MARIANO OSCAR GÓMEZ

EN BUSCA DE UN MODELO DE RESILIENCIA CIBERNÉTICA BASADO EN LAS EXPERIENCIAS DE LA OTAN Y SU POSIBLE TRANSFERENCIA A AMÉRICA DEL SUR

MARIANO OSCAR GOMEZ

En busca de un modelo de resiliencia cibernética basado en las experiencias de la OTAN y su posible transferencia a América del Sur

Editorial Autores de Argentina

Gómez, Mariano Oscar
En busca de un modelo de resiliencia cibernética basado en las experiencias de la OTAN y su posible transferencia a América del Sur / Mariano Oscar Gómez. - 1a ed . - Ciudad Autónoma de Buenos Aires : Autores de Argentina, 2019.
Libro digital, EPUB

Archivo Digital: online
ISBN 978-987-87-0208-7

1. Ensayo Argentino. 2. Seguridad Informática. I. Título.
CDD 658.478

EDITORIAL AUTORES DE ARGENTINA
www.autoresdeargentina.com
Mail: info@autoresdeargentina.com

Diseño de portada: Justo Echeverría
Diseño de maquetado: Maximiliano Nuttini

A mi esposa Guadalupe y a mis hijos María Lucía y Santiago. Un sincero homenaje por el apoyo incondicional y comprensión que me transmitieron durante la realización de la investigación.

Prólogo

Barriendo para casa (*como dicen aquí en España*), mi querida infantería fue sin lugar a dudas el primer arma de los ejércitos, luego aparecieron los caballos, cañones, barcos, los cables y radios, aviones, y hasta un hombre en el espacio. Yo tenía 10 años cuando Neil Amstrong pisó la luna. Hasta hace muy poco, seguía siendo el testimonio irrefutable que la Infantería siempre seguiría siendo el eslabón imprescindible de toda batalla pues, en las guerras que todos hemos estudiado en la historia militar, era el hombre (*infante por cierto…),* el que terminaba pisando ese terreno conquistado.

Hoy entra en juego este quinto escenario o ámbito militar que es el "Ciberespacio" y ya no puedo afirmar nada de lo anterior… ¿Cuál es el rol del soldado en esta batalla, en este escenario?

Al tomar conocimiento de la investigación del Mayor Mariano Gómez, y a su vez el honor de participar en el tribunal de su defensa, pude aprender varias nuevas ideas y reafirmar viejos conceptos que venía elaborando sobre "Ciberdefensa".

En primer lugar no dejo de asombrarme de su visión "global". Es poco frecuente que un militar expanda las fronteras de su Patria para elaborar una línea de pensamiento que aúne un continente entero. Claro, al ir leyendo la profundidad de este trabajo, se pone de manifiesto inmediatamente que su visión no es la clásica de un combatiente, es el enfoque de alguien que ha viajado, conoce diferentes doctrinas, lenguas, fronteras, estrategias y a su vez ha sido capaz de irse embebiendo del lenguaje tecnológico que requiere este

nuevo combate. Cualquiera que se esté capacitando en la línea informática o de telecomunicaciones de seguridad, sabe con total certeza que solo las grandes empresas tecnológicas son capaces de hacer frente técnico a estas nuevas amenazas. Hoy en día las Fuerzas Armadas de un país, de forma aislada, no puede librar este combate. Sin unir esfuerzos, sin alianzas, sin tecnología de punta, sin capacitación técnica, sin un acelerado desarrollo tecnológico, no tienen ninguna probabilidad de éxito.

Lo importante del enfoque de esta investigación, es que, siguiendo una metodología militar en el análisis del problema, documentándose exhaustivamente, analizando en profundidad un hecho concreto en Estonia, llega a conclusiones técnicas en cuanto a su mismo título "Resiliencia", y abre el camino, desafiando a Sudamérica a unir esfuerzos para esta nueva lucha. Evalúa diferentes organizaciones latinoamericanas, siempre bajo la idea de encontrar un curso de acción "UNIDOS", no cada uno por su lado… Esto es ¡brillante! (mis sinceras *felicitaciones Mariano*) es el mejor camino que se puede seguir hoy en día.

Esta idea expuesta queda clara en sus condiciones, motivadas por una serie de encuestas bien planteadas y que lo llevan a la primera de las conclusiones que a mí en particular me interesó, pues va de la mano con mi postura:

"Cooperación estatal, nacional, regional y privada"

Justamente de esto es de lo que estábamos hablando en los párrafos anteriores, a no enfrentar el problema dentro de nuestras fronteras, de nuestros cuarteles. Así no sirve. El militar de hoy, el ingeniero, político, o

estratega privado, debe ser consciente de la necesidad de nutrirse, compartir, apoyarse en estos pilares. No puede seguir creyendo que esta batalla se libra en el terreno, oficina, o entidad gubernamental, esta nueva guerra no tiene fronteras, no tiene enemigos visibles, no tiene declaración de guerra, no tiene teatro de operaciones, no tiene reglas, gloria ni honor. Un párrafo de esta investigación dice "*La diferencia clave entre los dominios físicos y el ciberespacio es que el ciberespacio es artificial y cambiante*". De más está decir que los ataques cibernéticos a nivel nacional que se han sufrido en los últimos años, en NINGUNO de ellos se pudo hacer responsable a un país en concreto de forma oficial, es decir ¿quién atacó oficialmente?, ¿puedo hacer frente a un enemigo que no está declarado?, ¿cómo lo combato?, ¿qué magnitud tiene?, ¿desde dónde me ataca?, ¿qué armas posee?, ¿cuál es su intención, su objetivo, finalidad?.... podríamos plantearnos muchos interrogantes más, pero la conclusión, es la de este trabajo, busquemos: "Cooperación estatal, nacional, regional y privada" pues solos no podremos.

La segunda condición de las dieciséis que propone este trabajo que también me llamó la atención es la que se refiera a:

"Formación de capital humano y especialización"

La condición anterior y esta última, son las que obtienen la mejor puntuación y con diferencia entre las cincuenta y ocho personas encuestadas en este trabajo.

La capacitación humana hoy en día es la clave del éxito, esta batalla se gana más con la mente que con el cuerpo y las armas. Es más, hasta me atrevería a invitaros a reflexionar si no es más importante que la tecnología o

el dinero, pues estamos muy acostumbrados a ver, cada vez con más frecuencia, que una persona desde su propia casa y con mínimos medios, ocasiona ataques o intrusiones a los sistemas más sofisticados, protegidos y caros de nuestro planeta.

Si somos capaces de formar personal, o equipos de trabajo, que tenga esta doble visión: militar-técnica, estaremos creando una generación capaz de volcar la organización y el orden de batalla militar en un escenario eminentemente técnico.

Conociendo la trayectoria del Mayor Mariano Gómez, y su implicación con este tema, no dudo que será uno de los generales del mañana que sabrá conducir por este camino. Además en su perfil personal aplica perfectamente la frase de Confucio:

"El buen líder sabe lo que es verdad; el mal líder sabe lo que se vende mejor"

Y como líder que fue, es y seguirá siendo, estoy seguro que en la búsqueda del verdadero camino de la ciberdefensa latinoamericana romperá barreras burocráticas, fronterizas y de mente, para que se logre enfrentar esta batalla con el horizonte del éxito.

Con el orgullo de haber podido aportar un pequeño grano de arena a este trabajo, y de haber participado del mismo, deseo fervientemente que quien lo lea sepa aprovechar su contenido.

Madrid 2019, Alejandro Corletti Estrada

RESUMEN

Los avances tecnológicos y la creciente infraestructura digital han hecho que poblaciones enteras dependan de sistemas interconectados y complejos, y hoy en día todos los servicios modernos dependen del uso de las Tecnologías de la Información y la Comunicación (TIC). Así es como, con el inevitable aumento de la dependencia tecnológica a nivel mundial, también se haya incrementado la vulnerabilidad a los ataques a las infraestructuras críticas a través del ciberespacio. Un ejemplo de esto fue el ciberataque masivo que sufrió Estonia en 2007 (hasta ese momento considerado uno de los países más desarrollados digitalmente del mundo), que ha tenido un impacto global, permitiendo a la sociedad digital obtener información sobre la nueva amenaza, posibilitando la creación de herramientas y órganos de cooperación entre los estados para hacer frente a esa debilidad poco conocida en esa época. Así surgieron agencias como el Centro de Excelencia Cooperativa de Defensa Cibernética de la OTAN (CCDCOE) y una serie de alianzas relacionadas, que les permitieron establecer normas, crear doctrinas, elevar los estándares de rendimiento cibernético, experimentar con técnicas de empleo y difundir las lecciones aprendidas a todo el mundo. Este documento pretende reforzar la necesidad de definir estrategias para preservar los sistemas propios de los países (especialmente los datos), dada la dificultad de prevenir ataques e identificar sus fuentes. Para delinear posibles estrategias, fueron analizadas un conjunto de medidas implícitas y explícitas adoptadas por el CCDCOE, la OTAN y la UE. El término que abarca esta estrategia es denominado “Resiliencia

Cibernética", y es un concepto de extrema relevancia en el contexto informático actual, siendo que su concepción correcta permitiría a un sistema asumir capacidades suficientes para adaptarse a las acciones hostiles en el ciberespacio (generalmente anónimas e impredecibles), restaurando información hasta momentos antes de esa acción, sin perder capacidades operativas significativas. Para esto, fueron investigadas las condiciones que conducen a la resiliencia de los sistemas cibernéticos, sometiéndolas al análisis de expertos y creando un modelo que podría ser implementado en el marco de América del Sur.

LISTA DE FIGURAS

LISTA DE TABLAS

INDICE

INTRODUCCIÓN

Los avances tecnológicos y la creciente infraestructura digital han hecho que poblaciones enteras dependan de sistemas interconectados y complejos. La demanda de Internet y conectividad digital requiere una creciente integración de las Tecnologías de la Información y la Comunicación (TIC) en productos que anteriormente funcionaban sin tales herramientas, como los sistemas de control de represas; control de tráfico; redes nacionales de salud; distribución de energía, agua y alcantarillado; gestión de transporte multimodal; tráfico aéreo, transacciones bancarias (transferencias, depósitos y pagos) y compras en línea. Hoy, prácticamente todos los servicios modernos dependen del uso de las TIC.

La llegada y la consiguiente evolución del ciberespacio han transformado el mundo y revolucionado la vida cotidiana de sus habitantes. Es un entorno que no tiene límites geográficos y está al alcance de cualquiera (la tecnología es económica). En este escenario, los actores son anónimos, desde adolescentes hasta organizaciones criminales, algunos que operan de manera independiente y otros respaldados por entidades gubernamentales.

Desde esta realidad, y tomando a Estonia como el punto de partida de nuestro análisis, buscaremos comprender las variables que llevaron a este país a constituirse en un estado con resiliencia cibernética, configurando un mecanismo que demuestre su funcionamiento.

Incluso habiendo identificado las variables y sus condiciones, la gran

pregunta sería: ¿cuáles conducen a la resiliencia de un sistema cibernético? Además, ¿por qué Estonia fue elegida como referencia? Con respecto a la primera pregunta, la respuesta será formulada en profundidad a lo largo del presente estudio. En cuanto a la segunda, una respuesta simple y preliminar que se podría dar sería que el ciberataque sufrido por Estonia en 2007 es reconocido como el primer ataque masivo de este tipo en la historia. Este evento marcó el comienzo de lo que hoy se llama guerra cibernética (FERRERO, 2013), y llevó a este país al grado de conciencia situacional sobre la importancia del tema que tiene hoy.

Estonia en ese momento era uno de los países con menor brecha digital[1] en el mundo y uno de los más avanzados en materia de TIC. Sin embargo, su evolución tecnológica fue severamente afectada el 26 de abril de 2007 por una serie de ataques cibernéticos. Estos fueron perpetrados después de la decisión del gobierno local de remover el monumento del Soldado de Bronce de Tallin, un símbolo de la influencia de la Unión Soviética en los países bálticos.

O'Connor (2003) afirma que el Soldado de Bronce es un monumento soviético de la Segunda Guerra Mundial inaugurado en Tallin (Estonia) el 22 de septiembre de 1947 y tiene un valor significativo tanto para los rusos como para la población de Estonia, ya que es un símbolo de la ocupación soviética desde 1940 hasta 1991. Entre 1941 y 1944 Estonia fue ocupada por Alemania en el contexto de la Segunda Guerra Mundial, y las fuerzas soviéticas la recuperaron pasando a formar parte de la Unión de Repúblicas Socialistas Soviéticas hasta 1991.

Según Aviar (2007), en abril de 2007, el gobierno estonio decidió reubicar al Soldado de Bronce y los restos de los soldados soviéticos, después de exhumados e identificados, al cementerio militar de las Fuerzas de Defensa de Estonia en Tallin en medio de controversias en la política interna y externa del país. Estas controversias, externalizadas por manifestaciones, disturbios, medidas de fuerza y tensiones diplomáticas entre países, culminaron en esa sucesión de ataques cibernéticos sin precedentes hasta ahora en la historia.

Czosseck, Ottis y Taliharm (2011) describen que el período de ataques cibernéticos en Estonia se produjo entre el 27 de abril y el 18 de mayo de 2007. Se llevaron a cabo en dos fases: una inicial, entre el 27 y el 29 de abril, caracterizada por el uso de herramientas rudimentarias contra sitios web del Ministerio de Defensa y otras estructuras estatales, así como contra partidos políticos; y la otra fase, del 30 de abril al 18 de mayo, con ataques más complejos y coordinados.

A partir de esto, la OTAN y la Unión Europea ofrecieron apoyo al país, de conformidad con las disposiciones del Tratado de Washington (o Tratado del Atlántico Norte) del 4 de abril de 1949.

Ferrero (2013) afirma que "el ataque cibernético de 2007 contra Estonia [...] representa la primera vez que un Estado miembro solicita el apoyo de la OTAN para un ataque a la infraestructura crítica de información del país" (p.93).

Al final de las operaciones cibernéticas en Estonia, comenzaron a desarrollarse ideas y medidas de cooperación cibernética, como explica

McNamara (2010). Prueba de ello es la creación del Centro de Coordinación de Defensa Cibernética, llamado “Defensa del Tigre”, con sede en Estonia, principal interesada en el tema.

Así, el 14 de mayo de 2008, se creó el CCDCOE (Centro de Excelencia Cooperativo de Defensa Cibernética), inicialmente con los siguientes países miembros: Alemania, Eslovaquia, España, Estonia, Italia, Letonia y Lituania. Con la adhesión de todos estos países, solo cinco meses después, la iniciativa alcanzó el estado de Organización Militar Internacional (TADDEO; GIORIOSO, 2017). En 2010 se incorporó Hungría, en 2011 los Estados Unidos de América y Polonia, en 2012 los Países Bajos y en 2014 Francia, el Reino Unido, la República Checa y Austria (este no miembro de la OTAN).

Corletti Estrada (2017) destaca que el ciberataque recibido por Estonia ha tenido un impacto mundial, haciendo que la sociedad digital sea consciente de la amenaza y la necesidad de que los países cooperen y se vuelvan proactivos sobre el tema cibernético. Basados en este contexto es que comienzan a surgir conceptos como la resiliencia, que abarca diversas áreas disciplinarias, siendo su origen la física.

Ya en el sector estatal e internacional, retomando el razonamiento de Estonia y la OTAN, es posible ver cómo la responsabilidad de los gobiernos en la esfera cibernética es un tema complejo que supera con creces los intereses de las corporaciones privadas. Aun así, el trabajo entre lo privado y lo público, nacional e internacional, civil y militar, en esta área, se traduce en una condición necesaria para lograr la efectividad deseada.

A través de esta integración, la recuperación de Estonia después del ciberataque sufrido, gracias a las medidas tomadas por ese país, la OTAN y, posteriormente, el CCDCOE, se vio materializada.

A partir del análisis bibliográfico abordado en la investigación, las medidas adoptadas por Estonia y la OTAN entre 2007 y 2019, y las consideraciones que podrían haberse tomado, se creó una lista de posibles condicionantes. Todo esto, convenientemente respaldado por la literatura, guiado por el uso de la herramienta metodológica llamada *Process Tracing* (rastreo de procesos), en busca de la creación de un posible modelo de ciber-resiliencia.

Con respecto a esta técnica, Rodrigues y Rodrigues (2017) definen que el rastreo de procesos "consiste en un conjunto de herramientas y pruebas para investigar inferencias causales a partir de datos cualitativos" (p. 2). También, a la luz de Amorim Neto y Rodrigues (2016), se pueden distinguir dos pasos en el método: el primero busca identificar las causas principales (o suficientes) que deberían dialogar con las condiciones necesarias; y el segundo busca instrumentar las medidas para su identificación. Como el enfoque del presente estudio es la identificación de las principales causas para la constitución de un posible sistema cibernético resiliente haciendo un análisis histórico de 2007 a 2019 dentro de la OTAN, el primer paso fue abordado en detalle, dejando la instrumentación de las medidas para futuros estudios.

Para profundizar el modelo deducido, todas las condiciones planteadas fueron sometidas al análisis de 58 especialistas, pertenecientes a 15 países

(Argentina, Brasil, Chile, Uruguay, Paraguay, Perú, Ecuador, Colombia, Guatemala, México, Estados Unidos de América, España, Angola, China y El Salvador), encontrándose representados en esa muestra los siguientes continentes y subcontinentes: América del Sur, América Central, América del Norte, Europa, Asia y África. Estos expertos dieron su visión cuantitativa y cualitativa del problema, y permitieron la identificación de causas necesarias, suficientes, INUS y SUIN, de acuerdo con la categorización que hace Mahoney (2015) al respecto:

- Condiciones necesarias (pero no suficientes): presencia o ausencia del resultado a explicar. Proposición de que un resultado no habría ocurrido en su ausencia, pero también que su presencia no sería suficiente para garantizar el resultado.
- Condiciones suficientes (pero no necesarias): su presencia garantiza el logro o la consumación del resultado a explicar. La presencia de tales condiciones significa la existencia del resultado.
- INUS: parte insuficiente pero necesaria de una condición que en sí misma no es necesaria pero suficiente para el resultado. Es decir, no es necesario ni suficiente.
- SUIN: Causa que es una parte suficiente pero no necesaria de un factor que es insuficiente pero necesario para un resultado.

Finalmente, para aportar contribuciones a Sudamérica que signifiquen una evolución en el asunto, se pretende transferir las políticas de resiliencia cibernética aplicables en el marco da la OTAN a Sudamérica (UNASUR, PROSUL, OEA), utilizando la base teórica llamada *Policy Transfer*

(transferencia de políticas).

La transferencia de políticas se entiende como un proceso en el que el conocimiento de programas, arreglos administrativos, instituciones y el sistema político permite el desarrollo de características similares en otro entorno (BENSON, 2000).

Además de esta visión, la historia muestra que un modelo aplicable a una región puede no funcionar en otra para problemas endógenos y exógenos de ese entorno. Es por eso que, empleando el concepto de transferencia de políticas, y tomando a Dolowitz y Marsh (2000) como referencia, se pretende transferir este patrón a América del Sur.

Si bien este posible modelo de Estonia puede generar resiliencia en otras partes del mundo, puede que no sea factible en América del Sur. En términos de gestión y acceso a recursos materiales, humanos y financieros, no siempre es posible desarrollar la totalidad de modelos complejos.

En relación entonces a los argumentos expuestos, la pregunta propuesta para ser respondida seria: según las prácticas del Centro de Excelencia de Defensa Cibernética Cooperativa de la OTAN, ¿cuáles son las condiciones necesarias que conducen a la resiliencia de los sistemas cibernéticos y cómo pueden transferirse estas prácticas a América del Sur?

