Mincyt
Ministerio del Poder Popular para Ciencia y Tecnología

oncti
Observatorio Nacional de Ciencia, Tecnología e Innovación

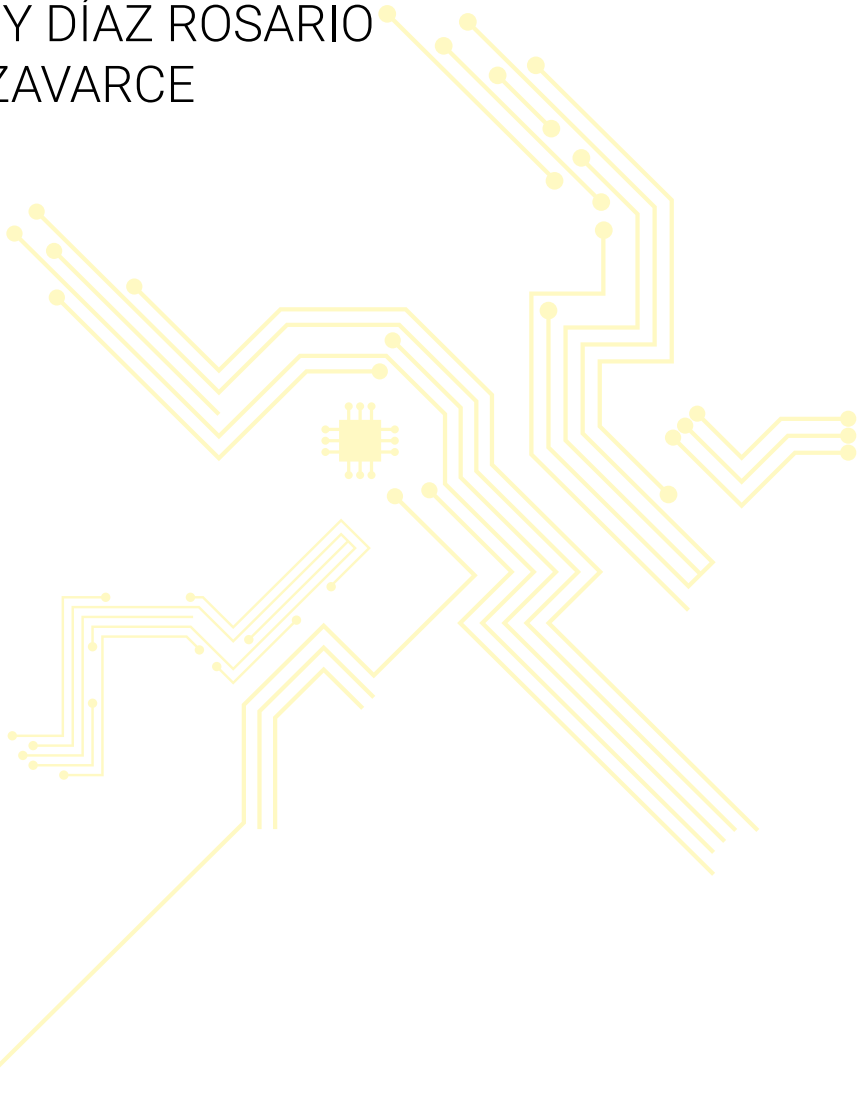
MODELO DE ORGANIZACIÓN CIBERNÉTICA DEL COMANDO CIBERNÉTICO NACIONAL

KENNY DÍAZ ROSARIO
CARLOS ZAVARCE CASTILLO

UMBV
Editorial Hormiguero UMBV

MODELO DE ORGANIZACIÓN CIBERNÉTICA DEL COMANDO CIBERNÉTICO NACIONAL

TCNEL. KENNY DÍAZ ROSARIO
DR. CARLOS ZAVARCE



CARACAS, NOVIEMBRE DE **2020**

Fondo Editorial

Ediciones oncti

© Kenny Díaz Rosario
Carlos Zavarce Castillo
Título: Modelo de organización cibernética del comando cibernético nacional

Edición: Noviembre, 2020
© Observatorio Nacional de Ciencia, Tecnología e Innovación
Fondo Editorial Ediciones Oncti

Co-Edición Editorial Hormiguero
Universidad Militar Bolivariana de Venezuela

Coordinadoras de Edición:
Magally Briceño y Fabiola Ortúzar
Correctora de Estilo:
Bárbara Caraballo
Diagramación:
Natalia Morao
Diseño de Portada:
Mónica Piscitelli

Comentarios y Sugerencias:
divulgaciones.CTI@oncti.gob.ve
publicaciones.oncti@gmail.com

Teléfono:
0212- 5557758 / 5557594

Dirección:
Av. Universidad, Esquina del Chorro.
Torre Ministerial. Piso 16.
Caracas, Venezuela.

