI) son el entorno más apropiado de minimizar los riesgos, al asegurar que se identifican y valoran los activos y sus riesgos, considerando el impacto para la organización, y se adoptan los controles y procedimientos más eficaces y coherentes con la estrategia de negocio.
Una gestión para la seguridad de la información debe garantizar:

- La confidencialidad, asegura que sólo quienes estén autorizados puedan acceder a la información.
- La integridad, asegura que la información y sus métodos de proceso son exactos y completos, que garantizan que la información destino es igual a la original
- La disponibilidad, asegura que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

Otro aspecto a considerar es la cuarta revolución industrial la cual está impulsando el cambio y la digitalización a un ritmo acelerado. Las nuevas tecnologías están cambiando las formas tradicionales de hacer negocios, se están abriendo nuevos mercados y con cada innovación, el mundo está vez más conectado digitalmente. A medida que el mundo interconecta, el ciberespacio crece y se mueve en múltiples dimensiones, a través de diferentes disciplinas más allá de las fronteras y entornos de Tecnologías de la información y las comunicaciones de una organización. Con frecuencia, la introducción de nuevos sistemas o productos de TIC en las organizaciones va acompañada de cambios en los procesos comerciales, las responsabilidades. Los empleados afectados por estos cambios enfrentan entornos laborales sociales y técnicos significativamente alterados (Hong, 2018).

6. CONSIDERACIONES FINALES Y CONCLUSIONES

Con el uso de la informática, se han reducido el costo de operación y aumentar la calidad de los servicios ofrecidos. Para proporcionar solo un par de ejemplos, no es de extrañar que hoy se tengan computadoras controlando los autos. Usando computadoras, se pueden tener autos más seguros y eficientes en combustible, y, por no mencionar, más económico de construir, los sistemas de información requieren una herramienta como el computador. (Babiceanu & Remzi, 2019).

Por otra parte, el ciberterrorismo es la capacidad de los terroristas para llevar a cabo acciones terroristas en el ciberespacio con la intención de crear violencia y destrucción o incluso la muerte de su objetivo. Juega con la fuerza conjunta de la psicología, la ideología y la economía para promover un gran miedo en la sociedad. En esencia, los ciberterroristas podrían apuntar a sistemas de infraestructura críticos (p. Ej., Redes eléctricas, suministros de agua y sistemas financieros y bancarios) en el ciberespacio para crear impactos sociales y económicos adversos. (Jian, Yan, & Xin (Robert), 2018). De igual modo la infraestructura critica de una organización puede estár conformada por todo ese conjunto de activos instalaciones, redes, bases de datos, y demás elementos en los que se apoya para el funcionamiento de la organización.

Es así que la Organización para la Cooperación y el Desarrollo Económicos (OCDE), asegura que la ciberseguridad ha pasado a ser una prioridad de la política nacional, que se aborda de una forma cada vez más integral, tomando en consideración aspectos económicos, educativos, legales, técnicos y de soberanía. Un aumento en los ataques de malware en los últimos años ha impuesto serias amenazas a los sistemas y capacidades de misión crítica. El sofisticado malware de día cero es capaz de penetrar en una red y replicar recursivamente nuevas firmas de sí mismo. De esta manera, el malware se propaga rápidamente a través de la red, interrumpiendo las operaciones comerciales y degradando las capacidades del sistema, las organizaciones implementan varios enfoques para defender y proteger su propiedad intelectual digital. Algunas organizaciones invierten la mayoría de sus recursos en sistemas de seguridad perimetral, como firewalls y sistemas de detección de intrusos (IDS), mientras que otras usan recursos para mitigar incidentes. Para resistir los ataques de día cero, un sistema de seguridad perimetral solo es inadecuado; más bien, requiere técnicas avanzadas de detección de día cero y un proceso de recuperación y respuesta a incidentes bien definido que implemente las herramientas de software y hardware adecuadas. (Hiep, Enrique , Pavel, & James, 2016).