---

1 Serrano [et al] (2003) define la brecha digital como "la separación que existe entre las personas (comunidades, estados, países, etc.) que usan las Tecnologías de la Información y la Comunicación (TIC) como parte rutinaria de sus vidas cotidianas y aquellas quienes no tienen acceso a ellos y quienes incluso los tienen no saben cómo usarlos" (p. 175).

CAPÍTULO 1
TEORIZACIÓN DE CONCEPTOS RELACIONADOS

Dada la complejidad de la dimensión en la que se inserta esta investigación, es necesario enmarcar algunos conceptos fundamentales para una mejor comprensión de este problema. Como el foco principal es la posibilidad de construir un modelo de resiliencia cibernética, el primer concepto que se abordará será la "resiliencia" en sí, dentro de su amplio ámbito de aplicación.

Su origen proviene de la física, definida por Corletti Estrada (2017) como "energía de deformación (por unidad de volumen) que puede recuperarse del cuerpo deformado cuando cesa el estrés que causa la deformación" (p. 30). El mismo autor dice, en otras palabras, que sería su límite elástico. Es decir, "una vez que se supera este límite, el material ya no puede recuperarse y se deforma" (p. 31).

Grotberg (2005) entiende que la resiliencia es "la capacidad humana de enfrentar, superar y ser fortalecido o transformado por experiencias de adversidad" (p. 15), mostrando una perspectiva eminentemente afectiva del término, mientras que Infante (2005) la define como "una respuesta global en la que están en juego los mecanismos de protección, entendiéndolos no como variantes contra los factores de riesgo, sino como la dinámica que permite al individuo salir más fuerte de la adversidad en cada situación específica, respetando las características personales "(p. 25), que es una

definición orientada no solo a la dimensión afectiva, sino también a la dimensión procedimental.

En el contexto organizacional, Poletti y Dobs (2007) consideran que la Resiliencia es "un conjunto de cualidades que favorecen el proceso de adaptación y transformación creativa a pesar de los riesgos y las adversidades" (p.13), sin embargo Tavarez (2001) afirma que "la resiliencia es la capacidad de responder de manera más consistente a los desafíos y dificultades del mundo, reaccionando de manera flexible y resistente a estos desafíos y circunstancias desfavorables, con una actitud optimista, positiva y perseverante" (p.35).

Como es visiblemente apreciado, el uso del concepto de resiliencia depende de la estrategia empleada por quien desee utilizarlo, pero la definición que se considerará válida para los fines de la investigación será la formulada por el CERT de Seguridad e Industria, en su trabajo "Resiliencia: Aproximación a una marca de medición" (2018):

> *Cuando un sistema es capaz de soportar todas las presiones sin cambiar su comportamiento, es robusto. Cuando un sistema no puede soportar más presiones, pero puede integrar cambios para disminuirlos y puede seguir adelante, es resiliente al ciberespacio (p. 11).*

Continuando con el razonamiento, la siguiente concepción a tratar será la de "cibernética", ya que constituye la clave esencial para insertar el mencionado principio de resiliencia.

Dado que la cibernética es un término que hoy en día resulta de una

simple deducción por tener una relación directa con las computadoras y las redes, y por estar transcurriendo nuestra sociedad la llamada "era de la información", a continuación se presentarán dos definiciones de autores que tienen contrapuntos bien marcados, lo que permitirá al lector construir una comprensión más profunda del concepto.

Así, Stel (2005), refiriéndose a la aplicación de la cibernética, dice que "incluye psicología, inteligencia artificial, economía, ingeniería de sistemas de control de organismos vivos, máquinas y organizaciones" (p.14), destacando que "al ponerla en movimiento, la información se convierte en un rendimiento o resultado deseado" (p.14).

Por su parte, Van Creveld (2010), con una visión orientada lógicamente al campo militar, dice:

> *La cibernética y las computadoras han traído más que cambios en la administración, la logística, las comunicaciones, la inteligencia y las operaciones, también han ayudado a que un nuevo grupo de personas, que pensaron en la guerra y que planificaron, liberaron y evaluaron, podrían unirse, haciéndose cargo de esto con la ayuda de nuevos criterios y desde un punto de vista completamente nuevo (p. 246).*

De esta manera, Stel enfatiza la importancia de la cibernética en la toma de decisiones que influyen en todos los componentes de un sistema, y Van Creveld se enfoca en el cambio que la cibernética ha generado en cada orden de campaña. Sin embargo, cualquiera de los conceptos presentados resalta claramente la importancia de la cibernética en el mundo de hoy.

En este sentido, la cibernética se inserta en un nuevo entorno que se llama "ciberespacio", que también tiene numerosas definiciones que, juntas,

permiten la comprensión concreta de este término.

Comenzando con Clark y Knake (2011), estos autores afirman que el espacio cibernético está conformado por "todas las redes informáticas del mundo y todo lo que conectan y controlan, no solo Internet" (p.104) incremente esta definición diciendo que el ciberespacio es "Internet más tantas redes de computadoras a las que se supone que no es posible acceder desde Internet" (p.104).

Continuando con este análisis sucinto, es necesario avanzar en las definiciones, abordando una visión más dirigida a la macroeconomía de los estados. Por lo tanto, Sierra (2015) define el ciberespacio como "el conjunto de medios y procedimientos basados en las TIC configurados para la prestación de servicios" (p.16). El mismo autor también hace un acercamiento con respecto a su constitución, diciendo que está conformado por "hardware, software, internet, servicios de información y sistemas de control que garantizan la provisión de esos servicios esenciales" (p.16).

A su vez, Williams (2014), a partir de un detalle casi excesivo del alcance del término, se refiere al ciberespacio como:

> *El dominio artificial creado al conectar todas las computadoras, enrutadores, cables de fibra óptica, dispositivos inalámbricos, satélites y otros componentes que nos permiten mover grandes cantidades de datos a velocidades muy rápidas. Al igual que en los dominios físico, terrestre, marítimo, aéreo y espacial, en el ciberespacio llevamos a cabo una variedad de actividades en beneficio de individuos, gobiernos y entidades comerciales. La diferencia clave entre los dominios físicos y el ciberespacio es que el ciberespacio es artificial y cambiante. Esta característica ofrece oportunidades y riesgos (p. 14).*

Desde un punto de vista más estratégico (seguridad del estado), Llongueras Vicente (2013) define el ciberespacio como "un elemento de poder dentro de la seguridad nacional" (p.1). Esta definición, sorprendente por su contenido y relevancia para el reino cibernético, se basa en su idea de que es un nuevo dominio artificial que ejerce una gran influencia estratégica en nuestra Era, distinguiendo la idea de que los actores más modestos pueden representar amenazas para grandes poderes, y que esta asimetría se basa en el nuevo concepto de operaciones militares centradas en la red.

Al ingresar al ámbito militar y de seguridad, según el Informe de Estrategia de Seguridad Nacional de Estados Unidos de América. 2010, la importancia del ciberespacio es tal que se ha definido como un nuevo "Global Commons[2]" (Gobierno de los Estados Unidos de América, 2011).

Finalmente, Ottis y Lorents (2012), ofrecen un componente que aún no se ha mencionado en las definiciones anteriores, siendo considerado por el autor como esencial para la correcta comprensión del ciberespacio. Los autores consideran el ciberespacio como un conjunto de sistemas de información interconectados dependientes del tiempo donde los usuarios interactúan con otros sistemas. Los autores traen el tiempo como una condición diferenciadora de las otras definiciones presentadas, ya que, en comparación con otros sistemas dependientes del tiempo, se observa que en el ciberespacio, pueden ocurrir cambios radicales en poco tiempo.

Dados los argumentos anteriores, es posible afirmar que la definición de Williams (2014), aunque muy detallada en algunos casos, sumado al concepto de tiempo propuesto por Ottis y Lorents (2012), constituye la

conjunción de conceptos más precisos para explicar el espacio cibernético en lo que hace a esta investigación.

Otro término que deriva y se decanta lógicamente de este enfoque teórico es el concepto de Guerra Cibernética que, según Stel (2005), podría definirse como el uso de las Fuerzas Armadas en el entorno cibernético contra otro actor en un escenario de conflicto, "para atacar sistemas, redes e instalaciones informáticas y de comunicaciones " (p.11).

Este mismo autor agrega a la definición presentada que la confrontación en el ciberespacio implica el uso de la fuerza convencional para complementarla.

Por su parte, Conti y Surdu (2009) abordan la necesidad de capacidad humana y creatividad para acciones cibernéticas exitosas, afirmando que este tipo de guerra requiere "no solo habilidades técnicas, sino también habilidades para resolver los problemas de creatividad, para actuar de manera equilibrada bajo presión y pensamiento crítico " (p.17).

Con una visión más pragmática del tema, Nye y Welch (2013) definen la guerra cibernética como una acción hostil en el ciberespacio cuyos efectos se extienden o son equivalentes a la violencia física relevante, demostrando un propósito manifiesto de dejar en claro cuán devastadora puede ser una guerra en el ciberespacio.

Como acompañamiento esencial del término guerra cibernética, vienen los conceptos de Seguridad Cibernética y Defensa Cibernética, que se abordarán en el mismo orden.

Relacionado con el término ciberseguridad, la bibliografía es muy

amplia, siendo posible entender su evolución a partir del análisis de las definiciones presentadas en un horizonte temporal. Actualmente es necesario establecer conceptos estandarizados por agencias internacionales, con interferencia en el asunto, para mejorar el uso correcto de este término.

Así, por ejemplo, Kemmerer (2003) afirma que la seguridad cibernética consiste, en gran medida, en "utilizar métodos defensivos para detectar y frustrar a posibles intrusos" (p. 707). De hecho, esta definición hoy es más aplicable a la seguridad informática que a la seguridad cibernética.

En este plano, Lewis (2006) se destaca enfatizando que la seguridad cibernética implica la protección de las redes de computadoras y la información contenida en ellas. Este autor comienza a presentar también los conceptos de daño malicioso e intrusión, pero sin la profundización necesaria, al menos en la definición.

Ya en 2008, el órgano denominado Unión Internacional de Telecomunicaciones - UIT, dependiente de las Naciones Unidas, ofrece una definición de seguridad cibernética en la Recomendación UIT-T X.12052 (2008), aprobada en la resolución 1813 (2010), consistente en:

> *La seguridad cibernética es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, pautas, métodos de gestión de riesgos, acciones, capacitación, buenas prácticas, seguros y tecnologías que pueden usarse para proteger los activos de la organización y los usuarios en el entorno cibernético. Los activos y usuarios de la organización son dispositivos informáticos conectados, usuarios y servicios / aplicaciones, sistemas de comunicaciones,*

> *comunicaciones multimedia y toda la información transmitida y / o almacenada en el entorno cibernético. La seguridad cibernética garantiza que las propiedades de seguridad de los activos y usuarios de la organización se cumplan y mantengan frente a los riesgos de seguridad correspondientes en el entorno cibernético.*

Con la evolución gradual de la expresión y el creciente alcance del concepto, el "Informe Especial para la Libertad de Expresión" de la "Comisión Interamericana de Derechos Humanos (CIDH)" de la "Organización de los Estados Americanos (OEA)", estableció en el documento "Libertad de Expresión e Internet (2014)", como salvaguarda de la población, que:

> *El concepto de la seguridad cibernética es comúnmente usado como un término genérico para referirse a diversos temas, desde la seguridad de la infraestructura y las redes nacionales de cualquiera de los cuales ofrece Internet, a la seguridad o integridad de los usuarios. Sin embargo, los acontecimientos posteriores sugieren la necesidad de limitar el concepto sólo para proteger los sistemas y datos informáticos.*

Por su parte, Newmayer (2015) define el término ciberseguridad como "el conjunto de prácticas políticas, capacitación y tecnologías diseñadas para proteger el entorno cibernético con el fin de garantizar la integridad de la información" (p.78).

En el escenario contemporáneo, la "Asociación de Auditoría y Control de Sistemas de Información - ISACA (2018)" aborda una definición de seguridad cibernética que se centra en proteger los activos de información al

abordar aquellas amenazas que podrían poner en peligro cualquier información procesada, almacenada y transportada por sistemas de información.

Por lo tanto, ISO 27001, refiriéndose al significado propuesto por ISACA (2018), define el "activo de información" como: "conocimiento o datos que tienen valor para una organización"; y "sistemas de información" como "que comprende las aplicaciones, servicios, activos de tecnología de la información u otros componentes que permiten su gestión".

Siendo ahora el turno de la defensa cibernética, se podría decir que comienza a definirse dentro de la OTAN en 2010, particularmente en noviembre de ese año, cuando los ministros de defensa de los países miembros, en conferencia, aprobaron la definición y, en junio 2011, la política de defensa cibernética junto con un "Plan de Acción de Defensa Cibernética".

La definición de la OTAN de ciberdefensa, según el "*MC0571-NATO Cyber Defence Concept"*, con referencia al "*National Cyber Security Framework Manual* (2012)" fue: "la aplicación de medidas de seguridad para proteger las infraestructuras críticas de los sistemas de información y comunicación contra ataques cibernéticos" (p. 181).

El mismo documento establece que la defensa cibernética es un marco de seguridad nacional en el que los estados deben tomar ciertas medidas, a todos los niveles (público y privado), ya sea por delitos o garantías y libertades individuales, para responder a todo tipo de agresiones, establecimiento de sistemas de respuesta y cooperación.

El tratamiento más reciente del concepto de defensa cibernética está siendo abordado por el Centro Conjunto de Desarrollo de Defensa (CESEDEN) del Estado Mayor de Defensa en el Reino de España. El CESEDEN (2018) definió lo siguiente:

> *Se considera esencial proporcionar una respuesta integral a las Fuerzas Armadas en su conjunto, y al Ministerio de Defensa en general, en línea con el desarrollo de las políticas existentes del departamento y en estrecha coordinación con los organismos de prestación de servicios y en operación y mantenimiento de redes y sistemas, permitiéndoles abordar de manera efectiva los desafíos importantes que enfrentan. La defensa cibernética como capacidad militar debe estar completamente integrada en todas las áreas de las Fuerzas Armadas y del Ministerio de Defensa en general, así como con el resto de los actores civiles y militares nacionales e internacionales, con quienes se comparten los riesgos y las amenazas. Por otro lado, el factor humano se considera la clave del éxito, referido no solo al personal técnico y operativo involucrado en las actividades del ciberespacio, sino también a todos los usuarios de los servicios que se brindan a través de redes y sistemas (p.6).*

Entrando ya en el marco estructural y conceptual de la investigación, se abordarán términos como cooperación e integración, que representan pilares para la construcción del conocimiento perseguido.

Comenzando con el análisis, la "Agencia Peruana de Cooperación Internacional (2010)" considera la cooperación internacional como un conjunto de acciones y herramientas internacionales para mover recursos e intercambiar experiencias para lograr objetivos comunes. También distingue varios criterios a tener en cuenta para restringir dicha cooperación, tales

como: solidaridad, equidad, eficiencia, sostenibilidad e interés mutuo.

Otro concepto estrechamente relacionado con la cooperación es el Desarrollo, luego del lanzamiento del Programa de las Naciones Unidas para el Desarrollo (PNUD).

En relación con esto, Sunkel y Paz (1981) afirman que la cooperación internacional es un participante en el desarrollo, de la siguiente manera:

> *"[...] crecimiento, el proceso de cambio estructural global, la concepción de desarrollo humano, la teoría de elección racional, entre otras [...] En este sentido, al analizar la Cooperación Internacional, se debe hacer una clara concepción de Desarrollo de un país y los esfuerzos propios que como tal hace para lograrlos [...]" (p. 15).*

Por lo tanto, la cooperación internacional no significa que el actor más desarrollado necesariamente protegerá y ayudará al actor menos desarrollado. Por el contrario, el sistema de cooperación internacional requiere que los actores hagan esfuerzos para lograr los objetivos establecidos y, por lo tanto, creen las condiciones para que dicha cooperación sea viable.

Para ampliar este conocimiento, será abordado ahora el concepto de Integración. Puchala (1972) lo define como un "conjunto de procesos que producen un sistema de acuerdos a nivel internacional, en el que los agentes encuentran posibilidades de armonizar coherentemente sus intereses" (p. 181).

Como contrapunto a la visión anterior, Caporaso y Pelowski (1975) consideran que "la integración consiste en el surgimiento de nuevas

estructuras y funciones en un nuevo nivel más integral de sistemas" (p. 421), y Contreras (1993) afirma que la integración, en sentido estricto, consiste en que "a través de tratados internacionales, dos o más estados ceden algunas de sus prerrogativas soberanas para crear una zona legal independiente de sus miembros" (p. 40).

En esta última definición, el autor centra su atención en la soberanía y el proceso de integración. Lo interesante de estas definiciones es que nos permiten inferir el período histórico en el que fueron construidas.

Por otro lado, Treto (2002) afirma que:

> *"[...] el crecimiento, el proceso de cambio estructural global, el concepto de desarrollo humano, la teoría de la elección racional, entre otros [...] En este sentido, cuando se considera la cooperación internacional, que se debe hacer, a través de una clara concepción de desarrollo de un país y de sus propios esfuerzos, tales como hacer para lograrlo [...] "(p. 15).*

En consecuencia, se puede decir que existe una relación directa entre integración y soberanía, siendo este último reconocido como un principio de derecho internacional, de conformidad con la Carta de las Naciones Unidas (Resolución 2625 de la Asamblea General de las Naciones Unidas), que establece que "todos los estados disfrutan de igualdad soberana, tienen los mismos derechos y deberes, y son miembros similares de la comunidad internacional, a pesar de las diferencias en la naturaleza económica, social, política u otra" (p. 95).

Finalmente, y continuando el sentido conceptual de las definiciones estructurales que sustentan la investigación, es el turno de referirnos a los

modelos (o sistemas), siendo que es lo que se pretende crear.

De esta manera, Shannon (1988) define "Sistema" como un conjunto de objetos o ideas que están relacionados entre sí, como una unidad para el logro de un fin. Al tratarse de una definición clásica más amplia, abordaremos la visión al respecto de Ladrière (1978), que la define como:

> *Una entidad ideal que finalmente posee una cierta estructura interna que puede caracterizarse generalmente en el transcurso del tiempo y que es probable que, en cualquier momento, se encuentre en un estado completamente analizable en principio. Poseer una estructura interna significa que puede descomponerse en otros subsistemas. Además de poseer los diferentes individuos o elementos que lo componen, tiene una serie de funciones y relaciones (p. 39).*

Siendo claramente entendido el concepto de sistemas, ahora es el turno del modelo.

Wartofsky (1983) considera que un modelo es una "versión derivada o representada de algo tomado del original; la nueva entidad se produce imitando la original" (p. 190), alineado esto con la visión de Bravo (1998) quien afirma que "en la perspectiva epistemológica el modelo puede considerarse como una especie de descripción o representación de la realidad [...]"(p. 130).

Continuando con el razonamiento, Ladirère (1978) afirma que "la construcción del modelo está impulsada por una cierta pre-concepción de la realidad estudiada" (p. 39). Según Bravo (1988), "el modelo es frecuentemente susceptible de sistematización" (p. 131).

El mismo autor afirma que "el modelo constituye un método para

ayudar al estudio de la realidad y contribuir a la comprensión de teorías y leyes, sirviendo en algunos casos para verificarlas" (p. 131).

Apoyando el punto de vista anterior, Bisquera (1989) afirma que "el modelo tiene un carácter instrumental" (p. 44), siendo esta última la razón principal de larelevancia del presente estudio.

2 *Global Commons*: espacios que, sin ser de soberanía de una nación en particular, pueden ser aprovechados en beneficio propio por cualquier actor, conforme a las reglas concretas aceptadas internacionalmente.