Depósito Legal: DC2020001172
ISBN: 978-980-7508-15-5

KENNY DÍAZ ROSARIO

Es Licenciado en Ciencias y Artes Militares, egresado de la Academia Militar de Venezuela, donde fue Alférez Mayor de la promoción Coronel Juan José Rondón, año 2002. Es Especialista en Infantería egresado del Centro de Estudios Tácticos, Técnicos y Logísticos. Magister Scientiarun en Seguridad de la Nación, egresado del Instituto de Altos estudios de Seguridad de la Nación, ambas instituciones adscritas a la Universidad Militar Bolivariana de Venezuela. Magister Scientiarun en Finazas, egresado de la Universidad santa maría. Profesor Agregado de la Academia Militar de Venezuela. Coautor con el Dr. Carlos Zavarce de los artículos *"Comando Cibernético Nacional"* publicado en la Revista Columnata. Vol XI-2019, Fondo Editorial Hormiguero, de la Universidad Militar Bolivariana de Venezuela (UMBV). y de los Artículos *"Hacia una organización disruptiva en materia de ciberseguridad de la República Bolivariana de Venezuela"* y *"Gestión de riesgos y condicionalidad política de la cooperación internacional en tiempos de Coronavirus en Venezuela"*, publicados en la Revista El Observatorio del Conocimiento. Vol 4- Nº 1 Septiembre – Diciembre 2019 y Vol. 5 - Nº 1 Enero - Abril 2020, del Observatorio Nacional de Ciencia y tecnología (ONCTI). Actualmente se desempeña como Director General del Despacho de la Vicepresidencia de la República.

CARLOS ZAVARCE CASTILLO

Es Licenciado en Administración, Mención Informática egresado de la Universidad Nacional Experimental Simón Rodríguez, con estudios de Especialización y Maestría en el área de informática. Doctorado y Post Doctorado en Ciencias Sociales por la Universidad Central de Venezuela. Post Doctorado en Ciencias Gerenciales de la Universidad Nacional Experimental de las Fuerzas Armadas. Post Doctorado en Seguridad de la Nación de la Universidad Militar Bolivariana de Venezuela. Profesor Titular de la Universidad Central de Venezuela. Profesor invitado del Instituto de Altos Estudios de la Seguridad de la Nación. Entre sus últimas publicaciones destacan la coautoría con el PhD Manuel Mariña, en la obra *"Modelo de Sistemas Viables para la Seguridad de la Nación"*. Coautor con el Dr. Víctor Córdova y el VA. Gilberto Pinto Blanco, en las obras *"Ética, Socialismo y Organización"*; *"Socialismo, Modos de Vida y Nuevas Tecnologías de Información"*; "*Gestión Pública y Ética Socialista"*; *"Eficiencia o nada: Derroteros de la Revolución Bolivariana"*, Publicaciones Editadas por el Comando Superior de Educación de la Armada Bolivariana de Venezuela Bolivariana de Venezuela. Actualmente se desempeña como Director Ejecutivo del Observatorio Nacional de Ciencia, Tecnología e Innovación (ONCTI).

ÍNDICE

ÍNDICE DE CUADROS

Pág.

ÍNDICE DE GRÁFICOS

Pág.

ÍNDICE DE FIGURAS

PRÓLOGO

Con la entrega de un proyecto, donde planteaba investigar sobre el desempeño de la información, como un "nuevo factor de poder", fui aceptado como aspirante a un Ph.D., en el Depto. de Cibernética de la Universidad de Brunel, en Londres, Inglaterra.

Era el año 1978. Como tutor de la investigación, me fue asignado un profesor, de gruesa y blanca barba, llamado Stafford Beer. Teórico británico, académico, y consultor, conocido por su trabajo en los campos de la investigación operacional y cibernética organizacional, Presidente de "The World Organization of Systems and Cybernetics".

Bajo su tutela, cuatro años más tarde, con el título "Vulnerable Sovereignty A Cibernetic Essay un Political Sciences", defendí la Tesis Doctoral que me permitió regresar al País, como "Doctor of Philodophy in Cibernetics"

Como docente de la UCV, a los pocos días de mi regreso, asumí el cargo de Director de Postgrado de la Facultad de Economía y, por supuesto, me encargué de la Cátedra de Cibernética de la Maestría en Ciencias Administrativas.

Los meses transcurrieron y muchos de los aspirantes a Magister Scientiarum, se entusiasmaron con el tema de la cibernética aplicada al estudio de organizaciones complejas. Pero hubo un estudiante que me solicitó la tutoría de su Trabajo de Grado, su nombre era Carlos Zavarce.

Luego de la disertación de su Trabajo de Grado, el entonces Magister Scientiarum. Carlos Zavarce, se dedicó a la docencia e investigación. En su desarrollo académico y luego de realizar un Doctorado en Ciencias Sociales en la UCV, se convirtió en un consecuente promotor de la Ciencia Cibernética en las aulas de clase tanto de la UCV como de la UMBV, donde se ha estado desempeñando como docente invitado de los Programas de Postgrado en el Instituto de Altos Estudios de la Seguridad de la Nación (IAESEN).

Quienes dictamos clases desarrolladas dentro del ámbito de la Línea de Investigación en Cibernética, asumimos como eje transversal de la asignatura, el estudio

de un constructo teórico creado por el Prof. Stafford Beer, conocido como el "Modelo de Sistema Viable" (MSV). Se trata de un modelo que irrumpe en el campo del diseño, desarrollo y gestión institucional, con una propuesta basada en las leyes que garantizan la excelencia en el funcionamiento de los sistemas naturales, su objetivo es la regulación y el control.

Durante los años que hemos tenido la oportunidad de participar en charlas, conferencias y tarimas de clase, promoviendo el estudio de la cibernética y de las leyes, principios y elementos teóricos conceptuales que sustentan el carácter transformador de del MSV, confieso que, tal vez, precisamente, por la alta concepción matemática - probabilística, que propone el modelo para el logro de la regulación de la planificación, o por su impacto, como un paradigma organizacional que irrumpe sobre sobre los arraigados modelos de gestión administrativa clásicos ya incrustados en nuestras instituciones, lo cierto es que, el tiempo de su discurso académico, continúo por años, sin que el MSV , lograra trascender el aula de clases.