Como resultado del Foro de Seguridad de la Información (ISF) se presentaron los 10 desafíos clave involucrados en el equilibrio de los riesgos

y las recompensas del ciberespacio, en base a los conocimientos de los miembros globales de la organización y su propia investigación (Michael, 2014) a saber:

1. Los beneficios y riesgos del ciberespacio son enormes, y los beneficios continuamente impulsan a las organizaciones y empleados a adoptar nuevas formas de interactuar y hacer negocios en línea. Sin embargo, deben poder hacerlo de forma rápida y segura, mientras gestionan el riesgo de entregar las recompensas.

2. Nadie está a salvo de los ataques, por lo que, además de tomar las medidas adecuadas, las organizaciones deben aceptar la incertidumbre y desarrollar lo que podría llamarse resiliencia cibernética. El ritmo de evolución y los posibles impactos de los ciberdelincuentes son tan grandes que la gestión tradicional del riesgo empresarial ahora es insuficiente para enfrentarlo.

3. ISF ha acuñado el término 'malspace' para reflejar una industria global que ha evolucionado para facilitar el cibercrimen. Malspace es una industria grande y altamente funcional que respalda todos los aspectos de la delincuencia moderna: el desarrollo y la venta de herramientas de ataque sofisticadas, servicios y lavado a gran escala de activos robados. Opera a escala y con la sofisticación de otras industrias globales.

4. El impacto de las amenazas cibernéticas puede ser una "cola de riesgo" muy larga y desproporcionada; por ejemplo, una violación de datos de hace años puede ser un "gigante dormido" que puede ser retirado o reactivado en cualquier momento. Los incidentes y las recompensas criminales también se magnifican en el ciberespacio, lo que hace que el impacto de incidencias incluso moderadas sea desproporcionadamente grande.

5. El hacktivismo también presenta amenazas significativas para la organización. Si bien algunas formas pueden ser legales (videos virales, blogs, boicots, campañas de correo electrónico y peticiones), el hacktivismo en todas sus formas puede tener un impacto negativo en las organizaciones seleccionadas.

6. La ciberseguridad es mucho más que solo seguridad de la información. Si bien la función de seguridad de la información tiene muchas de las habilidades necesarias para abordar las amenazas cibernéticas, la organización necesita perfeccionar habilidades adicionales para liderar la carga para mejorar tanto su seguridad como su resistencia cibernéticas.

7. El ciberespacio aumenta enormemente el riesgo de seguridad de la información. Las amenazas a la seguridad de la información son mucho mayores porque el ciberespacio reduce el riesgo de que los delincuentes sean detenidos. Facilita la colaboración, proporciona armas poderosas, concentra objetivos y proporciona una mortaja para ocultar lo que vendrá después.

8. La seguridad de la información es fundamental para la resiliencia cibernética. La mayoría de las ciberamenazas son para la confidencialidad, integridad y disponibilidad (CIA) de información y sistemas. Los fundamentos de seguridad de la información, incluidos los controles, los estándares, el cifrado y la gobernanza, son, por lo tanto, fundamentales para abordar las amenazas del ciberespacio.

9. La complejidad del ciberespacio permite que las amenazas se combinen de formas impredecibles y peligrosas. Del mismo modo que hubiera sido difícil predecir el surgimiento de Anonymous o LulzSec, es difícil predecir qué podría surgir luego del ciberespacio.

10. Cuando se trata de desarrollar resiliencia cibernética, existe un reconocimiento generalizado de que la seguridad y el éxito empresarial no se pueden lograr de forma aislada. Es esencial colaborar, compartir inteligencia y desarrollar las mejores prácticas. Las organizaciones, lideradas por su función de seguridad de la información, deben asociarse con otras funciones internamente y con partes interesadas externas (clientes, proveedores y organismos independientes) para compartir conocimientos y estrategias con el fin de crear resiliencia.