CAPÍTULO 2
OTAN Y LA RESILIENCIA CIBERNÉTICA

EVOLUCIÓN DE ESTONIA EN EL CAMPO CIBERNÉTICO HASTA EL ATAQUE MASIVO DE 2007

Según los registros históricos existentes proporcionados por el "*Institute of the Estonian Language*", Estonia comenzó a trabajar en el entorno cibernético en 1965 con la instalación de la computadora URAL-1 en la "*Nõo High School"* en la ciudad de Nyo. En ese momento, Estonia todavía estaba bajo el dominio soviético y este fue el primer proyecto de educación computarizado realizado por la Unión Soviética en ese país.

De esta manera, la evolución continuó y en 1967 la Universidad Tecnológica de Tallin recibió su primera computadora Minsk 22, también de origen soviético, y en 1982 se instaló la primera computadora en la Universidad de Tartu (AVIAR, 2007).

Jordan (2003) afirma que en 1989 se introdujo el sistema de redes informáticas FidoNet, una empresa creada a partir de una cooperativa de comunicaciones. Para el año 1990, FidoNet ya tenía alrededor de 30,000 sistemas informáticos conectados con casi 1.56 millones de usuarios.

En el mismo período, la red soviética RELCOM (comunicaciones confiables), hizo la conexión entre los servidores estonios y los servidores finlandeses, siendo el verdadero ícono del desarrollo y el salto tecnológico el

año 1991, oportunidad en la que se declaró la Independencia de la República de Estonia. Con esto, pronto surgió una modernización radical de la infraestructura nacional de telecomunicaciones.

Para García-Ajofrin (2016), a partir de esta situación, el proceso de digitalización de Estonia comienza a crecer llegando en 1996 la implementación del proyecto de innovación llamado "Salto do Tigre", el cual buscaría aumentar las inversiones en tecnologías de información y comunicación a nivel nacional, entre otros éxitos, lo que llevó a que el sistema educativo del país sea apoyado en Internet al proporcionar computadoras en todas las escuelas, un objetivo que se logró en el año 2000.

Según el "Manual Wiley de Ciencia y Tecnología para la Seguridad Nacional (2010)", en 2006 se establecería el "Equipo de Respuesta a Emergencias Informáticas para Estonia (CERT-EE)". La función principal de este organismo sería gestionar incidentes de seguridad en el dominio ".ee".

Pero toda esta evolución tecnológica se habría visto enormemente afectada el 26 de abril de 2007, luego de una serie de ataques cibernéticos perpetrados tras la decisión del gobierno de Estonia de retirar el monumento al Soldado de Bronce de Tallin, monumento que significaba el paso e influencia de la entonces Unión Soviética en los países bálticos.

Otro aspecto relevante que plantea Ferrero (2013) es el descontento ruso producido por la incorporación de Estonia a la OTAN en 2004.

Czosseck, Ottis y Taliharm (2011) describen que el período en el que Estonia fue objeto de ataques cibernéticos fue entre el 27 de abril y el 18 de mayo de 2007, distinguiendo dos fases, una al comienzo de las operaciones,

entre el 27 y el 29 de abril, caracterizado por el uso de herramientas rudimentarias contra sitios web del gobierno (principalmente en el Ministerio de Defensa), estructuras estatales y partidos políticos; y otra fase del 30 de abril al 18 de mayo, con ataques cibernéticos más complejos y coordinados.

De los eventos sufridos, el apoyo internacional en Estonia provino de sus aliados de la OTAN y de la Unión Europea, de conformidad con el Tratado de Washington (o Tratado del Atlántico Norte), de fecha 4 de abril de 1949.

Así, pueden destacarse en los artículos 4 y 5 de dicho tratado los siguientes conceptos:

> *- Artículo 4: las partes consultarán cuando, a juicio de cualquiera de las partes, se vea amenazada la integridad territorial, la independencia política o la seguridad de cualquiera de las partes.*
>
> *- Artículo 5: las partes acuerdan que un ataque armado contra uno o más de ellos, que tenga lugar en Europa o América del Norte, debe considerarse como un ataque dirigido contra todos y, en consecuencia, acuerdan que, si se produce, cada uno de ellos, en el ejercicio del derecho de autodefensa individual y colectiva reconocido por el Artículo 51 de la Carta de las Naciones Unidas, para ayudar a la Parte o Partes atacadas, y luego individualmente, a tomar las medidas que consideren necesarias, incluido el uso de la fuerza armada para restaurar la seguridad en el área del Atlántico Norte. Estas medidas finalizarán cuando el Consejo de Seguridad haya tomado las medidas necesarias para restaurar y mantener la paz y la seguridad internacionales.*

Dado que este tipo de ataques aún no fueron definidos adecuadamente (respecto a si fueron o no acciones militares), la respuesta de los países

involucrados en el Tratado no fue inmediata ni exigible. Inicialmente, la ayuda contrarrestaba las acciones de software malicioso, y luego creció con una entrega gradual de mayor ancho de banda, con la precaución de no liberar en exceso esta capacidad para evitar verse afectados también por dicho ataque.

Finalmente, Ferrero (2013) afirma que el "ataque cibernético contra Estonia en 2007 fue un hito histórico para la OTAN y puede considerarse como la primera acción de guerra cibernética" (p. 93), destacando claramente la magnitud de este evento. El mismo autor también afirma que representó la primera ocasión en que un estado miembro solicitó el apoyo de la OTAN al verse afectada su infraestructura de información crítica. También fue en esta circunstancia que se demostró que la OTAN no tenía un plan de acción para contingencias cibernéticas, lo que condujo a la elaboración de un informe sobre las lecciones aprendidas por esta organización.

MEDIDAS ADOPTADAS POR ESTONIA Y POR LA OTAN DESPUÉS DE LOS ATAQUES CIBERNÉTICOS DE 2007

Para el 19 de mayo, los ciberataques habían terminado, dejando como protagonistas a un atacante desconocido y una víctima totalmente clara e identificada. Aunque sin haber podido identificar al agresor, el Ministro de Asuntos Exteriores de Estonia (Urmas Paet) declaró que el responsable había sido Rusia, sin dejar ninguna duda sobre la postura de Estonia sobre el asunto. Esta acusación ha sido negada por las autoridades rusas, un hecho

que continúa hasta nuestros días (AVIAR, 2007).

Según el informe emitido por el Comité de Bucarest el 3 de abril de 2008[3], en referencia a la reunión de Ministros de Defensa de la OTAN en Bruselas el 14 de junio de 2007, se vio la necesidad de trabajar juntos en ese momento en el marco de la defensa cibernética. Esto llevó a la Organización a establecer medidas de cooperación en esta área.

Relacionado con esto, el artículo 47 de este informe establece:

> *La OTAN sigue comprometida con el fortalecimiento de los sistemas de información clave de la Alianza contra los ataques cibernéticos. Recientemente hemos adoptado una Política de Defensa Cibernética y estamos desarrollando las estructuras y autoridades para implementarla. Nuestra Política de Defensa Cibernética enfatiza la necesidad de que la OTAN y las naciones protejan los sistemas de información clave de acuerdo con sus respectivas responsabilidades; compartir las mejores prácticas; y proporcionar una capacidad para ayudar a las naciones aliadas, previa solicitud, a combatir un ataque cibernético. Esperamos desarrollar aún más las capacidades de defensa cibernética de la OTAN y fortalecer los vínculos entre la OTAN y las autoridades nacionales.*

A partir de la declaración anterior, comenzaron a desarrollarse medidas de cooperación cibernética, como fue el caso, según lo explicado por McNamara (2010), de la creación del Centro de Coordinación de Defensa Cibernética, llamado "Defensa del Tigre", en Estonia.

Así es como Taddeo y Giorioso (2017) hacen una cronología de lo que luego sería la creación del Centro de Excelencia Cooperativa de Defensa Cibernética (CCDCOE), que data del 14 de mayo de 2008. Los países que

iniciaron esta organización fueron Alemania, Eslovaquia, España, Estonia, Italia, Letonia y Lituania, logrando cinco meses después el estatus de Organización Militar Internacional.

Pero la organización continuó creciendo a medida que evolucionó el pensamiento en esta área y los riesgos que evidentemente fueron reconocidos por esta nueva dimensión de la guerra, incorporándose en 2010 Hungría, en 2011 Estados Unidos y Polonia, en 2012 Países Bajos, y en 2014 Austria (no siendo este país miembro de la OTAN), Francia, Reino Unido y República Checa.

Este crecimiento no solo fue militar, económico, político y tecnológico, sino también legal, según lo detallado por Ziolkowski (2013). El autor explica que en 2009, en la ciudad de Tallin, comienza a desarrollarse un manual que ese mismo año tuvo su primera versión (Manual Tallin[4]). Lo que se busca con este documento es, con base en las buenas prácticas en el campo de la cibernética, y en la experiencia adquirida, establecer, a la luz de las bases legales actuales, las reglas de conducta y los procedimientos que se abordarán en caso de un ciberataque.

Tikk, Kaska y Vihul (2010) en un trabajo exhaustivo sobre las consideraciones legales de los incidentes cibernéticos internacionales, detallan que el Manual de Tallin ha buscado (y busca) encontrar una armonía entre el derecho internacional y las responsabilidades de los estados, teniendo en cuenta que los conflictos cibernéticos y esta nueva dimensión desconocida no estaban sujetos a ninguna norma que los respaldara, por lo que intentaron generar una referencia, un vínculo que les permitiera dar un

tratamiento común a los problemas generados al respecto.

Corletti Estrada (2017) destaca que el ciberataque recibido por Estonia ha tenido un impacto mundial, permitiendo a la sociedad digital asumir la nueva amenaza y la necesidad de que los países cooperen y se vuelvan proactivos ante un problema que llegó para quedarse. Por ejemplo, Estonia, que pudo adaptarse rápidamente y superar la adversidad, es actualmente uno de los países con mayor penetración de Internet en el mundo, y puede hacerlo después de haber sufrido en 2007, porque ha creado las condiciones necesarias para la cooperación regional, más allá de haber creado una conciencia situacional adecuada en la población.

COMPONENTES ESENCIALES QUE PODRIAN TRANSFORMAR A UN SISTEMA EN CIBER-RESILIENTE

Para comprender las condiciones que llevaron a Estonia a convertirse en un Estado con una alta tasa de resiliencia cibernética, y su consecuente proyección a los países de Europa, con base en las pautas establecidas por la OTAN, a partir de las buenas prácticas del Centro Cooperativo de Excelencia Cibernética de esta organización, primero debemos identificar las variables que hicieron posible articular este modelo y el mecanismo causal que generó esta eficiencia, particularizando la causa de cada componente según su relevancia.

A partir de un *Process Tracing* histórico de las medidas tomadas por Estonia y la OTAN desde 2007 hasta 2019, y las consideraciones inferidas que podrían haber sido tomadas en cuenta por Estonia y el Centro de

Excelencia Cooperativo de Defensa Cibernética de la OTAN, se elaborará una lista de posibles factores condicionantes, convenientemente respaldados por la literatura, que guiarán el proceso de creación del mecanismo causal deseado.

Centrados en el contexto actual, tanto la OTAN como la UE han estado muy preocupados por la resiliencia, a pesar de que estas dos organizaciones tienen un alcance y responsabilidades diferentes.

La UE se ha centrado más en mejorar la gobernanza de la estructura a nivel local y regional mediante el establecimiento de tres vectores respaldados por la Comunicación de la Comisión al Parlamento Europeo y al Consejo el 3 de octubre de 2012, denominada "Planificación de la UE sobre resiliencia y reducción del riesgo de desastres en los países en desarrollo al aprender de las crisis alimentarias" (UE, 2012). Dichos vectores son:

- Anticipar posibles crisis mediante la evaluación de riesgos, sistemas de alerta temprana y vínculos más estrechos entre la información adquirida y la toma de decisiones a nivel nacional y regional.
- Prevención y preparación, abordando las causas profundas de fragilidad y vulnerabilidad a través del análisis de riesgos.
- Mejorar la respuesta a la crisis mediante el desarrollo de un marco analítico conjunto, identificando las causas fundamentales, los impactos en los grupos de población afectados, evaluando intervenciones, identificando áreas donde el impacto se maximizará, definiendo estrategias y prioridades a corto y largo plazo, y difundiendo experiencias obtenidas de proyectos exitosos.

Es en el año 2013 que la UE lanza su "Plan de Acción de Resiliencia 2013-2020" considerando que la resiliencia es una responsabilidad individual de cada gobierno nacional y, por lo tanto, corresponde a cada uno de ellos definir prioridades políticas, económicas, sociales y cuestiones medioambientales (UE, 2013).

Este plan establece tres fases: una primera que se enfoca en preparar a la sociedad para aumentar su capacidad de recuperación en temas como infraestructura, seguridad, derechos humanos, leyes, recursos, instituciones políticas, comunicaciones, suministros, energía etc; una segunda fase que presupone la ocurrencia del incidente cibernético, en el cual los servicios mencionados anteriormente se ven afectados, tratando en esa fase de enfrentar el desafío y adaptarse a él; y una tercera fase en la que se pretende abordar una recuperación gradual dirigida a alcanzar los niveles perdidos con el incidente lo más rápido posible (UE, 2013).

Preliminarmente, y con base en el análisis de los párrafos anteriores, se podría hacer un enfoque todavía muy incipiente a la distinción de algunas medidas a considerar para construir el modelo de resiliencia cibernética. Estos incluyen: gestión de riesgos y cambios; conocimiento profundo de la organización para poder articular las medidas previstas en la primera y segunda fase; capacidad de anticipar la crisis con organizaciones relacionadas (CERT); necesidad de una regulación oportuna y apropiada sobre infraestructura crítica; determinar las previsiones apropiadas para garantizar procesos continuos y operativos en todas las circunstancias; provisión de una estructura adecuada de sistemas de información (hardware y software); adecuación del marco legal; necesidad de cooperación privada,

estatal, nacional y regional; necesidad de adaptar la formación y especialización del capital humano para enfrentar estos nuevos desafíos; y, finalmente, implementación de estrategias de resiliencia a nivel nacional y regional.

Continuando con el enfoque histórico de las medidas tomadas en Europa para promover la resiliencia cibernética, el primer documento que aborda este tema es el llamado "*Strategic Foresight Analysis 2015"* (OTAN, 2015). Este documento destacó el tema de la resiliencia en las áreas urbanas como un tema relevante para la seguridad nacional teniendo en cuenta la creciente concentración de poblaciones en las ciudades.

En la misma línea, en julio de 2016, se firma el "Compromiso para fomentar la resiliencia" en el Comité de Varsovia (OTAN, 2016). En esa reunión, los mandatarios se comprometieron a continuar fomentando medidas de resiliencia contra las amenazas (incluidas las híbridas) desde cualquier dirección, y determinaron que la resiliencia es esencial para una disuasión y defensa creíbles.

Otro aspecto relevante de este compromiso fue la firma del documento "Requisitos mínimos de la OTAN para la resiliencia nacional", que establece siete áreas críticas principales (OTAN, 2016): continuidad de los gobiernos, suministro de energía, servicios de comunicaciones civiles, suministro de agua y alimentos, capacidad para gestionar grandes movimientos de población, capacidad para gestionar grandes cantidades de víctimas y sistemas de transporte civil.

Dado que se consideró la responsabilidad de cada nación de

implementar las medidas en las áreas anteriores, se establecieron las tareas orientadoras de los esfuerzos nacionales para lograr los estándares de desempeño deseados (OTAN, 2017):

- Desarrollar los recursos humanos para evaluar la vulnerabilidad nacional (redes cibernéticas, la infraestructura crítica, la infraestructura de suministro de energía, etc.).
- Desarrollar una política dirigida a una planificación coherente y gestión de la resiliencia que sea lo suficientemente integral.
- Modificar la legislación para permitir una mayor flexibilidad de acción de los gobiernos en situación de crisis.
- Mejorar la capacidad de las empresas civiles para hacer frente a las crisis.
- Evaluar los documentos de planificación en función de las nuevas amenazas.
- Establecer contacto con otras organizaciones afines para coordinar la acción.

Pero de todo lo que se ha presentado hasta ahora, lo más importante en lo que respecta a los deberes de la OTAN es la cooperación, que se aborda en la "Declaración Conjunta" de julio de 2016 (OTAN - UE, 2016). Este documento enumera pasos específicos para fomentar la cooperación entre la OTAN y la UE, incluyendo defensa cibernética, ejercicios de capacitación, gestión de crisis, cooperación en sí, investigación, capacidades de defensa, entre otros. Uno de los principales es fortalecer la resiliencia de manera

coordinada con expertos para apoyar a los estados miembros de la UE y los aliados de la OTAN.

Entre las políticas de seguridad que presenta el documento, con respecto a la resiliencia cibernética, se podría definir el papel de los CERT, el establecimiento de tareas y misiones de los operadores de infraestructura crítica, el establecimiento de estándares de seguridad públicos y privados, ayuda económica de la OTAN y la UE a los países miembros que no pueden alcanzar los niveles deseados de acuerdo con los estándares de desempeño establecidos, entre otros (OTAN-UE, 2016a).

Finalmente, y de la información presentada, las siguientes medidas clave podrían tomarse en consideración en la formulación preliminar de un posible modelo de resiliencia cibernética basado en las experiencias obtenidas por la OTAN (y la UE) durante el período considerado:

- Gestión de riesgos y cambios.
- Profundo conocimiento de la organización (interna y externamente).
- Área de cibernética con capacidad y participación a nivel gerencial y organización de toma de decisiones.
- Capacidad para anticipar la crisis (CERT).
- Simplificación de los sistemas de información para reducir procesos e interfaces.
- Procesos continuos y operativos bajo cualquier circunstancia.
- Garantizar regulaciones sobre infraestructuras críticas.
- Estructura del sistema de información (hardware y software).

- Desarrollo de ejercicios y modelos de simulación.
- Actualización del marco legal.
- Cooperación privada, estatal, nacional y regional.
- Herramientas de desarrollo y mejora continua de la ciberseguridad.
- Protección física del patrimonio tecnológico.
- Formación y especialización del capital humano.
- Implementación y actualización de estrategias de resiliencia cibernética.
- Suficiente asignación presupuestaria.

Considerando las condiciones planteadas, serán definidos a continuación los conceptos esenciales de cada una a la luz de referencias teóricas:

Gestión de riesgos y cambios. **Medidas preventivas y correctivas:**

Según Beaudoin, Japkowics y Matwin (2009), la gestión de riesgos logra el equilibrio adecuado entre el costo de las medidas adoptadas y el beneficio hipotético de su implementación. Es decir, este tipo de gestión es cuando se trata de amenazas. La gestión del cambio se refiere a la identificación de los cambios a realizar y los impactos organizacionales que deben tenerse en cuenta para un procesamiento adecuado. Es decir, este tipo de gestión es cuando se trata de la evolución de la exposición a eventos externos. Y las medidas preventivas son decisiones que se deben tomar como resultado de la gestión de riesgos que no se han podido prevenir o

anticipar, y que se evitarán en el futuro, y las medidas correctivas son aquellas que se toman para eliminar la causa de un problema.

Profundo conocimiento de la organización (interna y externamente):

Senge (2006) afirma que lograr un conocimiento real y profundo de la organización es una condición fundamental. La resiliencia cibernética requiere adaptabilidad y supervivencia, por lo que es necesario conocer la organización y el entorno. Visión crítica interna y externa de la organización. La organización tiene que programar la redundancia en sus sistemas, sus empleados y sus procesos. Es para evitar exponer cada uno de estos elementos de la organización a la misma amenaza. En conclusión, el balance de riesgos entre todos los elementos de la organización.