Pero, así como Stafford Beer, fue mi tutor en Brunel University y me convertí en vocero de la causa cibernética vista como "la ciencia del control y la regulación de los sistemas dinámicos complejos dónde la información juega un papel escencial", más tarde me tocó ser el Tutor de Carlos Zavarce, quien, siguiendo la causa cibernética, se encontró con otro joven estudiante que le pidió lo acompañara, en la tutoría de su Trabajo Grado del Instituto de Altos Estudios de la Seguridad de la Nación.

.

Así es que, en una suerte de tutorías, casi generacionales, el Prof. Zavarce aceptó la tutoría de un joven militar, esta vez, un inteligente cursante de la Maestría en Seguridad de la Nación, de nombre Kenny Díaz.

Bajo el título "Modelo de Organización Cibernética para el Comando Cibernético Nacional", el Tcnel. Kenny Díaz Rosario, logro desarrollar una inédita propuesta de lo que podríamos identificar como un trabajo de verificación práctica de aplicación del MSV, fuera de las paredes del aula universitaria.

En cinco capítulos, el Tcnel. Díaz Rosario, presentó al jurado examinador de su Trabajo de Grado, una extraordinaria propuesta que, luego de cubrir las exigencias epistemo-ontológicas requeridas para un dictamen favorable, concluye con ocho recomendaciones que, en nuestra opinión, representan el inicio de lo que podría ser "un cambio paradigmático salido de la academia".

El patriota soldado Kenny, con el aporte que, en este libro prologamos, estaría iniciando lo que podría ser un cambio de paradigma en la lucha por la instauración de estructuras organizacionales capaces de alcanzar una verdadera eficacia y eficiencia, en la gestión institucional de la Seguridad Integral de la Nación.

Ph.D Manuel Mariña Muller

PRESENTACIÓN

Es para mí un honor, como Presidente de la Fundación Muronto, Centro de Innovación para el Desarrollo de la Fuerza Armada Nacional Bolivariana, presentar esta publicación editada por el Observatorio Nacional de Ciencia, Tecnología e Innovación, en alianza con el Fondo Editorial Hormiguero, de la Universidad Militar Bolivariana de Venezuela, titulada "La Organización Cibernética del Comando Cibernético Nacional", cuya autoría corresponde al Tcnel. Kenny Diaz Rosario y al Dr. Carlos Zavarce Castillo.

Por ello, en primer lugar y en lo personal, no puedo menos que reconocer la contribución de los autores, quienes desde la trinchera académica e investigativa, aportan elementos conceptuales disruptivos, para la conformación de un Comando Cibernético Nacional, desde la perspectiva de la Teoría Cibernética, contribuyendo con una vieja aspiración de la Fuerza Armada Nacional Bolivariana, de debatir la pertinencia de contar con un ente rector, encargado de garantizar el Ciberespacio de la República Bolivariana de Venezuela.

No hay duda que, el llamado Ciberespacio, es el gran impulsor de avances sin precedentes que hoy trae consigo un nuevo tipo de amenazas globales, cuya orientación está marcada por tasas de innovación tecnológica crecientemente aceleradas, que modifican aspectos básicos en los procesos de seguridad física y lógica, y que atentan contra las infraestructuras críticas relacionados con la Seguridad y Defensa de las Naciones.

Y en tal sentido, quisiera resaltar que la ciberseguridad constituye una de las tendencias predominantes en el mundo actual, que impone a los gobernantes, líderes sociales y empresariales, cualquiera sea el modelo de desarrollo que estos promuevan, la toma de conciencia y acción, ante el acelerado crecimiento de la rata de ciberataques, que hacen que las prognosis más fundamentadas en materia de seguridad nacional estén permanentemente en tela de juicio.

En consecuencia, tanto en el discurso como en las orientaciones de política asociadas a la Seguridad de la Nación, se evidencian legítimas preocupaciones para hacer frente a las nuevas amenazas que trae consigo este nuevo campo de batalla conocido como el Ciberespacio.

Así que, vaya mi felicitación a los autores de esta obra, quienes, desde el seno del Instituto de Altos Estudios de Seguridad de la Nación, de la Universidad Militar Bolivariana de Venezuela, y como resultado de un intenso trabajo investigativo, reivindican con esta publicación el esfuerzo y dedicación de la Comunidad Científica y Tecnológica de la Fuerza Armada Nacional Bolivariana.

GD. Armando Villarroel
Presidente de la Fundación Muronto
Centro de Innovación para el Desarrollo de la FANB.

INTRODUCCIÓN

Basta solo revisar la sección de noticias del portal del Observatorio Nacional de Ciencia, Tecnología e Innovación (ONCTI), para percartarse de las más variadas referencias de ciberataques a ciudadanos, organizaciones, empresas y hasta instalaciones críticas de países, sobre todo en estos tiempos signados por la pandemia de la covid-19.

En un contexto tan particular como este, desde instalaciones que garantizan el funcionamiento de los sistemas públicos y privados salud, pasando por empesas públicas y privadas, así como infraestructuras críticas que soportan servicios públicos como telecomunicaciones, banca, energía eléctrica, sistemas de transporte multimodas, instalaciones asociadas a la industria petrolera y petroquimica, y hasta fábricas de diferentes índoles, reportan haber sido, en tiempos de pandemia, objeto de ciberamenazas, y en consecuencia son a diario reseñadas en los diferentes medios de comunicación social, no solo escritos, sino también en radio, televisión y, naturalmente, los medios electrónicos a través de internet.