Durante la última década, los ataques cibernéticos han seguido creciendo en sofisticación, alcance e impacto, dejando a las empresas cada vez más expuestas a pérdidas potenciales de importancia significativa. De hecho, no solo pueden incurrir en costos financieros directos (por ejemplo, debido al robo de información corporativa, la interrupción del negocio o el costo de reparar los sistemas afectados), sino también importantes daños a la reputación, que a su vez pueden conducir a la pérdida de clientes, ventas o beneficios y consecuencias legales como multas y sanciones regulatorias por haber comprometido datos personales. Aunque tener una política de gestión de riesgos de ciberseguridad y un plan de respuesta a incidentes es crucial y puede reducir el riesgo de una empresa de estar expuesto y sufrir un ataque cibernético, desafortunadamente es imposible eliminar los riesgos por completo. Como tal, muchas empresas están recurriendo a

las compañías de seguros para garantizar que tengan una protección adecuada contra esos riesgos, ya sea a través de pólizas de seguro generales o específicas de ciberseguridad. (Justine, 2019)

Siendo la seguridad de la información una herramienta para la protección de los activos de la organización contra la interrupción de las operaciones comerciales, la modificación de datos confidenciales o la divulgación de información privada. La protección de estos datos generalmente se describe como el mantenimiento de la confidencialidad, integridad y disponibilidad de los activos, las operaciones y la información de la organización. (Caballero, 2017) La seguridad va más allá de los controles técnicos y abarca a las personas, la tecnología, las políticas y las operaciones de una manera que pocos objetivos comerciales lo hacen

Así mismo La Agencia Europea de Seguridad de las Redes y de la Información (ENISA), es la entidad europea que contribuye al desarrollo de una cultura de red y seguridad de la información para el beneficio de los habitantes, consumidores, empresas y organizaciones del sector público de la Unión Europea contempla diecisiete métodos, para la gestión de la Ciberseguridad y gestión de riesgos. (INTECO, 2014) a saber:

1. **MAGERIT**. “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información”.
2. **OCTAVE**. “Operationally Critical Threat, Asset, and Vulnerability Evaluation” Metodología de Análisis y Gestión de Riesgos desarrollada por el CERT.
3. **Mehari**. Método de Gestión y Análisis de Riesgos desarrollado para soportar sus operaciones
4. **Citicus One**. Software comercial de Citicus, implementa el método FIRM del Foro de Seguridad de la Información.
5. **EBIOS**. Metodología francesa de análisis y gestión de riesgos de seguridad de sistemas de información
6. **CRAMM**. Metodología de análisis y gestión de riesgos desarrollada por el CCTA inglés.
7. **ENISA**. Inventario de metodologías y herramientas de análisis y gestión de riesgos de ENISA (European Network and Information Security Agency).
8. **ENISA – SME**. Guía de evaluación y gestión del riesgo para Pymes.
9. **GxSGSI**. Software de análisis de riesgos, en español, de la empresa SIGEA.
10. **ISO 27005**. Estándar ISO de la serie 27000 dedicado a la gestión de riesgos de seguridad de la información.
11. **UNE-ISO 31000**. Estándar ISO dedicado a la gestión de riesgos.
12. **BS 7799-3:2006.** Estándar británico de gestión del riesgo de la seguridad de la información de British Standards Institution. Guía para la gestión de riesgos de seguridad de la información
13. **NIST SP 800-30.** "Guide for conducting risk assessments". Publicada por NIST (National Institute of Standards and Technology) de EEUU
14. **RiskWatch.** Software no gratuito de realización de análisis de riesgos
15. **IRAM**. Information Risk Analysis Methodologies es una metodología de análisis de riesgos del Information Security Forum sólo disponible para sus miembros.
16. **@RISK. De Palisade**, es un software general de análisis de riesgos basado en la simulación de Monte Carlo. Existe versión en español y tiene coste.
17. **COBRA**. Consultative, Objective and Bi-functional Risk Analysis es un software -no gratuito- de evaluación del riesgo de "C&A Systems Security Ltd."