Área de cibernética con capacidad y participación a nivel gerencial de toma de decisiones:

De acuerdo con el detalle de las partes componentes de una organización y los niveles que tienen una estructura organizacional que establece Mintzberg (1989), se puede ver que para que un sistema logre su estado de resiliencia, se requiere un liderazgo armonioso y sinérgico en todos los niveles. y componentes de la organización en cuestión. Se necesita capacidad operativa para las medidas cibernéticas (gestión de riesgos, cambio, medidas preventivas y correctivas), la conciencia del personal y el liderazgo adecuado en los niveles más altos de la organización son necesarios para llevar a la acción.

Capacidad para anticipar la crisis (CERT):

Según Newmayer (2015), estas capacidades son la clave para la resiliencia. Los equipos de respuesta a emergencias (CERT) están integrados por especialistas en seguridad cibernética y tienen la responsabilidad de desarrollar acciones preventivas y reactivas a todo tipo de incidentes de seguridad de sistemas informáticos.

Simplificación de los sistemas de información para reducir procesos e interfaces:

Analizando la teoría de la estructura de Pelton y Singh (2015), la base de las arquitecturas de los sistemas materiales y las relaciones humanas debería ser lo más simple posible. Simplificar es un concepto que se refiere a lograr que algo se vuelva más simple, es decir, menos complejo, difícil o complicado. Dada la complejidad inherente de los sistemas informáticos, cuanto más simples sean los sistemas, más pequeños serán los procesos y las interfaces, se generarán menos vulnerabilidades y violaciones de seguridad. Las organizaciones más simples son aquellas con menos procesos, menos unidades, menos sistemas, menos interfaces entre ellas.

Procesos continuos y operativos bajo cualquier circunstancia:

Según Corletti Estrada (2017), cada sistema informático está compuesto por infraestructura, hardware, software y procesos, cada uno con un nivel particular de interferencia, que afecta, en mayor o menor medida, el correcto funcionamiento de la plataforma. Pero todos trabajan sinérgicamente para que puedan convertirse en un sistema resiliente en su conjunto. Pero este proceso debe ser continuo y operarse en todas las circunstancias, distinguiendo los procesos que son esenciales y deben escalar

las prioridades para el momento de la suspensión temporal.

Garantizar regulaciones sobre infraestructuras críticas:

Los autores Rowland, Rice y Shenoi (2014) definen las infraestructuras críticas como aquellas instalaciones y redes, servicios y equipos de tecnología física y de información cuya interrupción o destrucción tendría el mayor impacto en el funcionamiento efectivo de las instituciones estatales y las autoridades públicas. Es por eso que estas infraestructuras críticas deben regularse y estandarizarse adecuadamente para garantizar la protección necesaria.

Estructura del sistema de información (hardware y software):

Según Economy, Powers y Jablonski (2015), es necesario garantizar el diseño de seguridad cibernética de los elementos que respaldan los procesos de la organización. Requisito de compra (hardware y software) de sistemas estandarizados. Funcionalidad y fiabilidad de los sistemas de tecnología de la información y la comunicación.

Desarrollo de ejercicios y modelos de simulación:

Analizando los autores Carayannis y Campbell (2015), la simulación es necesaria para verificar el nivel de resiliencia cibernética del sistema, la efectividad de las medidas tomadas y la evaluación de la velocidad de respuesta, el desempeño de los ejercicios y los modelos de simulación, tanto sea en el interior como en el exterior del sistema.

Actualización del marco legal:

De acuerdo con el Manual de Tallin sobre el derecho internacional

aplicable a la guerra cibernética (2011), es necesario armonizar la legislación ambiental cooperativa de las políticas de seguridad de redes e información, así como el establecimiento de autoridades nacionales para la coordinación y activación del CERT.

Cooperación privada, estatal, nacional y regional:

Richards (2014) desarrolla el concepto de que la cooperación entre las autoridades de seguridad y las agencias es crítica. Promover la cooperación y el intercambio de información entre la industria y los servicios de seguridad cibernética.

Herramientas de desarrollo y mejora continua de la ciberseguridad:

Según Relia (2015), es importante tener en cuenta las herramientas de desarrollo y mejora militar, la inteligencia y las que respaldan sistemas de comunicación estratégicamente importantes. Este último, en cooperación con operadores privados. Para este tipo de herramientas, es deseable que la producción nacional sea tanto para generar el conocimiento como para mejorar el blindaje en la junta local.

Protección física del patrimonio tecnológico:

Donaldson et al. (2014) consideran que los sistemas de infraestructura de seguridad cibernética representan un punto extremadamente vulnerable como accesos al sistema o como partes necesarias para un funcionamiento sin problemas. La protección física de dicho patrimonio tecnológico también es esencial para lograr la resiliencia deseada.

Formación y especialización del capital humano:

De acuerdo con Hough et al. (2015), la formación continua y permanente de capital humano es necesaria para adquirir la experiencia requerida para la tarea. Ambiente profesional calificado con niveles extremos de conocimiento sobre las diferentes cubiertas de seguridad.

Implementación y actualización de estrategias de resiliencia cibernética (ciclo de vida):

Corletti Estrada (2017) considera que estas estrategias deberían aplicarse a la seguridad de redes, nodos y áreas, formando una defensa cibernética en profundidad y altura. Planes de gestión de segmentación y servicios de red. Es decir, todos los procedimientos y acciones que protejan y permitan a la organización volver a un estado operativo en el menor tiempo posible. Luego, será necesario adaptar todo el conjunto de medidas que están disponibles para la organización a intervalos apropiados.

Suficiente asignaciónpresupuestaria:

En referencia a esta condición, la mayor parte de la bibliografía consultada refuerza la necesidad de contar con un presupuesto adecuado para la renovación y actualización de recursos humanos y materiales continuamente para garantizar la resiliencia de los sistemas cibernéticos.

---

3 Issued by the Heads of State and Goverment participating in the meeting of the North Atlantic Council in Boucharest on 3 April 2008.

4 El Manual Tallinn es un documento académico, no vinculante, que trata sobre la aplicación de la ley internacional de los conflictos en el ámbito cibernético. Dicho manual fue desarrollado por el Comité del CCDCOE de la OTAN, en Estonia (SCHMITT, 2013).

CAPÍTULO 3

EN BUSCA DE UN MODELO DE RESILIENCIA CIBERNÉTICA

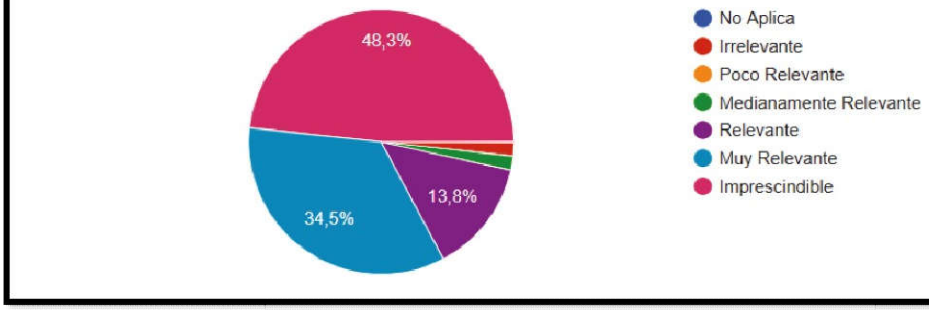
Teniendo en cuenta las condiciones identificadas en el capítulo anterior, se pretende consolidar un modelo de resiliencia cibernética a partir de la evaluación de expertos en el campo cibernético (58 en total, pertenecientes a los siguientes países: Argentina, Brasil, Chile, China, Colombia, El Salvador, Ecuador, España, Estados Unidos de América, Guatemala, México, Paraguay, Perú, Uruguay). Esta evaluación fue realizada a partir del análisis de una serie de cuestionarios completados por cada uno de los especialistas, teniendo como objetivo explorar los resultados obtenidos para extraer conclusiones de validez que permitan establecer las condiciones causales resultantes.

A continuación se presentarán los resultados cuantitativos de la evaluación realizada por los especialistas, discriminando cada condición identificada como un posible componente de un modelo de resiliencia cibernética y su respectiva valoración, considerando las variables en función de una ponderación en el orden de 7 (indispensable) y 1 (no aplicable).

FIGURA 1 - Resultados cuantitativos de los cuestionarios a expertos.

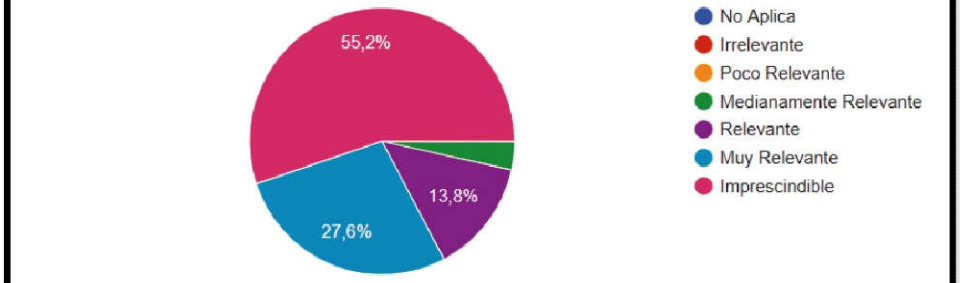
1. Condición: gestión del riesgo y de cambio.

58 respuestas



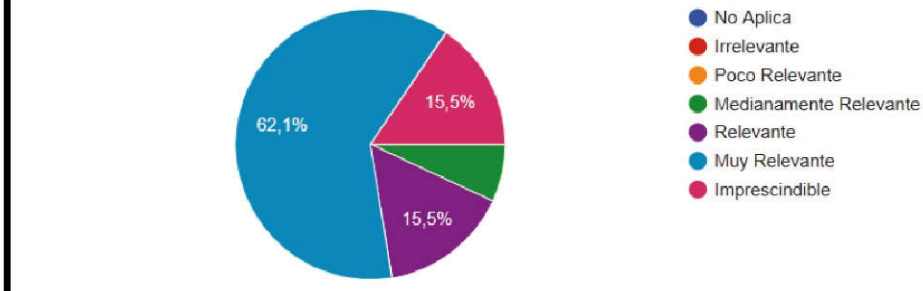
2. Condición: conocimiento profundo de la organización (interno y externo).

58 respuestas



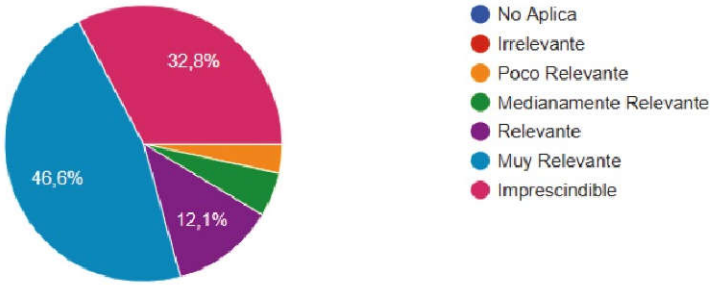
3. Condición: área de cibernética con capacidad y participación en la organización en el nivel gerencial y de toma de decisiones.

58 respuestas



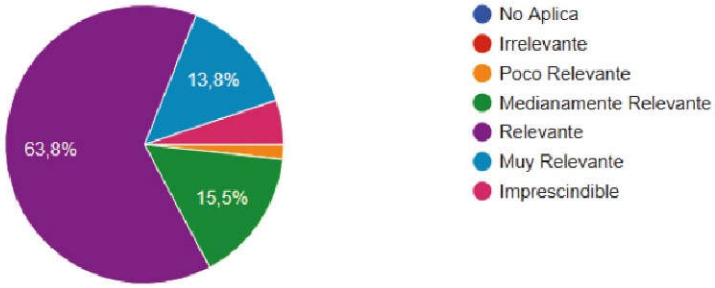
4. Condición: Capacidad para anticipar la crisis (CERT).

58 respuestas



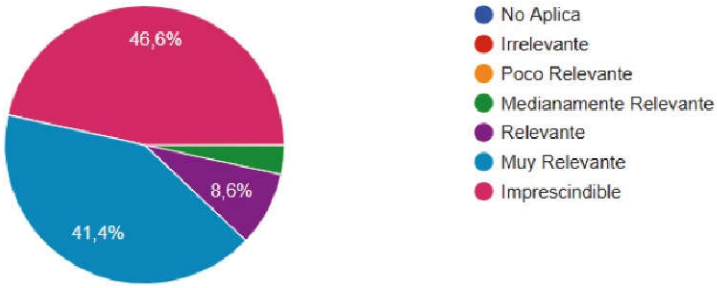
5. Condición: La simplificación de los sistemas de información para reducir los procesos e interfaces.

58 respuestas



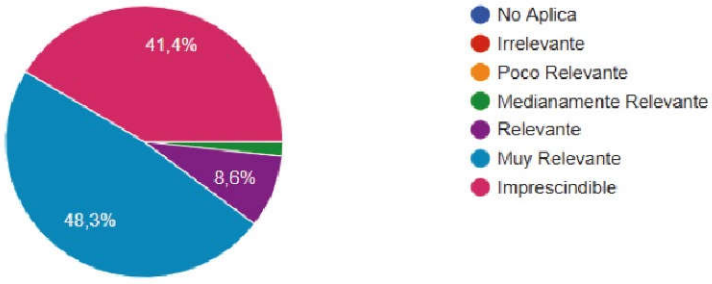
6. Condición: procesos continuos y operativos en todo momento.

58 respuestas



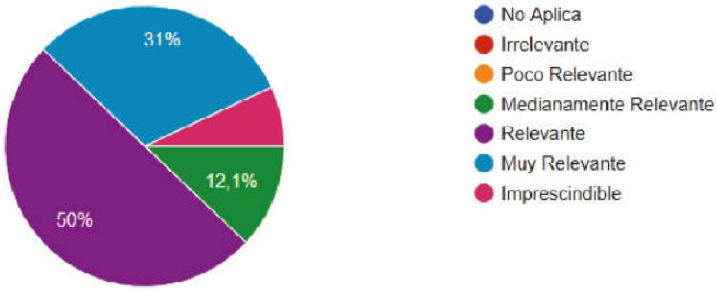
7. Condición: Garantizar la normativa sobre la infraestructura crítica.

58 respuestas



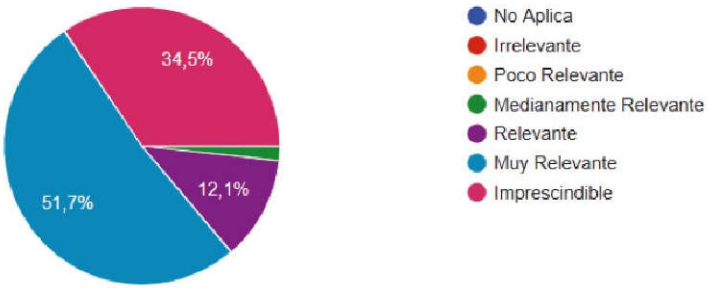
8. Condición: estructura del sistema de información (hardware y software).

58 respuestas



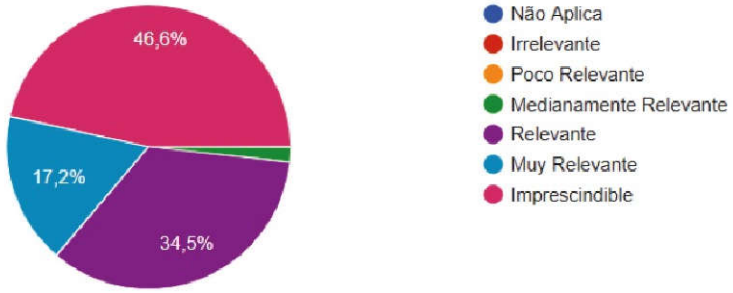
9. Condición: desarrollo de ejercicios y modelos de simulación.

58 respuestas



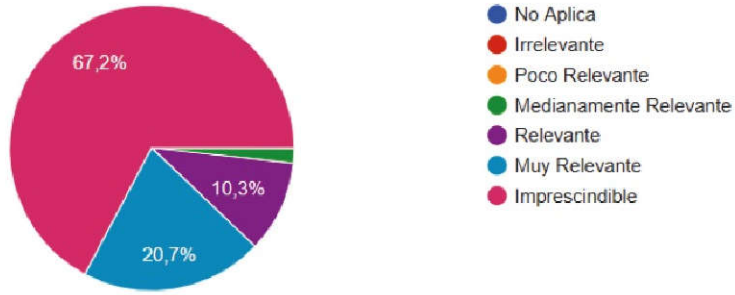
10. Condición: actualización del marco legal.

58 respuestas



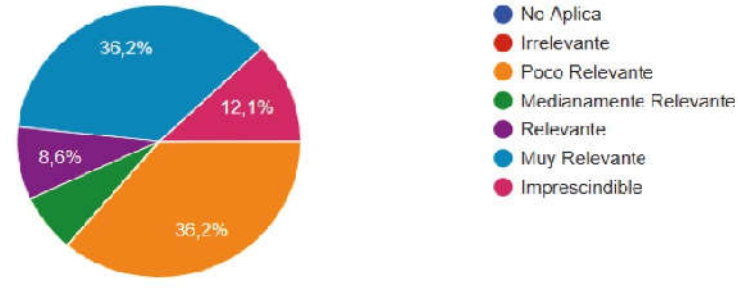
11. Condición: cooperación privada, estatal, nacional y regional.

58 respuestas



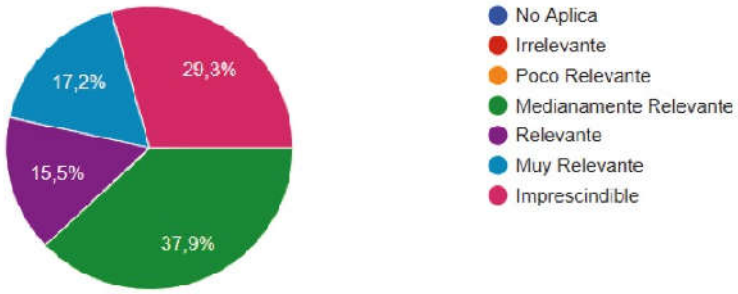
12. Condición: herramientas de desarrollo y mejora continua de seguridad cibernética.

58 respuestas



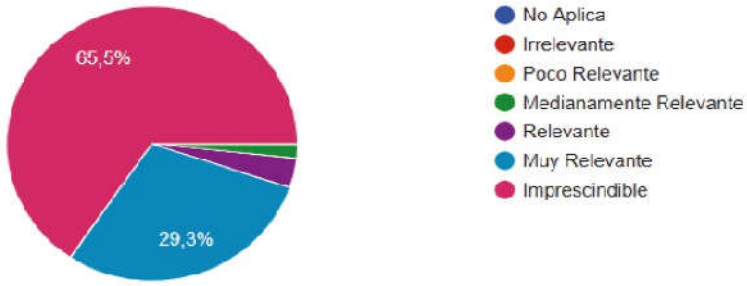
13. Condición: la protección física del patrimonio tecnológico.

58 respuestas



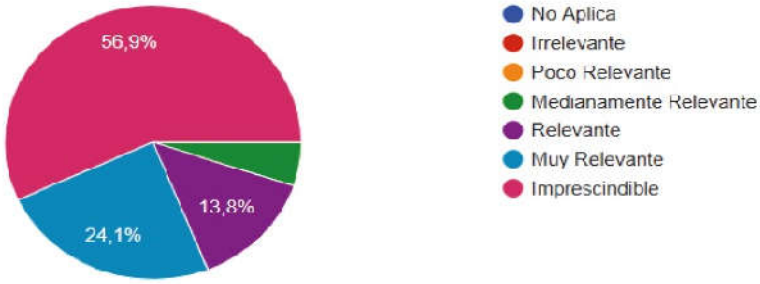
14. Condición: formación y experiencia del capital humano.