Esta particular situación se origina además en momentos en que más trabajadores realizan actividades remotas soportadas en infraestructuras públicas y privadas de internet, donde a la vez se cuenta con menos personal del área tecnológica (TI) y seguridad de información, listo para mitigar ataques e intrusiones cibernéticas, configurándose un ambiente propicio para que los ciberdelincuentes exploren vulnerabilidades para activar ataques cibernéticos. Con esto, la situación de pandemia generalizada ha creado condiciones propicias que aumentan la probabilidad de éxito de ataques cibernéticos y de allí la necesidad de contar con organizaciones dedicadas a atenuar el impacto de las mismas en la necesaria búsqueda de adaptación, regulación y control que permitan el logro de la estabilidad, y en el peor de los casos, el retorno a la calma, luego de una perturbación de esta naturaleza. Y este el tema central de nuestra obra. Toda vez que, en materia de seguridad, en las últimas dos décadas el llamado ciberespacio se ha consolidado una nueva dimensión de actuación donde nuevos actores pueden materializarse novedosas e insospechadas amenazas.

Si antes en el ámbito de la seguridad y defensa se consideraba como ámbitos de acción las dimensiones de tierra, mar y aire, e incluso el espacio superior suprayacente, ahora con el desarrollo vertiginoso de las telecomunicaciones se ha habilitado una dimensión adicional, que se encuentra en una dinámica evolución.

En tal sentido, y dado su interés como novedoso objeto de estudio, por materializar la existencia real de un nuevo campo de batalla debido a los riesgos y amenazas que su uso masivo plantea a la sociedad contemporánea, es por lo que en definitiva, el ciberespacio constituye una nueva dimensión para los estudiosos de la seguridad y defensa, caracterizada no solo por la ubicuidad de sus actores, sino por la inexistencia de fronteras y el potencial para confrontaciones de carácter asimétrico.

En este contexto, la República Bolivariana de Venezuela no ha permanecido inmune a las agresiones que utilizan el ciberespacio para atentar contra los más variados aspectos de la seguridad, llegando a verse comprometidos servicios críticos como el funcionamiento de la Industria Petrolera Nacional en el año 2009, los servicios de pago electrónico en el año 2014, la conectividad prestada por la empresa de Telecomunicaciones del Estado Venezolano Movilnet en el año 2016, las redes sociales y páginas web de instituciones públicas durante los años 2016- 2018, y entre los años 2019-2020 los intentos de ciberterrorismo frustrados contra la nación mediante el empleo de tres vehículos aéreos no tripulados de pequeño tamaño (Drones), así como el constante sabotaje al Sistema Eléctrico Nacional; eventos de carácter sociotecnológicos que con motivo de la pandemia de la covid-19 y ante la necesidad de mantener prosecución de actividades de diferente índole en casa, sin duda alguna se han intensificado, causando daños irreparables a la seguridad de la nación.

No obstante, es quizás a partir del ataque cibernético contra el Sistema Eléctrico Nacional cuando especialistas en la materia en asociación con expertos de naciones aliadas como Rusia y China, han llamado la atención sobre la necesidad de estudiar en profundidad no solo cuáles fueron las amenazas y los riesgos derivados en materia de Ciberseguridad sino el cómo prepararnos para que los organismos responsables de la Estrategia Nacional de Ciberseguridad puedan prever, responder y en última instancia, lograr adaptación, regulación y control al momento de ocurrir un evento de esta naturaleza.

Esto, toda vez que los eventos cibernéticos de alto impacto social de más reciente data, que se han suscitado antes y con motivo de la pandemia, y que por su naturaleza no han tenido la cobertura mediática, son elementos que en los actuales momentos constituyen la base de partida en la discusión del anteproyecto de Ley Constitucional del Ciberespacio de la República Bolivariana de Venezuela, que plantea la necesidad de desarrollar los derechos constitucionales, principios orientadores, procesos, bases y lineamientos del ciberespacio de nuestro país, con el objeto de contribuir a generar las condiciones que garanticen la seguridad de la Nación.

Para todo ello, la creación de una autoridad competente, que sea rectora en la organización de la necesaria sinergia que ha de darse entre los actores del Sistema Nacional del Ciberespacio de la República Bolivariana de Venezuela (tales como la Dirección de Ciberdefensa de la Fuerza Armada Nacional Bolivariana, el Consejo Científico Tecnológico Presidencial, el Consejo Científico Tecnológico Militar, la Suscerte, el CICPC, entre otros entes), que hoy se encuentran en colaboración con las entidades supranacionales en la esfera de la ciberseguridad, de gran utilidad para identificar nuevas amenazas y riesgos que siguen latentes, deberían integrarse para identificar la dimensión organizativa del problema e intercambiar experiencias que pudieran eventualmente redundar en un incremento de los niveles en materia de ciberseguridad a nivel nacional.