Al mismo tiempo los nuevos avances las tecnologías de la información y las comunicaciones han impulsado el desarrollo de sistemas de información basados en computadora como una herramienta estratégica para promover el desarrollo socioeconómico, siendo los sistemas de información uno de los principales ámbitos de estudio en el área de organización de empresas. El entorno donde las compañías desarrollan sus actividades se vuelve cada vez más complejo. (Joyanes Aguilar, 2015) Así mismo la creciente globalización, el proceso de internacionalización de la empresa, el incremento de la competencia en los mercados de bienes y servicios, la rapidez en el desarrollo de las tecnologías de información, el aumento de la incertidumbre en el entorno y la reducción de los ciclos de vida de los productos originan que la información se convierta en un elemento clave para la gestión, así como para la supervivencia y crecimiento de la organización empresarial. Si los recursos básicos analizados hasta ahora eran tierra, trabajo y capital, ahora la información aparece como otro insumo fundamental a valorar en las empresas. (Bélanger, Slyke, & Crossler, 2019).

La necesidad de tener Sistemas de Información dentro de cualquier organización o entidad hace que la resiliencia de dichos sistemas sea una prioridad (ISO 22316, 2017) y (Sharma & Kaul, 2018), más aún cuando en el mundo de tecnologías de información (TI), la infraestructura es una prioridad para poder proveer todos los servicios de TI. Partiendo

desde los mismos servidores, sistemas de comunicaciones o de seguridad, sistemas de bases de datos, sistemas de conectividad alámbrica e inalámbrica, son algunas de las aristas que se deben tener presentes para poder tener claridad en un procedimiento de continuidad de negocio a partir de la tecnología, con fin de proveer y mantener una continuidad operacional, a pesar de las fallas que se puedan presentar a nivel físico como lógico. Dentro de toda esta gama de problemas se tienen problemas por sobrecarga en sistemas eléctricos y de alta potencia, fallas en el centro de datos (datacenter), problemas de saturación de canales de comunicación, tráfico malicioso en la organización, amenazas avanzadas a nivel de software, exfiltración de información confidencial, ataques de secuestro digital de información (ransomware), virus, suplantación, denegación de servicios y un largo etcétera que cada día crece más con la necesidad de los delincuentes para poder hurtar o hacer daños a la información como lo define (Alguliyev, Imamverdiyev, & Su, 2018), (Accenture, 2018) y (Tarao & Okamoto, 2016).

En la actualidad es cacofónico hablar de tecnologías disruptivas pues de facto la tecnología rompe con las consideraciones básicas del manejo de información y de la forma de trabajo no solo a nivel de sistemas sino dentro de la resiliencia, la seguridad y el negocio mismo, tal como lo define (Instituto Español de Estudios Estratégicos. , 2015). En este sentido la utilización de dichas herramientas innovadoras tales como inteligencia artificial, aprendizaje de máquina (machine learning), big data, datos abiertos, ciudades inteligentes, AoT – Internet del todo, entre muchas otras invenciones, hace que den un espectro amplio de investigación y desarrollo. (Gunter & Seitz , 2019), (Instituto Español de Estudios Estratégicos. , 2015), (Tyler Technologies, 2017), (Alguliyev, Imamverdiyev, & Su, 2018).

Por tanto, el volver los sistemas proactivos con el fin de que no solo se defiendan sino que tengan la posibilidad de detener los ataques, aprender de estos y adelantar acciones encaminadas a capturar a los implicados, hace que todo lo anterior sean “caballos de troya” en contra de los incidentes de seguridad y una herramienta inexplorada en su totalidad para alcanzar y potencializar procedimientos, sistemas de información y organizaciones, altamente resilientes, como lo expone (Gunter & Seitz , 2019).