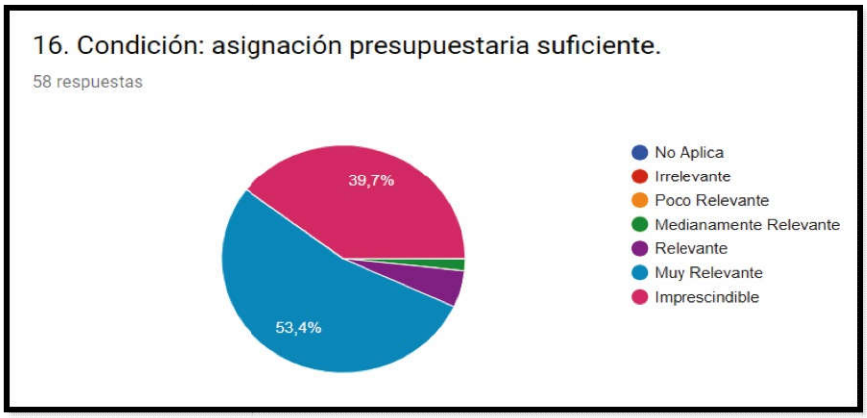
58 respuestas



15. Condición: implementación y actualización de las estrategias de resiliencia cibernética (ciclo de vida).

58 respuestas





Fuente - El autor.

Para un mejor análisis y visualización de los resultados en cuanto a los aspectos ponderados cuantitativamente por los especialistas, se presenta a continuación un cuadro resumen:

TABLA 1 - Cuadro resumen de los resultados de los cuestionarios a expertos

Condición / Asunto	
Condición 1	Gestión de riesgo y de cambio
Condición 2	Profundo conocimiento de la organización (interno y externo)
Condición 3	Capacidad y participación en el nivel gerencial y de toma de decisiones de la organización
Condición 4	Capacidad para anticiparse a la crisis (CERT)
Condición 5	Simplificación de los sistemas de información para reducir los procesos e interfaces
Condición 6	Procesos continuos y operativos en todas las circunstancias
Condición 7	Garantizar las regulaciones sobre las infraestructuras críticas
Condición 8	Estructura del sistema de información (hardware y software)
Condición 9	Desarrollo de ejercicios y modelos de simulación
Condición 10	Actualización del marco legal
Condición 11	Cooperación estatal, nacional, regional y privada
Condición 12	Herramientas de desarrollo y mejora continua de la seguridad cibernética
Condición 13	Protección física del patrimonio tecnológico
Condición 14	Formación de capital humano y especialización
Condición 15	Aplicación y actualización de estrategias de resiliencia cibernética (ciclo de vida)
Condición 16	Asignación presupuestaria suficiente

Condición	Porcentajes y Ponderaciones														TOTAL
	Imprescindible(%)	Coef 7	Muy Relevante (%)	Coef 6	Relevante (%)	Coef 5	Medianamente Relevante (%)	Coef 4	Poco Relevante (%)	Coef 3	Irrelevante (%)	Coef 2	No aplica (%)	Coef 1	
Nº 1	48,3	338,1	34,5	207	13,8	69	1,7	6,8	0	0	1,7	3,4	0	0	624,3
Nº 2	55,2	386,4	27,6	165,6	13,8	69	3,4	13,6	0	0	0	0	0	0	634,6
Nº 3	15,5	108,5	62,1	372,6	15,5	77,5	6,9	27,6	0	0	0	0	0	0	586,2
Nº 4	32,8	229,6	46,6	279,6	12,1	60,5	5,2	20,8	3,4	10,2	0	0	0	0	600,7
Nº 5	5,2	36,4	13,8	82,8	63,8	319	15,5	62	1,7	5,1	0	0	0	0	505,3
Nº 6	46,6	326,2	41,4	248,4	8,6	43	3,4	13,6	0	0	0	0	0	0	631,2
Nº 7	41,4	289,8	48,3	289,8	8,6	43	1,7	6,8	0	0	0	0	0	0	629,4
Nº 8	6,9	48,3	31	186	50	250	12,1	48,4	0	0	0	0	0	0	532,7
Nº 9	34,5	241,5	51,7	310,2	12,1	60,5	1,7	6,8	0	0	0	0	0	0	619
Nº 10	46,6	326,2	17,2	103,2	34,5	172,5	1,7	6,8	0	0	0	0	0	0	608,7
Nº 11	67,2	470,4	20,7	124,2	10,3	51,5	1,7	6,8	0	0	0	0	0	0	652,9
Nº 12	12,1	84,7	36,2	217,2	8,6	43	6,9	27,6	36,2	108,6	0	0	0	0	481,1
Nº 13	29,3	205,1	17,2	103,2	15,5	77,5	37,9	151,6	0	0	0	0	0	0	537,4
Nº 14	65,5	458,5	29,3	175,8	3,4	17	1,7	6,8	0	0	0	0	0	0	658,1
Nº 15	56,9	398,3	24,1	144,6	13,8	69	5,2	20,8	0	0	0	0	0	0	632,7
Nº 16	39,7	277,9	53,4	320,4	5,2	26	1,7	6,8	0	0	0	0	0	0	631,1

Fuente - El autor.

El razonamiento utilizado para la elaboración de la tabla precedente es el siguiente:

- En cada columna que responde a las variables de porcentaje alcanzado, se colocó el valor atribuido según los datos presentados como Figura 1.
- Fueron aplicados coeficientes del 1 al 7 considerando la relevancia que tiene la condición considerada para la constitución del modelo. Por lo tanto, el que tiene menos relevancia (no se aplica) recibió el

valor 1, y el que tiene el valor más alto (indispensable) 7.

- Los valores porcentuales de cada condición se multiplicaron por los coeficientes mencionados anteriormente, y en la última columna (Total) se sumaron todos los productos, obteniendo el valor de ponderación final asignado a cada condición.

Para clasificar los valores obtenidos, se identificaron cuatro niveles de relevancia de acuerdo al siguiente detalle:

- **Primer nivel**, que implica los pesos más altos y, en consecuencia, las condiciones que se considerarán como "necesarias" para constituir el modelo de resiliencia cibernética (MAHONEY, 2010). Para encuadrar este nivel se han considerado valores entre 658,1 a 619, encontrándose presentes entonces las siguientes condiciones:
  - Condición 1: gestión de riesgos y cambios.
  - Condición 2: conocimiento profundo de la organización (interna y externamente).
  - Condición 6: procesos continuos y operativos bajo cualquier circunstancia.
  - Condición 7: garantizar regulaciones de infraestructura crítica.
  - Condición 9: desarrollo de ejercicios y modelos de simulación.
  - Condición 11: cooperación privada, estatal, nacional y regional.
  - Condición 14: formación y especialización del capital humano.

- Condición 15: implementación y actualización de estrategias de resiliencia cibernética (ciclo de vida).
- Condición 16: asignación presupuestaria suficiente.

- **Segundo nivel**, que involucra aquellas condiciones cuyos pesos, no siendo los más altos, representan tal relevancia que no podrían descartarse del modelo. Por lo tanto, formarán parte como una sub-condición de algunas de las condiciones enumeradas como primer nivel. Los valores contenidos en este nivel se encuentran entre 618 y 580, y los siguientes componentes estarán contenidos en esta categoría:
  - Condición 3: área de cibernética con capacidad y participación a nivel de gestión de toma de decisiones en la organización.
  - Condición 4: capacidad para anticipar la crisis (CERT).
  - Condición 10: actualización del marco legal.
- **Tercer nivel**, que implica aquellas condiciones que se aprecia no se consideran muy relevantes, pero que podrían articularse para contribuir de alguna manera a la constitución del modelo, sin ser suficientes ni necesarias como tales. Los valores contenidos en este nivel se encuentran entre 579 y 530, distinguiéndose los siguientes componentes en esta categoría:
  - Condición 8: estructura del sistema de información (hardware y software).
  - Condición 13: protección física del patrimonio tecnológico.

- **Cuarto nivel**, que involucra aquellas condiciones que, debido al bajo peso dado por los especialistas, no cumplen con el requisito de un modelo cibernético resiliente, causa por la cual serán descartados del proceso. Los valores contenidos en este nivel están entre 530 y 480, identificándose los siguientes componentes en esta categoría:
  - Condición 5: simplificación de los sistemas de información para reducir procesos e interfaces.
  - Condición 12: herramientas de desarrollo y mejora continua de la ciberseguridad.

Del análisis anterior es posible extraer una clasificación preliminar de condiciones, sub-condiciones y componentes de la siguiente manera:

TABLA 2 – Modelo preliminar de condiciones, sub-condiciones y componentes.

N°	Condición	Sub-condición	Componente	Observaciones
1	Gestión de riesgo y de cambio.			--
	1. a	Capacidad de anticipar la crisis (CERT)		Ex Condición 4
2	Conocimiento profundo de la organización (interna y externa)			--
	2. a	Área de cibernética con capacidad y participación en el nivel de la organización gerencial y de toma de decisión.		Ex Condición 3
3	Procesos continuos y operacionales en cualquier circunstancia.			Ex Condición 6
		-	Estructura del sistema de información (hardware e software)	Ex Condición 8
		-	La protección física del patrimonio tecnológico	Ex Condición 13
4	Garantizar regulación en las infraestructuras críticas.			Ex Condición 7
5	Desarrollo de ejercicios y modelos de simulación.			Ex Condición 9
6	Cooperación privada, estadual, nacional e regional			Ex Condición 11
	6. a	Actualización del marco legal.		Ex Condición 10
7	Formación y especialización del capital humano.			Ex Condición 14
8	Implantación y actualización de las estratégicas de resiliencia cibernética (ciclo de vida).			Ex Condición 15
9	Dotación presupuestaria suficiente.			Ex Condición 16

Fuente - El autor.

Como otro aspecto constitutivo del análisis, y a partir de una visión cualitativa, fueron exploradas las respuestas presentadas por los expertos con respecto a las otras condiciones que sería conveniente incluir para la creación de un modelo ciber-resiliente, contribuyendo a la mejora del mismo. A partir de allí, los aspectos más relevantes que fueron levantados para el presente estudio son:

TABLA 3 - Temas o condiciones más relevantes obtenidos de la contribución de los expertos.

Concepto general	Resumen de las opiniones de los expertos
Establecer estándares de desempeño, control, desafío y respuesta	• Establecimiento de atributos de calidad basados en estándares. • Establecimiento de controles críticos de seguridad y auditorías periódicas de resiliencia. • Evaluación de sistemas a través de indicadores, basados en diagnósticos continuos y métricas apropiadas. • Respuesta a amenazas automatizada.
Estandarización de protocolos y sistemas a nivel nacional y regional	• Establecimiento de una Estrategia Nacional de Cibernética que integre todos los componentes estatales que contribuyan a la cooperación entre los sectores público y privado. • Existencia de un glosario común estandarizado de términos relacionados con el ambiente cibernético para fomentar la cooperación. • Estandarización de sistemas a nivel estatal (infraestructura, software, procedimientos y políticas asociadas).

Concepto general	Resumen de las opiniones de los expertos
Cooperación, confianza e integración nacional y regional, pública y privada	• Disponibilidad de una plataforma común para compartir datos y firmas digitales de ataques cibernéticos (centros tecnológicos unificados). • Redundancia, segmentación de información y cooperación. • Necesidad de crear un ambiente de confianza mutua entre las organizaciones de defensa cibernética.
Protección de activos críticos	• Trazabilidad adecuada para cualquier incidente de seguridad cibernética. • Fomentar el desarrollo de software seguro en la organización. • Clasificación clara y priorización de los activos a proteger.
Área de gestión de personas y conciencia situacional en la población	• Formación adecuada en ingeniería social a todos los niveles. • Conciencia de la organización en todos los niveles de toma de decisiones y en la sociedad sobre la importancia de la cibernética. • Preparar al público en diferentes niveles para convivir con sistemas cibernéticos. • Lealtad del personal vinculado a las áreas de ciberdefensa, seguridad informática y sistemas. • Establecimiento de un equipo multidisciplinario con las siguientes capacidades: inteligencia, contrainteligencia, gestión de riesgos, estudios de seguridad física e informática, programación, auditorías.

Fuente- El autor.

Teniendo en cuenta la pertinencia, y con la intención de consolidar la información proporcionada por los especialistas, los temas presentados anteriormente fueron clasificadas en sub-condiciones y componentes del

modelo, de la siguiente manera:

TABLA 4 - Categorización de las opiniones de los expertos.

Categoria	Resumen de condiciones
Sub-condiciones	• Establecimiento de atributos de calidad basados en estándares e indicadores, en diagnósticos continuos y métricas apropiadas. • Establecimiento de una estrategia cibernética nacional. • Estandarización de sistemas a nivel estatal (infraestructura, software, procedimientos y políticas asociadas). • Clasificación clara y priorización de los activos a proteger.
Componentes	• Establecimiento de controles críticos de seguridad y auditorías periódicas de resiliencia. • Fomentar el desarrollo de software seguro en la organización. • Capacitación adecuada en ingeniería social y conciencia de la organización, todos los niveles de toma de decisiones y en la sociedad sobre la importancia de la cibernética. • Disponibilidad de una plataforma común para compartir datos y firmas digitales de ataques cibernéticos (centros tecnológicos unificados). • Trazabilidad adecuada para cualquier incidente de seguridad cibernética. • Existencia de un glosario común estandarizado de términos relacionados con el ambiente cibernético para fomentar la cooperación. • Respuesta a amenazas automatizada. • Redundancia, segmentación de información y cooperación. • Necesidad de crear un ambiente de confianza mutua entre las organizaciones de defensa cibernética. • Lealtad del personal vinculada a las áreas de ciberdefensa, seguridad informática y sistemas. • Establecimiento de equipos multidisciplinarios con las siguientes capacidades: inteligencia, contrainteligencia, gestión de riesgos, estudios de seguridad física e informática, programación, reclutamiento, auditoria.

Fuente- El autor.

Finalmente, al alimentar el sistema con las sub-condiciones y componentes extraídos de la experiencia de los expertos, el modelo de resiliencia cibernética consecuente es el siguiente:

TABLA 5 – Modelo final de condiciones, sub-condiciones y componentes necesarios para que un sistema sea considerado como ciber-resiliente.

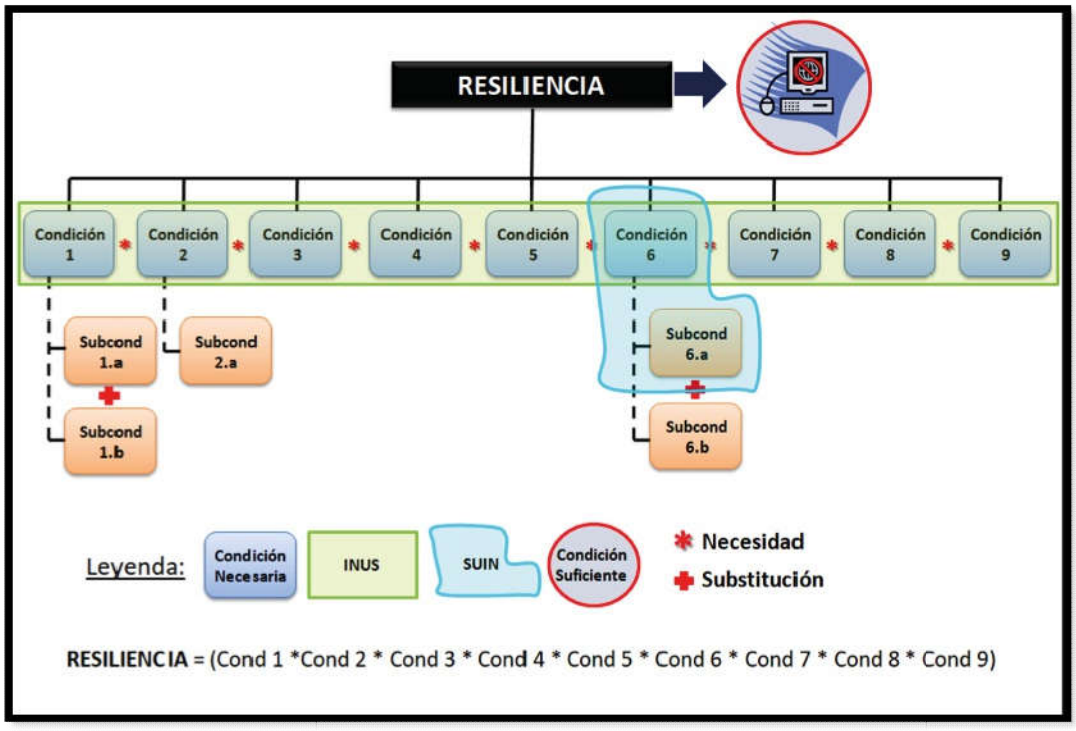
Nº	Condición	Sub-condición	Componente	Observaciones
1	Gestión de riesgo y de cambio.			--
		1. a	Capacidad de anticipar la crisis (CERT)	Ex Condición 4
		1. b	Establecimiento de atributos de calidad basados en estándares e indicadores, a partir de diagnósticos continuos y métricas adecuadas.	Especialistas
			- Adecuada capacidad de rastreabilidad ante cualquier incidente de seguridad cibernética.	Especialistas
			- Automatización de respuestas a amenazas	Especialistas
2	Conocimiento profundo de la organización (interna y externa)			--
		2. a	Área de cibernética con capacidad y participación en el nivel de la organización gerencial y de toma de decisión.	Ex Condición 3
			- Formación adecuada en ingeniería social en todos los niveles y concientización de la organización, de todos los niveles de toma de decisión y de la sociedad sobre la importancia de la cibernética.	Especialistas

3	Procesos continuos y operacionales en cualquier circunstancia.		Ex Condición 6
	-	Estructura del sistema de información (hardware e software)	Ex Condición 8
	-	La protección física del patrimonio tecnológico	Ex Condición 13
	-	Incentivo al desarrollo seguro de software en el sector de programación de la organización.	Especialistas
	-	Establecimiento de controles de seguridad críticos y auditorias periódicas relativas a la resiliencia.	Especialistas
	-	Redundancia, segmentación de la información y cooperación.	Especialistas
4	Garantizar regulación en las infraestructuras críticas.		Ex Condición 7
	-	Estandarización de los sistemas a nivel Estado (infraestructura, software, procedimientos y políticas asociadas)	Especialistas
	-	Clara categorización y priorización de los activos a proteger.	Especialistas
5	Desarrollo de ejercicios y modelos de simulación.		Ex Condición 9
6	Cooperación privada, estadual, nacional e regional		Ex Condición 11
6. a	Actualización del marco legal.		Ex Condición 10
6. b	Establecimiento de una estrategia nacional de cibernética.		Especialistas
	-	Existencia de un glosario común estandarizado de términos relacionados con la cibernética para favorecer la cooperación.	Especialistas
	-	Necesidad de crear un ambiente de confianza mutua entre las organizaciones orientadas a la defensa cibernética.	Especialistas

7	Formación y especialización del capital humano.		Ex Condición 14
		- Formación del personal vinculado a las áreas de defensa cibernética, seguridad informática y sistemas.	Especialistas
		- Construcción de equipos multidisciplinarios.	Especialistas
8	Implantación y actualización de las estratégicas de resiliencia cibernética (ciclo de vida).		Ex Condición 15
		- Disponibilidad de una plataforma común para compartir datos y firmas digitales de agresiones cibernéticas.	Especialistas
9	Dotación presupuestaria suficiente.		Ex Condición 16

Fuente - El autor.

FIGURA 2 – Esquematización de las condiciones causales obtenidas del proceso de análisis de evidencias.



Fuente - El autor.