En consecuencia, es esta la situación que generó las condiciones para impulsar la investigación que da origen a

esta publicación, y que se concretó con la presentación y defensa de un Trabajo de Grado ante el jurado evaluador designado por el Instituto de Altos Estudios de la Seguridad de la Nación (IAESEN), adscrito al Centro de Estudios Estratégicos y Polemológicos de la Universidad Militar Bolivariana de Venezuela, investigación que obtuvo la calificación de "Excelente" con mención "Honorífica y Publicación", al explorar la pertinencia de formular un modelo teórico que explicita la lógica organizacional que habría de adoptar el Comando Cibernético Nacional, entendido este como la instancia rectora prevista en el anteproyecto de Ley Constitucional del Ciberespacio de la República Bolivariana de Venezuela, para el abordaje de los diferentes procesos que hoy se ejecutan a través de diferentes estructuras organizativas de carácter técnico que existen a nivel nacional, los cuales habrán de alinearse en torno al objetivo de hacer frente a los desafíos que el uso del ciberespacio tiene para la seguridad integral de la nación.

Lo anteriormente mencionado surge en la aspiración de poder afrontar de modo coherente los retos y desafíos que plantea el acceso al Ciberespacio de la República Bolivariana de Venezuela, que hoy se encuentra asechado por intereses imperiales y que sin duda consiguen en el ámbito tecnológico nichos de riesgos para la seguridad integral de la nación.

Así pues, desde esta plataforma organizacional que ha sido formulada y propuesta por los autores de esta investigación, la cual está inspirada en los planteamientos de la Cibernética Organizacional, se fomentaría la necesaria sinergia entre el ecosistema de organizaciones públicas y privadas que, haciendo vida en el territorio nacional, tienen las competencias e infraestructuras requeridas para que en materia de ciberseguridad se pueda contribuir a generar las condiciones que garanticen la seguridad del Ciberespacio de la República Bolivariana de Venezuela, con el fin de dar cumplimiento al mandato constitucional relacionado con la seguridad y defensa de la nación.

De allí que la propuesta de creación del Comando Cibernético Nacional emerge como un reto para los actores de lo que sería el Sistema Nacional del Ciberespacio de la República Bolivariana de Venezuela, quienes en el ejercicio de sus nuevos y múltiples compromisos deben percibir las preocupaciones sociales, enalteciendo desde su accionar la lucha en contra de novedosas amenazas que buscan vulnerar las infraestructuras críticas, las cuales dan soporte a la prestación de servicios públicos, garantes actuales de la paz ciudadana, aún con las condiciones de asedio a las que se enfrenta la dinámica económica, política y social del Estado Venezolano; sin descartar, como ingrediente gerencial, la racionalización y el uso de los recursos por la vía de la eficacia, eficiencia y pertinencia administrativa de las instituciones dedicadas a la prestación de este particular servicio de la seguridad nacional.

Para llevar a cabo la investigación, se hizo uso de Modelo de Sistemas Viables (MSV), ampliamente considerado como una de las mayores contribuciones teóricas que desde la teoría Cibernética apalancan la Cibernética Organizacional y con ello el desarrollo del campo de la teoría organizacional. Dicho modelo

proveyó la plataforma teórico-conceptual para el abordaje de la complejidad organizacional en materia de ciberseguridad en la República Bolivariana de Venezuela, a través de la identificación del entramado de propósitos, capacidades y relaciones que hoy mantienen el ecosistema de ciberseguridad en el país en sus diferentes niveles de recursión, lo que permitió con base en la caracterización de las mejores prácticas en uso por partes de países como Estados Unidos, China y Rusia, determinar elementos de creación de valor en materia de Ciberseguridad con el fin de formular el Modelo de Organización Cibernética del Comando Cibernético Nacional para la República Bolivariana de Venezuela, el cual ha sido pensado de forma tal que cuente con capacidades de adaptación, regulación y control que le permitiera generar señales de alerta temprana en materia de ciberseguridad, mucho antes de que estas generen crisis o contingencias en las plataformas críticas de la nación, de manera que se creen los correctivos a tiempo para el retorno a la calma después de una eventual perturbación.

En esta perspectiva, los contenidos que aquí se presentan invocan las premisas del Enfoque de Sistemas, la Cibernética Organizacional, y en particular, el Modelo de Sistemas Viables (MSV) para identificar, conocer y comprender las fuerzas internas y externas que motorizan y direccionan las estructuras, acciones y procesos de las instituciones dedicadas a la Ciberseguridad del Estado Venezolano, lo cual permitió formular un modelo teórico que pensamos podría contribuir a la transformación estratégica de los servicios estadales de ciberseguridad, para hacerlos eficaces y eficientes dotados de una arquitectura innovadora, dinámica y flexible.

Para dar cuenta del proceso investigativo que se adelantó, esta publicación se ha estructurado en cuatro (04) momentos.

Momento I, *"Aproximación al Objeto de Estudio"*: Contiene la contextualización y problematización de la situación que originó la investigación, la formulación de las interrogantes que guiaron la indagación, así como los objetivos generales y específicos propuestos; también se resalta la importancia y justificación de su realización. Posteriormente, a efectos de ejemplificar el cómo justificar metodológicamente una investigación, se presenta la metódica que guió a la misma, de forma que quedan plenamente argumentados los aspectos metodológicos de esta, tales como el abordaje epistemológico, el tipo y diseño de investigación, el método empleado, y los protocolos técnicos para la recolección de datos e informaciones.

Momento II, intitulado *"Saberes para Construir el Modelo"*: Incorpora los elementos constitutivos del referencial teórico al cual se aproximan los autores, entre los cuales se incluyen las bases conceptuales en torno a tres ejes temáticos. El primero de ellos, dirigido a la temática del Ciberespacio y de los riesgos que en él se generan. El segundo, orientado hacia la Ciberseguridad, y el tercero de ellos enfocado en la Cibernética Organizacional desde los fundamentos asociados a la Teoría Cibernética Organizacional (Beer, 1977). Todo ello, como insumos básicos necesarios para el despliegue de un sistema de conceptos que permitió avanzar en la conceptualización de un Comando Cibernético Na-

cional.