Así mimos las organizaciones continúan sufriendo incidentes y ataques a la seguridad de la información como resultado del error humano a pesar de que los humanos son reconocidos como el eslabón más débil con respecto a la información seguridad de la información. Las organizaciones continúan enfocando su atención a los controles técnicos de seguridad en lugar del factor humano y no han incorporado émtodos pormenorizados, como el análisis de confiabilidad humana (HRA), que se utilizan en alta capacidad de sectores como el ferrocarril, la aviación y la energía (Evans Mark, 2018).

A partir de la creciente complejidad y la interconectividad de los sistemas, así como las fallas relevantes debido a imprevistos o eventos impredecibles, requiere un cambio en los sus enfoques de los desarrollos para abordar este problema y utilizar procedimientos que aseguren funciones críticas del sistema cuando estos eventos ocurren, para afrontar este reto los métodos de la seguridad convencional, como el análisis de riesgos, deben utilizarse siempre que sea posible prepararse y prevenir las consecuencias de eventos predecibles. Sin embargo, la resiliencia debe implementarse para garantizar una rápida recuperación y adaptación a un evento adverso. La resiliencia no sirve como sustituto de los principios de diseño de sistemas o análisis de riesgos; más bien se integra como estrategia para mitigar los riesgos e impacto, mejorar. En pro de absorber, recuperar al sistema y posteriormente se adapta a la situación indeseable. (Bastan Ondrej, 2018) Por lo tanto, la seguridad definida en este contexto propende por la reducción del riesgo en la infraestructura crítica de las organizaciones, en aspectos como las intrusiones, ataques cibernéticos, accidentes o desastres.

Como resultado de un estudio realizado por “Ponemon Institute” e “IBM” Resilient sobre la importancia de la resiliencia cibernética para reforzar el estado de la seguridad concluyen que a las organizaciones les sigue costando mucho responder a los incidentes de Ciberseguridad a nivel global. Esto se debe principalmente a la falta de planes formales de respuesta ante incidentes y asignación de presupuestos insuficientes. (Ponemon Institute, 2018) En este sentido una organización ciberresistente reúne las capacidades de ciberseguridad, continuidad y resiliencia empresariales. Aplica estrategias de seguridad fluidas a responder rápidamente a las amenazas, para que pueda minimizar el daño y continuar operando bajo ataque. Como resultado, el negocio ciber resiliente puede introducir estrategias innovadoras y los modelos de negocios de forma segura, fortalecen la confianza del cliente.

En consecuencia, y a manera de conclusiones relevantes, se tienen:

• En la resiliencia cibernética convergen diferentes actores como entidades reguladoras, empresas, así como los hackers y criminales.

• La resiliencia es la capacidad de un actor (individuo u organización) para resistir, responder y recuperarse de incidentes cibernéticos a fin garantizar la continuidad del negocio desde el punto de vista empresarial.

• La necesidad de seguridad cibernética aumenta a medida que los ataques cibernéticos incrementan día a día, éstos son tantos y tan sofisticados que para un sistema de información resiliente se convierte en un gran reto; lo que implica implementar y obtener la resiliencia suficiente necesaria para mantener la prestación de servicios en diversas situaciones.

REFERENCIAS

Accenture. (2018). *THE NATURE OF EFFECTIVE DEFENSE:Shifting from Cybersecurity to Cyber Resilience*. New York: Accenture.

Akashdeep, B., & Sam, G. (2018). Reducing the threat surface to minimise the impact of cyber-attacks. *Network Security, 2018*, 15-19.

Alguliyev, R., Imamverdiyev, Y., & Su, L. (2018). Cyber-physical systems and their security issues. *Computers in Industry*(100), 212-223.

Asia Pacific Economic Cooperation. (2017). *Guía para Desarrollar un Plan de Continuidad de Negocios.* Mexico: Asia Pacific Economic Cooperation.