En la figura anterior, elaborado a la luz de Mahoney (2010), es posible identificar cómo las 9 variables consideradas como principales constituyen cada una de ellas una **condición necesaria**, ya que la resiliencia no se puede obtener en ausencia de alguna de ellas, aunque también, con su sola presencia individual, no es suficiente para garantizar el resultado.

En este mismo razonamiento, la fórmula "RESILIENCIA = (Cond 1 * Cond 2 * Cond 3 * Cond 4 * Cond 5 * Cond 6 * Cond 7 * Cond 8 * Cond 9) " donde el vector " * " es un enlace de necesidad (es decir, estas condiciones no pueden estar ausentes de la ecuación) para determinar que este conjunto de variables conectadas constituye una **condición INUS**, ya que podría definirse que es una parte insuficiente pero necesaria de una condición que en sí misma no es necesaria, pero suficiente para el resultado.

Al reducir el nivel para el tratamiento de las sub-condiciones identificadas en el modelo, es posible construir las siguientes fórmulas: "Cond 1 = Subcond 1.a + Subcond 1.b"y "Cond 6 = Subcond 6.a + Subcond 6.b", siendo el vector "+" un vínculo de sustitición (es decir, se puede reemplazar una de las dos sub-condiciones planteadas para cada variable), lo que da lugar a la constitución de **condiciones SUIN**, donde cada una de las sub-condiciones podría identificarse como una causa que es suficiente pero no necesaria, de un factor que en sí es insuficiente pero necesario para el resultado. Al tomar parte del modelo como ejemplo, para lograr la condición necesaria de "gestión de riesgo y de cambio" (Condición Nº 1), se han identificado dos sub-condiciones: "capacidad de anticipar la crisis (CERT)" (Sub-condición 1.a) y "establecimiento de atributos de

calidad basados en estándares e indicadores de diagnósticos continuos y métricas apropiadas" (Sub-condición 1.b), es posible que la sub-condición 1.a no esté presente, pero se haya alcanzado la Condición 1, debiendo estar presente como mínimo la sub-condición 1.b (principio de sustitución). Esta relación de variables se llama causa SUIN.

Finalmente, y solo con el propósito de identificar en el modelo la última de las variables planteadas en la literatura, podría señalarse sólo una **causa** llamada "**suficiente**" para lograr la resiliencia cibernética deseada, considerando un sistema absolutamente aislado de la red, del contacto físico con dispositivos externos de cualquier tipo, de cualquier interferencia virtual o física, logrando la categorización de "circuito cerrado". Dado que una causa suficiente es aquella en la que su presencia garantiza la concreción o consumación del resultado a explicar, es decir, la presencia de esta condición significa la existencia de resultado (resiliencia), solo podría considerarse posible en el caso de estudio si el sistema estuviese absolutamente aislado, afectando esta condición con el rendimiento eficiente de este modelo, haciéndolo inviable.

CAPÍTULO 4
¿ES POSIBLE una América del Sur ciber-resiliente?

Para responder a esta pregunta resulta imperioso en primera instancia abordar dos conceptos cruciales: “Difusión de Políticas” y “Transferencia de Políticas”.

Comenzando con la difusión de políticas, Levi-Faur (2005) entiende que es “el proceso mediante el cual la adopción de la innovación por parte de los miembros de un sistema social se comunica a través de ciertos canales a lo largo del tiempo, activando mecanismos que aumentan la probabilidad de adopción por otros miembros que aún no los han adoptado” (p. 23).

Weyland (2006) señala que es relevante distinguir si la difusión de políticas es un modelo o un principio. El primero se refiere a la difusión de una política o programa específico y concreto que se reproduzca. El segundo se refiere a la difusión de un principio, una directriz que conduce las decisiones a ciertas políticas.

Estos autores afirman que los estudios sobre difusión de políticas públicas constituyen una perspectiva de análisis consolidada que contribuye a la comprensión de los procesos de difusión de políticas que pueden ocurrir dentro de un país, oa nivel regional y global.

A su vez, la transferencia de políticas se entiende ampliamente como un proceso mediante el cual el conocimiento de políticas, arreglos administrativos, instituciones e ideas en un sistema político (pasado o

presente) se utiliza para desarrollar características similares en otro (BENSON, 2000).

Bennet y Howlett (1992) lo definen como "el aumento general de las políticas de conocimiento" (p. 288). El dilema presentado en esta declaración es que solo los humanos pueden generar y asimilar conocimiento. Como señalan Sabatier y Jenkins-Smith (1993), el aprendizaje guiado requiere no solo de la asimilación del conocimiento, sino también del uso de políticas en otros lugares. Esta transferencia de políticas generalmente es utilizada por los gobiernos y se denomina aprendizaje organizacional.

Argyris y Schon (1994) hacen un abordaje al aprendizaje organizacional al inferir que "ocurre cuando los hombres actúan en nombre de la organización e interactúan con los demás". En este caso, "el aprendizaje deriva de las creencias, actitudes y valores de estos miembros relevantes de la organización, y como transferencia de políticas, el comportamiento organizacional también cambia" (p.191).

Como se ha visto, la diferencia entre estos dos conceptos no es fácil de identificar. Es por eso que, a partir de un análisis en profundidad de la literatura presentada por Obingera, Shmitta y Stakea (2013), fue posible construir un marco comparativo entre la transferencia y difusión de políticas que permita una comprensión más detallada de estos conceptos.

TABLA 6 - Comparación entre transferencia y difusión de políticas.

Criterios	Transferencia de políticas	Difusión de políticas
Definición	Un proceso que denota la acción política utilizando el conocimiento sobre estrategias, arreglos administrativos, instituciones e ideas en un sistema político para desarrollar arreglos administrativos, instituciones e ideas en el otro sistema político.	El proceso por el cual las decisiones políticas en un país afectan las decisiones políticas de otros países.
Orientación literaria	Se basa en trabajos previos en relación con el diseño.	Se refiere a la literatura cuantitativa sobre la difusión de innovaciones y programas de adopción.
Motivación	Relevancia del conocimiento y papel de los procesos internacionales (sucursales).	En general, incluye procesos estructurales basados en intereses.
Enfoque metodológico	Dominante en estudios de caso orientados a la investigación.	Se utiliza con mayor frecuencia en la literatura de investigación cuantitativa.
Propósito	Tanto la política de difusión como la política de transferencia se refieren a las interdependencias entre los sistemas políticos en el proceso de toma de decisiones.	
Finalidad	Las descripciones y explicaciones de las políticas son el resultado de decisiones interdependientes.	

Fuente: Adaptación de autor de los conceptos presentados por Obingera, Shmitá y Stakea (2013).

Como información adicional relevante, los autores Obingera, Shmitta y Stakea (2013) afirman que las diferencias entre los dos procesos son

marginales y se basan principalmente en diferentes tradiciones de investigación, lo que deja en claro que, con el tiempo, es posible que haya similitudes en los resultados obtenidos al aplicar cualquiera de los procesos.

Basado en esta última declaración, y considerando que esta investigación es de naturaleza cualitativa, que está orientada al mapeo de un caso histórico, que está motivado por la relevancia del conocimiento y de los procesos internacionales, y que tiene una estrecha relación con el diseño de modelos, es que la literatura sobre transferencia de políticas será abordada como herramienta de referencia.

La historia muestra que un modelo aplicable en una región puede no funcionar en otra por varios problemas subyacentes, tanto endógenos como exógenos en ese entorno. Es por eso que el empleo de la técnica de transferencia de políticas, con referencia a Dolowitz y Marsh (2000), además de la revisión bibliográfica de Benson y Jordan (2011), buscará transferir este modelo a América del Sur, cuya realidad es considerablemente diferente a la de Europa como para que sea importado directamente.

A continuación se presentará la visión de Dolowitz y Marsh (2000) sobre la transferencia de políticas. Estos autores afirman que este proceso se organiza en torno a seis preguntas, resumidas en la siguiente tabla:

TABLA 7 – Visión de Dolowitz y Marsh (2000) respecto a la transferencia de políticas.

Pregunta	Orientación
¿Por qué los actores participan en la transferencia de políticas?	Los actores participan en la transferencia de políticas de forma voluntaria, coercitiva, o combinando estas dos variantes. Voluntariamente a partir del modelado de lecciones aprendidas, que presupone una racionalidad perfecta. Coercitivamente, a partir de una imposición directa dada por grupos de presión, partidos políticos, empresarios o expertos en políticas. De manera mixta a partir del modelo de lecciones aprendidas de una racionalidad limitada que surge de las presiones internacionales (imagen, consenso, percepciones), restricciones (préstamos, condiciones asociadas con la actividad comercial) y obligaciones.
¿Quiénes son los actores clave involucrados en el proceso de transferencia de políticas?	En primer lugar, es necesario reconocer y distinguir entre los países que normalmente son prestamistas y aquellos que generalmente reciben esos beneficios, y esta relación debe evitar ser desproporcionada. Aun así, esta no es una regla universal, a veces los países clasificados como prestamistas extraen lecciones, pero los países clasificados como beneficiarios actúan como modelos para otros sistemas políticos. Así, se podrían clasificar nueve categorías principales de actores políticos involucrados en la transferencia de políticas: los funcionarios elegidos; los partidos políticos; burócratas / empleados; grupos de presión; empresarios expertos en políticas de emprendimiento; corporaciones transnacionales; grupos de reflexión; organismos supra-institucionales, gubernamentales y no gubernamentales.

Pregunta	Orientación
¿Qué se transfiere?	Hoy en día, casi todo se puede transferir de un sistema político a otro, dependiendo del problema o la situación en cuestión. Aun así, se pueden distinguir ocho categorías diferentes: objetivos de políticas, contenido de políticas, instrumentos de políticas, programas de políticas, instituciones, ideología, ideas y actitudes.
¿De dónde se extraen las lecciones?	En esencia, se argumenta que los formuladores de políticas pueden observar los tres niveles de gobierno: internacional, nacional y local. Dentro de una nación, los actores de transferencia de políticas pueden aprender de otros sistemas o unidades políticas en su propio país. También es común que los gobiernos y agentes transfieran políticas de una nación a otra. Además, es importante extraer lecciones de otros países, no solo mirando a los gobiernos nacionales, sino también mirando a otros niveles y unidades de gobierno sub-nacionales. Finalmente, se pueden extraer lecciones, forzadas a un sistema político, desde el nivel internacional.
¿Cuáles son los diferentes grados de transferencia?	La transferencia de políticas no es un proceso en absoluto, ya que cualquier caso particular puede implicar combinaciones. Aun así, existen básicamente cuatro gradaciones diferentes (o grados de transferencia): copiado, que implica transferencia directa y completa; emulación, que implica la transferencia de ideas detrás de la política o programa; combinaciones, que mezclan varias políticas diferentes; e inspiración, donde la política en otra jurisdicción puede inspirar un cambio.

Pregunta	Orientación
¿Qué restringe o limita el proceso de transferencia de políticas?	El proceso puede verse limitado por su propia complejidad política; por las diversas publicaciones disponibles en periódicos, revistas, televisión o radio; por la estructura; por las propias instituciones; viabilidad (ideología, proximidad cultural, tecnología, economía, burocracia); y por idioma.
¿Cómo se relaciona el proceso de transferencia de políticas con la política de éxito o fracaso?	En cuanto al éxito, al difundirse esta transferencia a través de los medios de comunicación, informes, conferencias, reuniones, visitas, declaraciones (escritas o verbales). En cuanto al fracaso, a partir de una transferencia no uniforme, incompleta o inadecuada.

Fuente: Adaptación de autor de los conceptos presentados por Dolowitz y Marsh (2000).

Profundizando los conceptos presentados anteriormente, Benson y Jordan (2011) formulan una serie de preguntas para guiar el proceso de revisión de la literatura Dolowitz y Marsh (2000), ofreciendo también las respuestas correspondientes basadas en varias producciones académicas. Por lo tanto, se podrían identificar los siguientes aspectos relevantes para nuestra investigación:

TABLA 8 – Síntesis de revisión académica de Benson y Jordan (2011).

Pregunta	Orientación
¿Qué elementos de la política se transfieren?	Objetivos de política, estructura y contención; instrumentos técnicos políticos y administrativos; instrucciones; ideologías ideas, actitudes y conceptos; lecciones negativas.
¿Hay diferentes tipos de transferencias?	Inicialmente identificaron: copia, emulación, hibridación, síntesis e inspiración. En la actualidad, se pretende combinar la hibridación con la síntesis para denotar los casos en que los elementos de la política se diseñan en función de diferentes contextos. Sin embargo, hay más categorías y tipos de transferencias a considerar.
¿De dónde vienen estas políticas?	Originalmente, la transferencia de políticas se daba tanto de una fuente endógena como exógena. Sin embargo, cada vez más personas que trabajan desde una perspectiva de europeización, globalización y gobernanza multilateral han sugerido que las lecciones también podrían extraerse y transferirse fácilmente entre muchos lugares diferentes, abarcando múltiples escalas espaciales y temporales.
¿Qué factores permiten y limitan esta transferencia?	Dependencia de la trayectoria que surge de decisiones pasadas; impedimentos institucionales y estructurales; falta de compatibilidad ideológica entre los países de transferencia; la insuficiencia de recursos tecnológicos, económicos, políticos y burocráticos para poner en práctica las políticas de transferencia.

Fuente: Adaptación de autor de los conceptos presentados por Benson y Jordan (2011).

Sintetizando el análisis realizado, se presentan a continuación una serie de preguntas (debidamente adaptadas de la literatura), que se tendrán en cuenta para la aplicación práctica de la teoría en el contexto de la transferencia de políticas públicas de la OTAN a América del Sur:

- ¿Por qué se pretende que actores participen de la transferencia de políticas en el ambiente cibernético?
- ¿Quiénes son los actores clave involucrados en el proceso de transferencia de políticas entre la OTAN y América del Sur?
- ¿Qué se pretende transferir y de dónde fueron extraídas las lecciones?
- ¿Cuáles son los diferentes grados de transferencia y cuál es su posible proyección en el tiempo?
- ¿Qué factores permiten y limitan el proceso de transferencia de políticas en el caso particular de América del Sur?

En las siguientes sub-secciones cada pregunta será respondida, en el mismo orden presentado, con la intención de aplicar la teoría a la realidad regional.

¿POR QUÉ SE PRETENDE QUE LOS ACTORES PARTICIPEN DE LA TRANSFERENCIA DE POLÍTICAS EN EL MARCO DE LA RESILIENCIA CIBERNÉTICA?

Siguiendo la clasificación presentada por Dolowitz y Marsh (2000), se podría afirmar que los actores participan en una transferencia voluntaria, que

presupone, a partir de una racionalidad perfecta, la modelización del sistema previsto basado en las lecciones aprendidas, en este caso por la OTAN.

Por lo tanto, se entiende que los actores participan en la transferencia porque la estructura organizacional de la OTAN para la ciberdefensa y la ciberseguridad se desarrolla sólidamente a través de la constitución del Centro de Excelencia Cooperativo de Defensa Cibernética y la implementación de medidas de desempeño estandarizadas que contribuyan con el crecimiento en el asunto, apuntalando a la confianza mutua entre los países que conforman esta alianza y fortaleciendo los sistemas cibernéticos dentro de ellos.

Por el contrario, América del Sur tiene estructuras muy incipientes al respecto. Aunque la OEA es un organismo tan antiguo como la OTAN, las actividades de integración y cooperación cibernética son recientes, y no existe un organismo similar al CCDCOE, recordando que esos dos principios (cooperación e integración) resultan esenciales para que esa resiliencia pueda ser viable.

¿QUIÉNES SON LOS ACTORES CLAVE INVOLUCRADOS EN EL PROCESO DE TRANSFERENCIA DE POLÍTICAS ENTRE OTAN Y SUDAMÉRICA?

Según Dolowitz y Marsh (2000), la OTAN puede identificarse como un prestamista del modelo, corroborando esto con todos los argumentos ya desarrolladas de previamente. El problema ahora es qué organismo en

América del Sur puede identificarse como un beneficiario, considerando, de acuerdo con la clasificación sugerida por estos autores, que sería un organismo supra-institucional equivalente a la OTAN, pero en la región.

Para conocer la realidad regional se pueden distinguir tres actores bien diferenciados, que serán analizados para identificar uno de ellos como el más apropiado para simular la transferencia. Estos actores son:

• OEA (Organización de los Estados Americanos);

• UNASUR (Unión de Naciones Suramericanas);

• PROSUR (Foro de Progreso de América del Sur).

La OEA es una organización fundada en 1948, con sede en Washington, Estados Unidos de América, cuyo objetivo es construir un orden de paz y justicia en el continente americano, para promover la solidaridad, el desarrollo y la cooperación entre los estados de la Región, además de defender la democracia y los derechos humanos (BRASIL, 2019).

Tiene funciones esencialmente diplomáticas y representativas, ya que es un foro para la cooperación política. Aun así, tiene derecho a ejercer un cierto nivel de coerción si es necesario, siempre que no viole los principios fundamentales de su carta, como el derecho a la soberanía de las naciones y siempre que tenga el voto positivo de los Estados miembro (OEA, 2019).

Mejias (2008) describe que la Organización de Estados Americanos está compuesta por los siguientes países: Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, República Dominicana, Ecuador, El Salvador,

Estados Unidos, Guatemala, Haití, Honduras, México, República Dominicana, San Cristobal y Nieves, Nicaragua, Panamá, Paraguay, Perú, Uruguay, Barbados, Trinidad y Tobago, Jamaica, Granada, Surinam, Canadá, Guyana, Belice, Bahamas, San Vicente y las Granadinas, Antigua y Barbuda, Santa Lucía, Venezuela (país en proceso de separación).

UNASUR es una organización que nació en Brasilia en 2008 y su constitución contó con la participación de doce países de América del Sur: Argentina, Bolivia, Chile, Colombia, Ecuador, Guyana, Paraguay, Perú, Surinam, Uruguay y Venezuela (UNASUR, 2011).

Nació con el objetivo de construir un espacio de integración y unión social, económica, cultural y política entre los países sudamericanos.

Actualmente, los siguientes países están en proceso de separación de esta alianza por diversas causas de orden político y organizacional: Perú, Colombia, Argentina, Chile, Brasil, Ecuador y Paraguay; sólo quedan en su estructura respecto a la organización original: Bolivia, Guyana, Surinam, Uruguay y Venezuela (SABATINI y ALBARTONI, 2019).

El primer país en abandonar UNASUR fue Colombia, en agosto de 2018 y ya en enero de 2019, el presidente de ese país (Iván Duque) anunció la intención de varios gobiernos iberoamericanos de crear una nueva organización, a la cual llamarían PROSUR. Esta intención fue respaldada de inmediato por el presidente de Chile, Sabastián Piñeira, quien señaló que este nuevo foro estaría abierto a todos los países de América del Sur que respeten el pleno estado de derecho y promuevan el respeto de las libertades

y de los derechos humanos (SABATINI y ALBARTONI, 2019).

El PROSUR comenzó a operar el 22 de marzo de 2019, cuando se celebró la primera reunión de esta organización, la cual tuvo lugar en Santiago de Chile, con la participación de los siguientes países: Argentina, Brasil, Chile, Colombia, Ecuador, Paraguay y Perú. Como observadores, pero no miembros del Foro, ni suscriptores del protocolo, también estuvieron presentes: Bolivia, Surinam y Uruguay (SABATINI y ALBARTONI, 2019).

El 23 de julio de 2019, se llevó a cabo la primera reunión de Coordinadores Nacionales de PROSUR en Santiago de Chile, sede de la Presidencia *pro tempore* de esa organización. En este evento, el Ministro de Relaciones Exteriores de Chile (Teodoro Ribera) declaró que los países participantes comparten la intención estratégica de que la región sea reconocida en el escenario global. En esta reunión, las áreas prioritarias del Foro fueron: infraestructura, energía, salud, defensa, seguridad y lucha contra el crimen, preservación y gestión de desastres naturales (CHILE, 2019).