Momento III, denominado *"Diseño del Modelo de Organización Cibernética del Comando Cibernético Nacional"*: Contiene el producto del proceso de acercamiento a la realidad que permitió concretar la propuesta del Modelo de Organización Cibernética para el Comando Cibernético Nacional de la República Bolivariana de Venezuela.

Momento IV, identificado como *"A manera de colofón"*: Muestra las conclusiones y recomendaciones que se desprenden de la investigación.

Finalmente, se exhiben las referencias bibliográficas consultadas en el desarrollo de la misma y la inclusión de apéndices que sirven de soporte a la ejecutoria de esta investigación.

Momento I
APROXIMACIÓN AL OBJETO DE ESTUDIO

Contextualización y problematización del Objeto de Estudio

No es la primera vez que el tema de la ciberseguridad está sobre la mesa en un país en vías de desarrollo como Venezuela. Antes de comienzos del presente siglo, con motivo del llamado fenómeno del Y2K, docentes, investigadores y tecnólogos venezolanos habían llamado la atención sobre la necesidad de considerar las vulnerabilidades en materia tecnológica a la que se enfrentan organismos públicos y privados, e inclusive las personas, motivado no solo por apetencias de países dominantes, sino por intereses delictuales de grupos terroristas e incluso individualidades con alto nivel de especialización en la materia.

En aquellos días, el debate estaba guiado por encontrar respuesta a una pregunta central: ¿Estamos preparados para afrontar un desastre de carácter sociotecnológico originado por una guerra de información?

Todo lo ya mencionado surge, en la dirección de alertar no solo sobre las debilidades en materia de seguridad tecnológica de las instalaciones críticas para el buen desenvolvimiento de las actividades económicas y sociales del país, sino sobre el cómo organizarnos para enfrentar contingencias derivadas de un ciberataque, fenómeno que ya en aquel entonces se consideraba que podría ocasionar perturbaciones devastadoras a una sociedad como la nuestra.

No fue sino hasta la materialización de los ataques cibernéticos a la Industria Petrolera Nacional desde el año 1998 al 2002, cuando comenzó a crearse una cierta conciencia, entendida esta como la reflexión permanente sobre lo vulnerable que somos, lo que hacemos y lo que dejamos de hacer en esta materia tecnológica, y por ende, la necesidad estratégica de garantizar el funcionamiento ininterrumpido de la infraestructura tecnológica que da soporte a la prestación de servicios básicos en el país, por parte de entes tanto públicos como privados.

Concurrentemente, en otras latitudes, el debate sobre esta particular temática era motivo de interés permanente no solo por académicos y especialistas en seguridad de la nación, sino por los propios Jefes de Estado. Muestra de ello fue que la discusión en esta materia cobró tal relevancia, que el tema de la ciberguerra adquirió presencia en reuniones de organismos internacionales como la ONU y el G20, donde la discusión sobre este asunto fue aprobada, ya que la Ciberguerra fue entendida como ataques supuestamente patrocinados por diferentes gobiernos que impulsan la estrategia de promover guerras de menor costo, donde se tengan el menor número de bajas físicas y que logren doblegar al adversario en el menor tiempo posible.

Evidencias empíricas que han sido registradas y difundidas en redes sociales dan cuenta, por ejemplo, que en el año 2017 fue el mismo presidente de la Federación Rusa, Vladímir Putin, el que propuso al Gobierno de Estados Unidos pactar un acuerdo sobre seguridad informática después del ataque

WannaCry (en inglés WannaCry ransomware attack o Wanna Cry Doble Pulsar Attack), ataque que se dio el viernes 12 de mayo de 2017 y que ha sido descrito como sin precedentes en tamaño, al lograr infectar más de 230.000 ordenadores en más de 150 países a nivel global, destacando que los países más afectados fueron Rusia, Ucrania, India y Taiwán, así como el servicio nacional de salud de Gran Bretaña (NHS), la Telefónica de España, FedEx, Deutsche Bahn, y las aerolíneas LATAM, junto con muchos otros blancos a nivel mundial.

No obstante, las críticas no se hicieron esperar por esta inesperada posibilidad de cooperación con Rusia, por parte tanto de demócratas como republicamos, al considerar que esta nación era un aliado que nunca será fiable ni constructivo en materia de ciberseguridad a los intereses de los EEUU, razón por la cual el presiente Trump pasó a cuestionar la posibilidad de crear este grupo de trabajo. En tal sentido, el 9JUL17 Donald Trump escribió en su cuenta de twitter:

> **"**The fact that President Putin and I discussed a Cyber Security unit doesn't mean I think it can happen. It can't-but a ceasefire can,& did!**"**
> **"**El hecho de que el presidente Putin y yo discutiéramos una unidad de ciberseguridad no significa que yo piense que eso ocurra. No puede**"**

Con esto quedó evidenciado que el debate sobre el tema de la ciberseguridad era y sigue siendo un tema de agenda mundial, aunque en contextos altamente politizados como el que atraviesa la Venezuela de hoy. La mayoría de ocasiones, cuando se habla de ciberseguridad, los actores en pugna lo consideran o bien, un tema de carácter estratégico nacional, o un tema de ciencia ficción.