ATKINS. (2018). *Infraestructura cibernética: Asegurando nuestras capacidades críticas de infraestructura y defensa nacional*. Denmark: ATKINS - HM Government.

Babiceanu, R., & Remzi, S. (2019). Cyber resilience protection for industrial internet of things: A software-defined networking approach. *Computers in Industry, 104*, 47-58.

Babiceanu, R., & Seker, R. (2019). Cyber resilience protection for industrial internet of things: A software-defined networking approach. *Computers in Industry*, 47-58.

Bastan Ondrej, B. T. (2018). Resiliency, the Path to Safety II. *IFAC-PapersOnLine, 51*, 468-472.

Bélanger, F., Slyke, C., & Crossler, R. (2019). *Information Systems for Business.* Burlington: Prospect Press,.

British Standars International. (2014). *BS 11200 : Crisis management. Guidance and good practice*. Londres: BSI.

Caballero, A. (2017). Chapter 24 - Information Security Essentials for Information Technology Managers: Protecting Mission-Critical Systems. En *Computer and Information Security Handbook* (págs. 393-419). Cambridge: Morgan Kaufmann.

Colbaugh, R., & Glass, K. (2011). Proactive defense for evolving cyber threats. *Proceedings of 2011 IEEE International Conference on Intelligence and Security Informatics*, 125-130.

Conrad, E., Misenar, S., & Feldman, J. (2014). Business Continuity and Disaster Recovery Planning. En *Eleventh Hour CISSP: Study Guide.* Amsterdam: Elsevier - Syngress.

Ding, D., Han, Q.-L., Xiang, Y., Ge, X., & Zhang, X.-M. (2018). A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing*(275), 1674–1683.

ESET. (2017). *ESET Security Report Latinoamérica 2017*. ESET.

Evans Mark, H. Y. (2018). computers&security80(2019)74–89Availableonlineatwww.sciencedirect.comjournalhomepage:www.elsevier.com/locate/coseHEART-IS:Anoveltechniqueforevaluatinghuman error-relatedinformationsecurityincidents. *Computer & Security, 80*, 74-89.

EY PERU LIBRARY. (2017). *El camino hacia la resiliencia cibernética. Encuesta global sobre seguridad de información 2016 - 2017*. Lima: EY PERU LIBRARY.

Gunter, D., & Seitz , M. (2019). *A Practical Model for Conducting Cyber Threat Hunting.* Ukraine: SANS Institute.

Hiep, T., Enrique , C.-N., Pavel, F., & James, W. (2016). Cyber resilience recovery model to combat zero-day malware attacks. *Computers & Security, 61*, 19-31.

Hong, S. e. (2018). An analysis of security systems for electronic information for establishing secure internet of things environments. *An analysis of security systems for electronic information for establishing secure internet of things environments*, 18.

Hua, J., Chen, Y., & Luo, X. (2018). Are we ready for cyberterrorist attacks?—Examining the role of individual resilience. *Information & Management*(55), 928–938.

Instituto Español de Estudios Estratégicos. . (2015). *TECNOLOGÍAS DISRUPTIVAS*

Y SUS EFECTOS SOBRE LA SEGURIDAD. España: CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL .

INTECO. (22 de 04 de 2014). *Ciber-Resiliencia Aproximación a un marco de medición.* Recuperado el 28 de 10 de 2019, de https://bit.ly/2JMof2r

International Organization for Standardization. (2018). ISO 31000. Ginebra: ISO.

International Organization for Standardization. (05 de 2019). *ISO 22301*. (ISO) Recuperado el 2019 de 11 de 07, de https://www.iso.org/search.html?q=22031

ISO. (2019). *ISO 22301:2019*. (ISO) Recuperado el 11 de 2 de 2019, de https://www.iso.org/standard/75106.html

ISO 22316. (2017). *Seguridad y resiliencia.* Suecia: ISO-IEC.