De acuerdo con lo presentado hasta ahora, y considerando que América del Sur tiene una organización en vías de disolución (UNASUR) y otra en proceso de creación (PROSUR), sin una estructura definida todavía, es la OEA la que ciertamente cumple más con los principios de cooperación e integración sudamericana.

Basado en un proceso exploratorio de los principales portales de la OEA, organizaciones relacionadas y agencias gubernamentales de los países de la región, a continuación se enumerarán una serie de noticias e

información para extraer conclusiones sobre la relevancia o no de la OEA como facilitador regional y articulador del modelo de resiliencia cibernética creado.

Los criterios utilizados para seleccionar estos portales de noticias fueron: tomar como fecha de inicio de la muestra el comienzo del proceso de disolución de la UNASUR, basado en la declaración de Colombia de abandonar esta organización en agosto de 2018; y que estos portales sean oficiales o brinden información oficial de los gobiernos de la región.

TABLA 9 - Resumen de noticias oficiales sobre la participación de la OEA en el campo de la cibernética en América del Sur.

Fecha	País / Región	Noticias
08/03/2018	Argentina	La Dirección Nacional de Cooperación de Seguridad Internacional del Ministerio de Seguridad de la República Argentina, junto con la Dirección Nacional de Inteligencia Criminal, recibió capacitación internacional sobre Ciberseguridad, dentro de un programa de Liderazgo y Estrategia de Ciberseguridad. El programa fue organizado por la Organización de Estados Americanos y la Universidad Internacional de Florida. De esta manera, las acciones de cooperación internacional continúan consolidándose en vista de los desafíos contemporáneos planteados por las amenazas cibernéticas y su proyección futura. Con el fin de actualizar la información para prevenir riesgos de ciberseguridad, el programa incluyó módulos sobre ciber-amenazas, estrategias de seguridad operativa, problemas de ciberseguridad nacional y ejercicios de simulación de respuesta (ARGENTINA, 2018).

Fecha	País / Región	Noticias
24/10/2018	América	La Secretaría General de la OEA y *Amazon Web Services* (AWS) presentaron en Colombia un Libro Blanco conjunto que aborda los desafíos y oportunidades que la seguridad cibernética implica, y establece recomendaciones para la sostenibilidad de las ciudades inteligentes. Este documento es el cuarto de una serie que, junto con otras iniciativas conjuntas, busca elevar el nivel de conciencia entre los líderes gubernamentales, el sector privado y la sociedad en general sobre la importancia de la ciberseguridad (OEA 2018).
28/11/2018	América	La Junta Interamericana de Defensa, por delegación de la OEA, celebró una Conferencia de Defensa Cibernética para proponer recomendaciones a los Estados Miembros de la OEA sobre la seguridad de la gestión de la información a través del ciberespacio y la protección de la tecnología de la información. Esta fue la primera Conferencia de Ciberseguridad en el Hemisferio.
14/12/2018	Paraguay	Presentación del Plan Nacional de Ciberseguridad de Paraguay. Varios sectores involucrados en el tema de seguridad cibernética de Paraguay sobre el apoyo y la facilitación de la OEA participaron en esta presentación (PARAGUAY, 2018).
06/03/2019	Chile y América	Simposio de Ciberseguridad de la OEA 2019, que se realizará del 24 al 27 de septiembre de 2019 en la ciudad de Santiago de Chile. Chile asume la Presidencia del Grupo sobre medidas de fomento de la confianza y cooperación en el ciberespacio de la OEA. A la reunión de este grupo, celebrada en abril de 2019, asistieron representantes de los países de la región, expertos internacionales, junto con el apoyo y los auspicios de la Secretaría Ejecutiva del Comité Internacional contra el Terrorismo de la OEA (CHILE, 2019).

Fecha	País / Región	Noticias
09/23/2018	América Latina y el Caribe	La OEA presenta un Informe sobre Ciberseguridad y Entidades Bancarias en América Latina y el Caribe, en el marco del Simposio de Ciberseguridad ofrecido por la propia organización. Este informe proporciona un análisis exhaustivo del estado de las entidades bancarias de la región con respecto a diferentes aspectos de la seguridad cibernética. El noventa y dos por ciento de las entidades bancarias latinoamericanas han sido víctimas de un incidente cibernético en el último año, y el 37% de ellas han sido atacadas con resultados exitosos por delincuentes (OEA 2018).

Fuente: El autor.

La intención de presentar las noticias anteriores es simplemente demostrar la relevancia de la OEA en América del Sur para la ciberdefensa y la seguridad, y luego su posible consideración como una contraparte de la OTAN para ejercer el proceso de transferencia de políticas públicas para la aplicación del modelo creado.

Además, y para reforzar la postura adoptada, serán presentadas a continuación una serie de opiniones de expertos, extraídas de los respectivos cuestionarios distribuidos, versando sobre la posibilidad o no de transferencia de las experiencias de la OTAN a América del Sur, existiendo un consenso bastante amplio al respecto de que la OEA es el órgano responsable de hacer funcionar el sistema de cooperación e integración regional.

En resumen, una gran mayoría de estos expertos considera que la transferencia es posible a partir de la cooperación actual con la OEA. Aun así, la unificación de criterios es necesaria, creando y fortaleciendo un marco cooperativo basado en la confianza mutua.

También fue considerado como problemático el vacío legal existente, la falta de coherencia ideológica entre los países de la región y la falta de políticas de una superestructura regional basada en el consenso regional.

¿QUÉ SE QUIERE TRANSFERIR Y DE DÓNDE FUERON EXTRAÍDAS LAS LECCIONES?

En base al criterio de los autores Dolowitz y Marsh (2000), aplicado al presente caso, las categorías de políticas que podrían transferirse serían: objetivos, instrumentos, programas y actitudes, dirigiendo su mirada hacia lo internacional (inicialmente regional, sin desconectarse de realidad) y nacional (considerando la particularidad de cada país miembro).

En relación con el párrafo anterior, el objetivo es transferir el Modelo de Resiliencia Cibernética creado a partir de las lecciones aprendidas por las mejores prácticas de la OTAN en el campo y la visión de los casi 60 expertos en el campo que contribuyeron con la investigación.

Tal modelo propuesto, que involucra objetivos, instrumentos, programas y actitudes a ser articulados, podría resumirse en los siguientes temas:

TABLA 10 – Síntesis de contenidos del modelo a ser transferido.

Gestión de riesgos y cambios (trazabilidad adecuada contra cualquier incidente de seguridad cibernética y automatización de respuesta a amenazas), respaldada por una capacidad adecuada de anticipación de crisis (CERT) y el establecimiento de padrones de calidad basados en estándares e indicadores, diagnósticos continuos y métricas apropiadas.
Profundo conocimiento de la organización (capacitación adecuada en ingeniería social en todos los niveles y conciencia de la organización, todos los niveles de toma de decisiones y sociedad sobre la importancia de la cibernética), lo que hace que el área cibernética sea capaz de y participación a nivel de gestión de toma de decisiones en la organización.
Procesos continuos y operativos en todas las circunstancias (estructura del sistema de información, protección física del patrimonio tecnológico, fomento del desarrollo de software seguro en el sector de programación de la organización, establecimiento de controles críticos de seguridad y auditorías periódicas sobre resiliencia, redundancia, segmentación de información y cooperación).
Asegurar regulaciones de infraestructura críticas (estandarización de sistemas, categorización clara y priorización de activos a proteger).
Desarrollo de ejercicios y modelos de simulación.
Cooperación privada, estatal, nacional y regional (existencia de un glosario común estandarizado de términos relacionados con la ciberseguridad para fomentar la cooperación y la necesidad de crear un ambiente de confianza mutua entre las organizaciones de defensa cibernética). Esto requiere actualizar el marco legal y establecer una Estrategia Nacional Cibernética para cada estado miembro.
Formación y especialización de capital humano (del personal vinculado a las áreas de ciberdefensa, seguridad informática y sistemas; constitución de equipos multidisciplinares).
Implementación y actualización de estrategias de resiliencia cibernética (disponibilidad de una plataforma común para compartir datos y firmas digitales de ataques cibernéticos).
Asignación presupuestaria suficiente.

Fuente: El autor.

¿CUÁLES SON LOS DIFERENTES GRADOS DE TRANSFERENCIA Y CUÁL ES SU POSIBLE PROYECCIÓN EN TIEMPO?

Considerando que las graduaciones propuestas por Dolowitz y Marsh (2000) son copiar, emular, combinar o inspirar, el objetivo es aplicar una combinación para hacer posible esta transferencia. Aun así, y para el estudio de este caso particular, también se propusieron graduaciones en el proceso de aplicación de esta transferencia, como una forma de hacer que su implementación sea más plausible y factible.

Así, se establecieron los siguientes grados de transferencia (en profundidad), distinguiéndose un primero como inmediato, un segundo como a corto y mediano plazo, y un tercero como a largo plazo.

TABLA 11 - Grados de transferencia para el modelo pretendido.

Grado	Medidas
1er Grado	Gestión de riesgos y cambios. Tal como se presentó, estas son medidas que se están implementando actualmente en los países de la región, considerando la necesidad de preservar su propia información y sistemas.
	Desarrollo de ejercicios y modelos de simulación. Este es otro tema que se está trabajando bilateral y regionalmente en su conjunto, principalmente por países como Brasil, Colombia y Chile.
	Formación y especialización del capital humano. Alineado con el razonamiento de las dos condiciones anteriores, la formación y especialización del capital humano es una cuestión de extrema relevancia.

Grado	Medidas
2do Grado	Procesos continuos y operativos bajo cualquier circunstancia. Si bien la gestión de riesgos y las medidas de cambio se pueden incorporar al primer grado de transferencia a la región, los procesos en curso y operativos bajo cualquier circunstancia requieren una infraestructura cooperativa e integrada en la región que debe construirse pero que no se puede hacer a corto plazo.
	Garantizar la regulación de las infraestructuras críticas. A pesar que la infraestructura crítica es responsabilidad de cada estado protegerla, ya sea que el soberano lo haga o no, la cooperación e integración regional ayudarían en gran medida a estandarizar las medidas que se tomarán para cada tipo de infraestructura crítica, además de las que tienen un impacto más allá de las fronteras de los países. El tiempo de madurez, adaptación e implementación de estas medidas puede llevar un período que ciertamente no será a corto plazo.
	Cooperación privada, estatal, nacional y regional. Esta condición es parte del proceso. Algunos países de la región ya están en camino, pero a nivel regional, aún queda mucho trabajo por hacer. Bilateralmente entre países puede existir, pero regionalmente aún es incipiente.
	Implementación y actualización de estrategias de resiliencia cibernética. Al igual que con la OTAN, con pautas y orientación para los países miembros, podría ser una buena práctica para cada país de la región adaptar sus estrategias de ciberseguridad y defensa cibernética, tendiendo a establecer estándares de rendimiento comunes que favorezcan la sinergia y hagan la seguridad regional más robusta.

Grado	Medidas
3er Grado	Profundo conocimiento de la organización. Se ha colocado en este grado de transferencia porque la región aún no ha definido una organización internacional que coordine y regule el ciberespacio, como sí es el caso de Europa con el CCDCOE de la OTAN. Sin una organización similar, o incluso sin la constitución de estructuras organizativas compartidas por todos, ni siquiera será posible cumplir con esta condición.
	Asignación presupuestaria suficiente. Esta condición responde a una realidad regional de desigualdad, necesidades y crisis profundas y continuas en diferentes países de la región. A nivel local, cada estado puede crear estructuras consistentes y resistentes, pero dentro del ámbito corporativo de América del Sur, la mayoría de los países deben poder proporcionar asignaciones presupuestarias suficientes a los sistemas de la región en su conjunto para ser ciber-resilientes.

Fuente: El autor

¿QUÉ FACTORES PERMITEN Y LIMITAN EL PROCESO DE TRANSFERENCIA DE POLÍTICAS EN EL CASO DE SUDAMÉRICA?

En el caso específico de América del Sur, los factores que permiten o limitan el proceso de transferencia de políticas son muy diversos y heterogéneos. Considerando lo propuesto por Dolowitz y Marsh (2000), y la conveniente revisión de Benson y Jordan (2011), la complejidad política regional abordada en conjunto es la gran síntesis del problema. Aun así, la viabilidad puede verse comprometida por las ideologías existentes, las

disparidades tecnológicas entre los países miembros y la burocracia de las estructuras estatales. Aunque para los hispano-hablantes Brasil sea el único país con idioma diferente, no deja de ser un lenguaje inteligible para el español, no significando un obstáculo para la comunicación.

Actualmente, según lo presentado, la falta de madurez y la cooperación regional son los principales obstáculos para la articulación de un modelo común. Existen todavía una serie de problemas estatales, regionales e ideológicos que crean obstáculos para esta cooperación tan necesaria para alcanzar el camino de la eficiencia.

Como han presentado varios expertos, América del Sur se encuentra en la misma situación que Europa, ya que la amenaza cibernética no distingue fronteras ni soberanía. Por lo tanto, debe intentar y ser capaz de asumir el desafío.

CONSIDERACIONES FINALES

El presente estudio adquiere relevancia porque busca identificar un mecanismo causal y las condiciones de necesidad y suficiencia para construir un sistema cibernético resiliente dentro de América del Sur mediante la evaluación de las prácticas del Centro de Excelencia Cooperativo de Ciberdefensa de la OTAN en Estonia.

Esta relevancia se incrementó a partir de las contribuciones ofrecidas por los casi 60 expertos en la materia consultados, que formaron parte de la investigación, alejando los resultados de una visión puramente personal para transformarse en un consenso común compartido por un importante conglomerado de expertos en el campo.

La concatenación y estructuración de la investigación, tal como se hizo, permitió una mejor comprensión y construcción metodológica del resultado, comenzando con la teorización de conceptos relacionados, que le dio el marco adecuado al estudio; un enfoque de Estonia como ejemplo de víctima y actor clave de este cambio de paradigma en la era de la información y la evolución de la cibernética de la OTAN desde el establecimiento de la CCDCOE; la construcción del modelo de resiliencia cibernética a partir de datos obtenidos de la OTAN sometidos al análisis y juicio de casi 60 expertos en el tema; y finalizando con la presentación de una ruta de transferencia de políticas de la OTAN a la OEA buscando que este modelo sea aplicable en América del Sur.

La aplicación del *process tracing* como técnica metodológica, estableciendo el mecanismo causal derivado del mapeo histórico de eventos permitió el establecimiento de variables que, sometidas a revisión de expertos, posibilitaron la formulación de condiciones, sub-condiciones y componentes (aplicando la técnica literaria de análisis de condiciones causales) que, al clasificarlos en necesarios, suficientes, INUS y SUIN, dieron lugar al posible modelo de resiliencia cibernética creado. Esto, junto con la aplicación de literatura de transferencia de políticas para comprobar la posibilidad (o no) de llevarlo a América del Sur, resultó de gran ganancia para el proceso racional empleado con el fin de construir conclusiones relevantes. El uso de Estonia como herramienta para comprender la evolución de la OTAN en el área no solo ha demostrado con un ejemplo concreto qué es la resiliencia en sí misma, sino que también emula los conceptos de cooperación, integración, compromiso nacional, regional y global, que son condiciones esenciales para progresar en este nuevo escenario cibernético.

Identificar los componentes clave que podrían convertir un sistema en ciber-resiliente evaluando las medidas tomadas por la OTAN con sus estados miembros representó el comienzo del camino de construcción del modelo.

El desarrollo del mismo, a partir del análisis de las medidas adoptadas por la OTAN en Europa, y la consulta a 58 expertos en el tema (muchos de ellos de muy alto nivel), representantes de los siguientes países: Argentina, Brasil, Chile, China, Colombia, El Salvador, Ecuador, España, Estados Unidos de América, Guatemala, México, Paraguay, Perú y Uruguay,

constituyó una ganancia real en el nivel y la calidad del estudio.

El dinamismo que ofrece la tabla de síntesis de resultados de los cuestionarios de investigación de los expertos, caracterizados por tener una ponderación particular de sus opiniones y establecer una categorización de los resultados obtenidos, permitió de hecho construir el árbol de condiciones según el grado de relevancia que cada una de ellas representa en el modelo.

Para mejorarlo, se analizaron y exploraron las respuestas de los expertos y, a partir de la relevancia y de las contribuciones hechas por ellos, se identificaron sub-condiciones y componentes adicionales.

Teniendo en cuenta que la base del modelo proviene de una organización internacional que tiene una estructura que permite su implementación (OTAN), se debió identificar una organización internacional de características similares en América del Sur, para simular su debida transferencia a la región. A partir de allí, UNASUR, PROSUL y OEA fueron analizados como posibles receptores de este modelo, resultando la OEA el más apropiado en la actualidad.

También se consideró, por el debilitamiento de UNASUR y la falta de estructura de PROSUL, que es posible percibir el reciente crecimiento de la OEA en el área de cooperación e integración regional en materia cibernética, aspecto este que surgió de la necesidad o intención de ocupar los espacios vacíos que las organizaciones internacionales antes mencionadas habían dejado libre. Para materializar esto, se analizaron una serie de noticias oficiales.

En estas noticias fue posible identificar una serie de condiciones

encontradas en el modelo de resiliencia cibernética creado, las cuales fueron tratadas y desarrolladas en los foros respectivos, incluyendo: gestión de riesgos y cambios; procesos continuos y operativos bajo cualquier circunstancia; desarrollo de ejercicios y modelos de simulación; cooperación privada, estatal, nacional y regional; formación y especialización de capital humano; e implementación y actualización de estrategias de resiliencia cibernética (ciclo de vida).

Antes de someter el modelo al proceso de transferencia de políticas entre la OTAN y la OEA, se analizaron las diversas opiniones de los expertos consultados sobre el tema, lo que resultó en un porcentaje muy alto de profesionales que consideraron este proceso factible y una cantidad mínima que pensó que tal transferencia no sería posible.

Con toda la información presentada a lo largo de la investigación, y respondiendo al proceso que ofrece la literatura sobre transferencia de políticas como una buena práctica, fueron elaboradas las siguientes preguntas orientadoras para dicho proceso:

- ¿Por qué se pretende que actores participen de la transferencia de políticas en el ambiente cibernético?
- ¿Quiénes son los actores clave involucrados en el proceso de transferencia de políticas entre la OTAN y América del Sur?
- ¿Qué se pretende transferir y de dónde fueron extraídas las lecciones?
- ¿Cuáles son los diferentes grados de transferencia y cuál es su posible proyección en el tiempo?

- ¿Qué factores permiten y limitan el proceso de transferencia de políticas en el caso particular de América del Sur?

Como resultado general, después de responder las preguntas, se concluyó que es posible transferir el modelo que surgió en la OTAN a la OEA, pero con una graduación diferenciada en el tiempo, discriminando tres niveles de plazos (inmediato, corto/medio y largo plazo).

Finalmente, y considerando la pregunta de estudio que guió el trabajo (**de las prácticas del Centro de Excelencia Cooperativo de Defensa Cibernética de la OTAN, ¿cuáles son las condiciones necesarias que conducen a la resiliencia de los sistemas cibernéticos y cómo estas prácticas pueden transferirse a Sudamérica?**), se puede concluir que fue posible arribar a resultados relevantes y aplicables a una realidad regional no tan sólida y robusta, pero que se presenta próspera y optimista, dejando el camino abierto para los futuros estudios que conduzcan a la aplicación práctica de este posible modelo teórico creado.