Ahora bien, a efectos de este Trabajo de Grado, al emplear el vocablo "ciberataque" nos referimos al uso ofensivo de información y de Sistemas de información para corromper o destruir en el enemigo, su información, sus procesos basados en información, sus sistemas de información y sus redes de computación, mientras se protegen los propios. Tales acciones están diseñadas para obtener ventajas sobre enemigos militares o empresariales, y que son presumiblemente perpetrados por Estados o grupos terroristas especializados, aunque es raro encontrar pruebas que garanticen la autoría del ataque de manazas a infraestructuras del Estado venezolano no son nuevas.

Este tipo de amenazas a infraestructuras del Estado venezolano no son nuevas. La sistematización de eventos de esta naturaleza puede encontrase en el cuadro que se muestra a continuación:

Cuadro Nro. 1. Sistematización de Ciberataques contra Instalaciones del Estado Venezolano

HECHOS	CAUSAS	CONSECUENCIAS
PARALIZACIÓN DE LA INDUSTRIA PETROLERA (1998)	• Outsourcing de Capacidades al Consorcio INTESA filial de SAIC. • Sabotaje a la plataforma tecnológica de la Industria Petrolera Nacional.	• Daños a la Infraestructura Tecnológica. • Fuga de talentos. • Inoperancia de la Industria Petrolera Nacional. • Colapso de la Economía Nacional.
INTERRUPCIÓN PROLONGADA DE LAS TELECOMUNICACIONES MÓVILES VENEZOLANAS (2002).	• Ataque masivo a la infraestructura tecnológica que da soporte a la Red de Telecomunicaciones móviles de Movilnet.	• Paralización de los Servicios de Comunicaciones Móviles prestados por MOVILNET. • Incomunicación de Industrias, Comercio, Banca y Finanzas, Empresas y ciudadanos.
INTERRUPCIÓN DEL SISTEMA DE PAGOS ELECTRÓNICOS.	• Ataque masivo a la infraestructura tecnológica del Consorcio CREDICAR que da soporte a la Red de Telecajeros y Puntos de Venta.	• Paralización de los Servicios de Intermediación Financiera. • Incomunicación , Comercio , Banca y Finanzas, Empresas y ciudadanos.
VULNERACIÓN SITIOS WEB Y REDES SOCIALES DE ORGANISMOS PÚBLICOS (2014)	• Llamado continuado a Guarimbas por parte de Grupos Opositores al Gobierno Nacional.	• Desinformación a la ciudadanía. • Zozobra y desesperanza en la población.
DESCONOCIMIENTO POR REDES SOCIALES DE RESULTADO DE LAS ELECCIONES PRESIDENCIALES (2018)	• Resultados adversos obtenidos por Grupos Opositores al Gobierno Nacional.	• Desinformación a la ciudadanía. • Zozobra y desesperanza en la población.
MAGNICIDIO EN GRADO DE FUSTRACIÓN. (2019)	• Empleo de sistemas de movilización espacial (Drones) con fines terroristas.	• Violación del Espacio aéreo en Zonas de Seguridad. • Atentado físico contra el Presidente Constitucional y Altas personalidades.
ATAQUE CONTINUADO DEL SISTEMA ELÉCTRICO NACIONAL.	• Interrupción del Sistema Automatizado de Comando y Control de Güri. • Interferencia electromagnética a líneas de transmisión. • Ataque continuado contra plataformas tecnológicas y físicas que soportan el Sistema Eléctrico Nacional.	• Suspensión del Servicio Eléctrico a nivel nacional por mas de 72 horas. • Paralización del Circuito Económico Nacional. • Zozobra y desesperanza en la población.
INCORPORACIÓN DE NUEVOS ACTORES Y AMENAZAS NACIONALES E INTERNACIONALES. (2019)	• Agudización de la crisis política venezolana. • Inherencia extranjera.	• Aparición de nuevas amenazas que vulneran Plataformas de Servicios Críticos. • Corromper y vulnerar la mente de la población.

Fuente: Elaboración propia de los autores, (2020).

De allí que, en la actualidad, el gobierno venezolano, así como los de naciones aliadas, tienen más claro que nunca que deben tomar medidas para protegerse.

La sistematización de ciberataques contra el Estado venezolano presentada en el Cuadro Nro.1, muestra la tendencia creciente en esta actividad y cómo infraestructuras críticas han sido vulneradas. De igual manera, resalta que el ataque cibernético contra el sistema informatizado de control de la Central Hidroeléctrica Simón Bolívar (Guri) en el estado Bolívar, se materializó con la interferencia del Centro de Comando y Control de la Corporación Eléctrica Nacional, que derivó en la interrupción de la energía eléctrica en más de 80% del territorio nacional, y logró paralizar el proceso de generación y distribución de energía eléctrica nacional por más de 72 horas, con las consecuencias dramáticas que un evento de esta naturaleza dejó a la sociedad venezolana en su conjunto.