ISO. (s.f.). *ISO/IEC 27001 INFORMATION SECURITY MANAGEMENT*. (2015) Recuperado el 1 de 11 de 2019, de https://www.iso.org/isoiec-27001-information-security.html

Jian, H., Yan, C., & Xin (Robert), L. (2018). Are we ready for cyberterrorist attacks?—Examining the role of individual resilience. *Information & Management, 55*(7), 928-938.

Joyanes Aguilar, L. (2015). *Sistemas de Información en la empresa.* México: Alfaomega.

Justine, F. (2019). Cyber insurance – What coverage in case of an alleged act of War? Questions raised by the Mondelez v. Zurich case. *Computer Law & Security Review, 35*(4), 369-376.

Lee, J., Bagheri, B., & Jin, C. (2016). Introduction to cyber manufacturing. *ScienceDirect*(8), 11-15.

Matteo, C., & Valverde, L. (2019). Toward a pluralistic conception of resilience. *Ecological Indicators, 107*, 1-13.

Michael, d. (2014). Building cyber-resilience to tackle threats. *Network Security, 2012*, 5-8.

Ponemon Institute, I. S. (2018). *Tercer estudio anual sobre la ciber-resiliencia empresarial.* Michigan: Ponemon Institute.

Qian, C. (2019). Chapter Three - Toward realizing self-protecting healthcare information systems: Design and security challenges. En *Advances in Computers* (págs. 113-149). Texas: Ali R. Hurson.

Rehak D., S. S. (2017). Evaluation the resilience of critical infrastructure subsystems. *Faculty of Safety Engineering, VŠB-Technical University of Ostrava, Ostrava, Czech Republic*(ISBN 978-1-138-62937-0), 965-962.

Rehak David, H. M. (2015). Failures in a Critical Infrastructure System. En *Dynamic Resilience Evaluation of* (págs. 76-90). Ostrava, Czech Republic: Ministry of the Interior of the Czech Republic.

Rehak David, M. J. (2013). Quantitative evaluation of the synergistic effects of failures in a critical infrastructure system. *International Journal of Critical Infrastructure Protection, 14*, 3-17.

ROMERO, Y. (2014). *Guía general para la elaboración de planes de recuperación de desastres desde el PMI en las áreas de tecnología informática de las empresas pequeñas y medianas en Bogota D.C.* Bogotá: UNIVERSIDAD DE LA SALLE.

Sharma, S., & Kaul, A. (2018). A survey on Intrusion Detection Systems and Honeypot based proactive security mechanisms in VANETs and VANET Cloud. *Vehicular Communications*(12), 138-164.

Strigini, L. (2012). Resilience: What Is It, and How Much Do We Want? *IEEE Security & Privacy, 10*(3), 72-75.

Suárez, H., & Peláez, J. (2018). *Ciber-Resiliencia. Aproximación a un marco de medición.* Instituto Nacional de Tecnologías de la Comunicación.

Symantec. (2014). *THE CYBER RESILIENCE BLUEPRINT: A NEW PERSPECTIVE ON SECURITY.* Mountain View: Symantec.

Tarao, M., & Okamoto, T. (2016). Toward an Artificial Immune Server against Cyber Attacks: Enhancement of Protection against DoS attacks. *Procedia Computer Science: 20th International Conference on Knowledge Based and Intelligent Information and Engineering*(96), 1137 – 1146.

Tyler Technologies. (2017). *A Guide to Cyber Threat Hunting.* Texas: Tyler Technologies.

Wei, D., De Aguiar, L., Collar, B., & Otto, M. (2015). Improving control system resilience by highly coupling security functions with control. *2015 Resilience Week (RWS)*, 1-4.

Yuxia, C., Qing, W., Wenzhi, C., & Bei, W. (2018). Distributed shielded execution for transmissible cyber threats analysis. *Journal of Parallel and Distributed Computing, 122*, 70-80.