BIBLIOGRAFÍA

AGUIRRE, J. Mecanismos causales y *process tracing*. Una introducción. Mendoza: SAAP, Vol.11, Nº 1, 2017.

ALZUGARAY TRETO, C. Nuevo regionalismo e integración regional en América Latina y el Caribe. España: Cursos de Derecho Internacional y Relaciones Internacionales, Servicio Editorial Universidad del País Vazco, pp. 47-79, 2002.

ARGENTINA. Presidencia de la Nación. Organizamos capacitación internacional sobre ciberseguridad junto a la OEA. Mensaje publicado en el portal de la Presidencia de la Nación Argentina el 3 de agosto de 2018.

ARGYRIS, C.; SCHON, D. Theory in practice-increasing professional effectiveness. San Francisco: Jossey – Bass Inc., 1994.

AVIAR, P. A situação nas ruas é calma. Tallin, Estônia: Eesti Päevaleht, 2007.

BEACH, D. Process- Tracing Methods : Foundations and Guidelines. First ed. Michigan, United States of American: The University Michigan Press, 2013.

BEACH, D. It ' s all about mechanisms – what process-tracing case studies should be tracing should be tracing. New Political Economy, [S.l.]: v. 3467, n. February, 2016.

BEAUDOIN, L.; JAPKOWICZ, N.; e MATWIN, S. Autonomic

Computer Network Defence Using Risk State and Reinforcement Learning. New York: Cryptology and Information Security Series, v.3, pp.238-248, 2009.

BENNET, B. Understanding, Assessing, and Responding to Terrorism: Protecting Critical Infraestructure and Personnel. New Jersey: Wiley - Interscience, 2007.

BENNET, C.; HOWLETT, M. The Lessons of Learning: Reconciling Theories of Policy Learning and Policy Change. Netherlands: Kluwer Academic Publishers, 1992.

BENSON, D.; JORDAN, A. What Have We Learned from Policy Transfer Research? Dolowitz and Marsh Revisited. London: Political Studies Review, Vol 9, p. 366-378, 2011.

BERINATO, S.; PERRY, M. As tendências da segurança em números. [S.I.]: Hardvard Business Review Brasil, 6 de julio de 2018.

BISQUERRA, R. Métodos de investigación educativa. Guía práctica. Barcelona: Grupo Editorial CEAC, 1989.

BUCHAREST SUMMIT DECLARATION. Bucharest: Declaration issued by the Heads of State and Government participing the meeting of the North Atlantic Council, 2008.

BUSINESS CONTINUITY INSTITUTE. Informe de exploração das perspectivas de futuro (*Horizon Scan*). [S.I.]: BCI, 2018.

CANONGIA, C.; MANDARINO, R. Cybersecurity: The New Challenge of the Information Society. In Crisis Management:

Concepts, Methodologies, Tools and Applications. Hershey: PA, IGI, 2014.

CAPORASO, J,; PELOWSKI, A. Economic and political integration in Europe: a time series quasi- experimetal analysis. Estados Unidos: American Political Science Review, p. 421, 1975.

CARVAJAL CONTRERAS, M. Derecho Aduanero. México: Editorial Porrúa, p. 40, 1993.

CARVAJAL VILLAPLANA, A. Teorías y modelos: formas de representación de la realidad. Costa Rica: Escuela de Ciencias Sociales del Instituto Tecnológico de Costa Rica, p. 8, 2012.

CARAYANNIS, E. G.; CAMPBELL, D. F. J. Cyber- Development , Cyber-Democracy and Cyber-Defense; Challenges, Opportunities and Implications for Theory, Policy and Practice. New York: Springer, 2014.

CARRASCO, L. Ciber-Resiliencia. Madrid, España: Instituto Español de Estudios Estratégicos, 2015.

CCDCOE NATO. National Cyber Security Framework Manual. Tallin, Estonia: 2012. CESEDEN. Concepto de defensa resumen ejecutivo. Madrid, España: Estado Mayor de la Defensa, 28 de septiembre de 2018.

CHALMES, A. What is the thing called science? Queensland, Australia: Hackett Publishing Company, Inc., 1999.

CHILE. Secretaria de Ciberseguridad. Comunicado de prensa. Mensaje publicado el 6 de marzo de 2019. Disponible en <https://www.cibersegu

ridad.gob.cl/noticias/anuncian-fecha-para-simposio-de- ciberseguridad-de-la-oea-en-chile/>.

CHILE. Ministro de Relaciones Exteriores (Teodoro Ribera). Mensaje enviado al portal Noticias de América Latina y el Caribe el 18 de julio de 2019 por Teodoro Ribera, Ministro de Relaciones Exteriores de Chile. Santiago de Chile, 2019.

CLARKE, R.; KNAKE, R. Guerra en la red, los nuevos campos de batalla. Barcelona: Editorial Planeta, 2011.

CONTI, G.; SURDU, J. Army, Navy, Air Force, and Cyber—Is It Time for a Cyberwarfare Branch of Military?.[S.I.]: Springer, Vol. 12, No. 1, p. 17, 2009.

CORLETTI ESTRADA, A. Estrategia de seguridad informática por capas, aplicando el concepto de Operación Militar de Acción Retardante. Madrid, España: Tesis (Doctorado en Informática) Universidad Nacional de Educación a Distancia – Escuela Técnica Superior de Ingeniería Informática, 2011.

CORLETTI ESTRADA, A. Ciberseguridad: Una Estrategia Informático-Militar. Primera ed. Madrid: DarFe, 2017.

CZOSSECK, C.; GEERS, K. The Virtual Battlefeld: Perspectives on Cyber Warfare. Tallinn: IOS Press BV, 2009.

CZOSSECK, C.; OTTIS, R.; TALIHARM, A. Cyber Attacks: Legal, Strategic and Organizational Changes in Cyber Security. Sydeny: International Journal of Cyber Warfare and Terrorism, 2011.

DOLOWITZ, D. P.; MARSH, Y. D. Learning for abroad : The rule of policy transfer in the actual politics decitions. Dolowitz y Marsh Revisited. [S.l.]:v. 13, n. 1, 2000.

DONALDSON, S.; SIEGEL, S.; WILLIAMS, C.; ASLAM, A. Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats. New York: [s.n.].

ECONOMY, T. P.; POWERS, S. M.; JABLONSKI, M. The Real Cyber War. Urbana, Chicago and Sprinfield: University of Illinois Press, 2015.

FERRERO, J. La ciberguerra. Génesis y evolución. Madrid: Revista General de la Marina, 2013.

GAMERO, A. Cyber Conflicts in International Relations: Framework and Case Studies. Estados Unidos: Seminario sobre "Cyber International Relations", 2014.

GARCÍA-AJOFRIN, L. Gigantes de la Educación: lo que no dicen los rankings. Madrid: Editorial Ariel – Fundación Telefónica, 2016.

GEERS, K. Strategic Cyber Security. NATO Cooperative Cyber Defense Centre of Excelence. Estonia: Seminario, 2011.

GROTBERG, E. Introducción: nuevas tendencias en resiliencia. Wisconsin: Universidad de Wisconsin, 1995.

HARRINGTON, A.; THEOHARY, C. Cyber Operations in DOD Policy and Plans: Issues for Congress. Congressional Research Service. CRS Report – Prepared for Members of Commitees of Congress. Estados Unidos: Congreso de los Estados Unidos de América, 2015.

HOUGH, P; MALIK, S.; MORAN, A.; PILBEAM, B. International Security Studies: Theory and Practice. London, 2015.

HUTCHINS, E. Cognition in the Wild. Cambridge: MIT Press, 1995.

INFANTE, F. A resiliência como processo: uma revisão da literatura recente. Tradução Valério Campos. Porto Alegre: Artmed, 2005.

INTECO. Resiliencia: Aproximación a un marco de medición. Madrid: CERT de Seguridad e Industria – INTECO: Instituto nacional de Tecnologías de las Comunicaciones, 2018.

ITU. Global Cyber Security Index 2017 (GCI). [S.I.]: International Telecommunications Union, 2017.

ITU. Guide to developing a National Cyber security Strategy. Outubro de 2018. Disponible en: https://ccdcoe.org/uploads/2018/10/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

JID. Comunicado de prensa. Mensaje publicado el 28 de noviembre de 2018. Disponible en <http://www.jid.org/?p=2662>.

JORDAN, T. Cyberpower: the culture and politics of cyberspace and the internet. Washington DC: Library of Congress, 2003.

JORDANA, J.; LEVI-FAUR, D.; FERNÁNDEZ, J. The Global Diffusion of Regulatory Agencies: Channels of Transfer and Stages of Diffusion. New York: Comparative Political Studies, vol. 44, 201.1

KEMMERER, R. Cybersecurity. [S.I.]: 25th IEEE International Conference on Software Engineering: p 705-715, 2003.

KLIMBURG, A. National Cyber Security: Framework Manual. Estonia: NATO Cooperation Cyber Defense Centre of Excelence, 2014.

LADRIÈRE, J. El reto de la racionalidad. La ciencia y la tecnología frente a las culturas. Salamanca: UNESCO /Sígueme, 1978.

LEVI-FAUR, D. The Global Diffusion of Regulatory Capitalism. New York: The annals of the American Academy of Politician and Cocial Science, Vol 598, 2005.

LEWIS, J. Cybersecurity and Critical Infrastructure Protection. Washington, DC: Center for Strategic and International Studies, 2006.

LLONGUERAS, A. La guerra inexistente, la ciberguerra. Madrid: Editorial Acad MIA Espa Ola, 2013.

MAHONEY, J; RUESCHEMEYER, D. Comparative Historical Analysis in the Social Sciences. New York: Cambridge University Press, 2003.

MAHONEY, J.; GOERTZ, G. A Tale of Two Cultures: Contrasting Quantitative and Qualitative Research.[S.l.]:n. 0093754, p. 227–249, 2006.

MAHONEY, J. Process Tracing and Historical Explanation. Security Studies, [S.l.] 2015.

MALHOTRA, N. [et al]. Introdução à pesquisa de marketing. São

Paulo: Pearson Prentice Hall, 2005.

MEJIAS, S. La OEA: un actor regional en la gestión de crisis. Logros y limitaciones. Madrid: Adenda, pp 69-98, 2008.

MC NAMARA, S. NATO summit 2010: Time to Turn Words Into Action. Washington DC: The Hertiage Foundation. Backgrounder, 2010.

MINTZBERG, H. Mintzberg on Management: Inside our Strange Word of Organizations. New York, The Free Press, 1989.

NEWMEYER, K. Ciberespacio, ciberseguridad y ciberguerra. Lima, Perú: II Simposio Internacional de Seguridad y Defesa, 2015.

NETO, O.; COSSIO RIDRIGUEZ, J. O novo método histórico-comparativo e seus aportes à ciência política e à administração pública. Revista de Administración Pública, [S.l.]:v. 50, n. 6, p. 1003– 1027, 2016.

NYE, J.; WELCH, D. Understanding Global Conflict and Cooperation, an Introduction to Theory and History. Boston, Pearson, 9th Edition, 2013.

OBINGERA, H.; SHMITTA, C.; STARKEA, P. Policy Diffusion and Policy Transfer in Comparative Welfare State Research. Bremen, Germany: Social Policy & Administration, Vol. 47, No. 1, 2013.

O´CONNOR, K. The History of the Baltic States. Wesport: Greenwood Press, 2003. OEA. Disponible en: <http://www.oas.org>.

OEA. Comunicado de prensa. Mensaje publicado el 23 de septiembre de 2018. Disponible en <http://www.oas.org/es/centro_noti cias/comunicado _prensa.asp?sCod igo=AVI-130/18>.

OEA. Comunicado de prensa. Mensaje publicado el 24 de octubre de 2018. Disponible en <http://www.oas.org/es/centro_noticias/comunica do _prensa.asp?sCodigo=C-065/18>.

OEA; CIDH. Libertad de expresión e Internet. 31 de diciembre de 2013. Disponible en (PDF): https://www.oas.org/es/cidh/expresion/docs/ informes/ 2014_04_08_internet_web.pdf

OTAN. Strategic Foresight Analysis 2015. Bruselas, 2015.

OTAN. Commitment to enhance resilience. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council. Bruselas, 2016.

OTAN. Defense College. The evolution of the Hibrid Threat and Resilience as a Conuntermeasure. Bruselas: Nro 139, 2017.

OTAN-UE. Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization. Bruselas, el 8 de julio de2016.

OTAN-UE. Statement on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization. Bruselas, 6 de diciembre de 2016. Disponible en:< http://www.nato.int/cps/en/natohq/official_texts_138829.htm>.

OTTIS, R. Analysis of the 2007 cyber attacks against Estonia from the

information warfare perspective. Tallin: Corporative Cyber Defence Center of Excellence (CCDCOE), 2008.

OTTIS, R.; LORENTS, P. Cyberspace: Definition and Implications. Tallin, Estonia: Cooperative Cyber Defence Centre of Excellence, 2012.

PARAGUAY. Ministro de Relaciones Exteriores (Rodolfo Nin Novoa). Mensaje publicado en el portal del Ministerio de Relaciones Exteriores de Paraguay el 14 de diciembre de 2018 por Rodolfo Nin Novoa, Ministro de Relaciones Exteriores de Paraguay. Asunción, 2018.

PELTON, J.; SINGH, I. Digital Defense: A Cybersecurity Primer. New York: Springer, 2015.

PIEDRA, D. Lecciones de aprendizaje, transferencia de políticas y la difusión internacional de la política Ideas. Centrer for the Study of Globalisation and Regionalisation, [S.l.]:p. 41, 2001.

POLETTI, R.; DOBBS, B. A resiliência: a arte de dar a volta por cima. Tradução de Stephania Matousek. Petrópolis, RJ: Vozes, 2007.

PUCHALA, D. Of blead men, elephants and international integration. Londres: Journal of Common Market Studies, X-No 3, p. 277, 1972.

RELIA, S. Cyber Warfare: Its Implications on National Security. New Delhi: Vij Books India Pvt Ltd, 2015.

RICHARDS, J. Cyber-War: The Anatomy of the Global Security Threat. London: Palgrave Pivot, 2014.

RODRIGUES, K. F.; RODRIGUES, I. S. Process tracing: o método,

inovações e perspectivas para o campo da Administração Pública. V Encontro Brasileiro de Administração Pública - Universidade Federal de Viçosa, [S.l.]: p. 15, 2017.

ROWLAND, J.; RICE, M.; SHENOI, S. The anatomy of a cyber power. [S.l.]: International Journal of Critical Infrastructure Protection, Sv. 7, n. 1, p. 3–11, 2014.

RUDIO, F. Introdução à pesquisa científica. São Paulo: Livraria Grandes Editores ltda, 1978.

SABATIER, P.; JENKINS-SMITH, H. The Advocacy Coalition Framework: Assessment, Revisions and Implications for Scholars and Practitioners. Boulder: Westview Press, 1993.

SABATINI, C.; ALBERTONI, N. Prosur y el mito de la integración latinoamericana. New York Times, New York, 29 de marzo de 2019.

SAMPIERI, R.; FERNÁNDEZ COLLADO, C.; BAPTISTA LUCIO, P. Metodología de la Investigación. 6ta Ed ed. México DF: Mc Graw Hill Education, 2014. SANCHEZ, F [et al]. Psicología Social. Madrid: McGraw-Hill, 1993.

SCHMITT, M. Tallinn Manual on the International Law Applicable to Cyber Warfare. New York, United States of America: Cambridge University Press, 2013.

SENGE, P. La quinta disciplina en la práctica: estrategias y herramientas para construir la organización abierta al aprendizaje. Buenos Aires, Ediciones Granica S.A, 2006.

SERRANO, A.; MARTINEZ, E. La Brecha Digital: Mitos y Realidades. México: UABC, 2003.

SHANNON, R. Simulación de Sistemas. Diseño, desarrollo e implementación. México: Trillas, 1988.

SIERRA, D. Las dos caras de la tecnología. [S.I.]: Informe mensual de ciberseguridad, v. 2, p. 16, 2015.

SIERRA BRAVO, B. Ciencias sociales. Epistemología, lógica y metodología. Madrid: Paraninfo, 1988.

STEL, E. Guerra Cibernética. Buenos Aires: Círculo Militar, 2005.

SUAREZ, E.; MELILLO, A. Resiliencia: Descubriendo las propias fortalezas. Buenos Aires: Paidós, 2005.

SUNKEL, A.; PAZ, J. El subdesarrollo latinoamericano y la teoría del desarrollo. México: Editorial Siglo 21, pp. 15-268, 1981.

TADDEO, M.; GLORIOSO, L. Ethics and Policies for Cyber Operations. A NATO Cooperative Cyber Defence Centre of Excellence Initiative. Switzerland: Springer International Publishing, 2017.

Tallinn Manual on the International Law Appicable to Cyber Warfare.New York: Cambridge University Press, 2013.

TAVARES, J. Resiliência e educação. 2.ed. São Paulo: Cortez, 2001.

TIKK, E.; KASKA, K.; VIHUL, L. International Cyber Incidents. Legal Considerations. Tallinn: Cooperative Cyber Defence Centre of

Excellence (CCDCOE), 2010.

TRATADO DEL ATLÁNTICO NORTE. Washington DC: Tratado firmado entre los Estados firmantes, 1949.

UE. Parlamento Europeo. Comunicación del a Comisión al Parlamento Europeo y al Consejo sobre "El planeamiento de la UE sobre la resiliencia y la reducción del riesgo de catástrofes en los países en desarrollo: aprender de las crisis alimentarias", 3 de octubre de 2012.

UE. Parlamento Europeo. Action Plan for Resiliencie in Crisis Prone Countries 2013-2020. Bruselas, 2013.

UNASUR. Tratado Constitutivo de la Unión de Naciones Suramericanas. Entrada en vigor el 11 de marzo de 2011. Disponible en: https://www.unasursg.org/images/descargas/DOCUMENTOS%20CONSTITUTIVOS%20DE%20UN UNASUR-solo.pdf.

VAN CREVELD, M. Technology and War: From 2000 B.C. to the Present.Washington: Simon and Schuster, p. 246, 2010.

VERGARA, S. Métodos de pesquisa em administração. São Paulo: Atlas, 2008. WARTOFSKY, M. Introducción a la filosofía de la ciencia. Madrid: Alianza editorial, 1983.

WEYLAND, K. Bounded rationality and policy diffusion: social sector reform in Latin America. New Jersey: Princeton University Press, 2006.

WILLIAMS, B. The Joint Force Commander´s Guide to cyberspace Operations. Unites States: Joint Force, Quarterly 73, p. 14, 2014.

ZIOLKOWSKI, K. (ed.). Peacetime Regime for State Activities in Cyberspace. Tallinn: International Relations and Diplomacy, NATO CCD COE Publication, 2013.

SÍNTESIS DEL CURRÍCULUM DE MARIANO OSCAR GÓMEZ

- Oficial del Ejército Argentino.
- Oficial de Estado Mayor del Ejército Argentino (ESG), Oficial de Estado Mayor Conjunto (ESGC) y Oficial de Estado Mayor del Ejército de Brasil (ECEME).
- Licenciado en Administración (UNDEF - Argentina).
- Magister en Dirección Estratégica en Telecomunicaciones (Universidad Europea Miguel Cervantes – España).
- Magister en Ciencias Militares con orientación en Defensa Nacional (Instituto Meira Mattos (IMM) – ECEME - Brasil).
- Posgrados Universitarios de nivel Especialización en: Conducción de Operaciones Militares (EsAO – Brasil); Conducción de Organizaciones Militares Terrestres (ESG - Argentina); Estrategia Operacional y Planeamiento Militar Conjunto (ESGC - Argentina); Ciencias Militares (ECEME - Brasil).