Si bien atribuir con certeza quién está detrás de un ataque es muy complejo, en este particular evento todo apunta a que el ataque tiene autoría intelectual y material en el Gobierno de los EEUU y su aliado, Canadá, y en tal sentido, no se hicieron esperar las denuncias de especialistas en el tema como las de los voceros oficiales de diferentes gobiernos, argumentando que el gobierno de dicho país estuvo detrás. Así lo deja entrever un reciente artículo publicado por la revista Forbes (2019), firmado por un colaborador llamado Kalev Leetaru, experto en Inteligencia Artificial y Big Data, quien con el sugestivo título "¿Podría el apagón de Venezuela realmente ser un ciberataque?", subraya que los 'ciberataques' existen, e intenta revelar al mundo que este tipo de estrategias son una realidad, y que Estados Unidos tiene la capacidad de efectuar un ataque de esta magnitud. Adicionalmente, destaca que en el futuro estos serán el tipo de ataque que se ejecutarán entre países, enfatizando además que es "realista" pensar que una potencia como Estados Unidos podría fácilmente atacar a Venezuela, debido a que el país cuenta con un internet obsoleto y una infraestructura fácil de quebrantar, que haría relativamente fácil remover cualquier tipo de rastro de una intervención extranjera.

Por su parte, la portavoz oficial del Ministerio de Asuntos Exteriores de la Federación Rusa, María Zajárova, aseguró en relación a este evento (2019) que el apagón que afectó a Venezuela durante varios días fue originado por un ataque informático internacional, enfatizando que: "…el ataque a distancia fue realizado con equipamiento …". "…fue producido en Canadá y estuvo dirigido contra el sistema de control de las principales estaciones de distribución eléctrica, y estas acciones dañinas contra objetivos de la infraestructura de los cuales depende directamente la vida de personas, son usadas cada vez con mayor frecuencia como parte de la llamada guerra híbrida".

De igual manera, en este contexto, en fecha 14MAR19, el presidente Nicolás Maduro Moros , ante estos acontecimientos, informó a la opinión pública nacional e internacional que había solicitado apoyo de la ONU y de expertos en Rusia, China, Irán y Cuba, "países con gran experiencia en estos temas de la defensa a los ciberataques", y que designó una comisión presidencial de in-

vestigación encabezada por la vicepresidenta de la República Delcy Rodríguez, con participarán el Ministerio Público, el Consejo Científico Nacional, e institutos científicos del país encargados de estudiar el ciberataque que afectó el sistema eléctrico nacional.

De esta manera, el ciberataque al sistema eléctrico nacional emergió como un hecho irrefutable, cuyas consecuencias evidencian más allá de las causas imperiales que le dieron origen, la debilidad de la estrategia y organización nacional para prever y contrarrestar ataques cibernéticos, quedando demostrado en el mejor de los casos, vacíos e insuficiencias del Estado venezolano para actuar de manera efectiva y lograr adaptación, regulación y control de la situación, a fin de garantizar la seguridad de la nación en este contexto.

Importa destacar que, ante los eventos reseñados, la institucionalidad del Estado venezolano para hacerle frente a este tipo de amenazas (organismos dedicados a la ciberseguridad) se mostró incapaz de anticiparse a estas amenazas para generar señales de alerta temprana, y mucho menos estabilizar (lograr adaptación) las infraestructuras afectadas con un tiempo de reacción que fuera imperceptible a los usuarios de las mismas.

Esto obedeció, entre otras causas, no solo a la falta de planes, sino a la inexistencia de una organización rectora capaz mantener alineación estratégica de forma tal de sincronizar las capacidades instaladas en organismos tales como el Comando Estratégico Operacional de la Fuerza Armada Nacional Bolivariana, a través de la Dirección Conjunta de Ciberdefensa (DICOCIBER); el Ministerio de Ciencia y Tecnología, a través de sus órganos adscritos como el Centro Nacional de Tecnologías de Información (CNTI), la Superintendencia de Certificación Electrónica (SUCERTE) con su Sistema Nacional de Gestión de Incidentes Telemáticos de Venezuela (VenCERT), y el Centro Nacional de Informática Forense (CENIF), que además incorpora al Ministerio del Poder Popular para las Relaciones Interiores, Justicia y Paz a través de la División Contra Delitos Informáticos del CICPC, a fin de ejecutar con calidad estrategias de mitigación de riesgos.

Así, se pone en evidencia vacíos estratégicos y organizacionales para que las capacidades y talentos se alineen en torno al logro de los propósitos que el Estado venezolano tenga en materia de Ciberseguridad, de forma tal de combatir con calidad las amenazas reales que se ciernen sobre este en dicha materia.

De esta manera, los mencionados eventos han puesto en evidencia los vacíos legales e institucionales existentes en un modelo de creación de valor, que al no existir, hace que hoy se dificulte la articulación de las capacidades instaladas (estructuras de funcionamiento e infraestructuras tecnológicas) así como las relaciones (alianzas estratégicas) puestas en marcha por los organismos de seguridad nacional e internacional, para contar con una organización rectora en materia de ciberseguridad, que pueda explorar y generar innovaciones disruptivas, como por ejemplo, constituirse en una organización altamente adaptativa diseñada bajo los preceptos de la cibernética organizacional que, entre otras, pueda adoptar las estrategias

contenidas en el pacto de cooperación esbozado en un su momento por la Federación Rusa en el G20; estrategias cada vez más pertinentes para la Seguridad y Defensa Integral de la Nación, a los fines de contrarrestar eventuales amenazas en materia ciberseguridad nacional, toda vez que tanto a lo interno, como de cara a las confrontaciones con otras naciones que intenten constreñir la consolidación del proceso de cambio nacional, existen otras organizaciones de ciberseguridad y ciberdelincuentes que cuentan con novedosas estructuras, estrategias y técnicas para aprovechar la más mínima vulnerabilidad de las plataformas tecnológicas que hoy soportan las infraestructuras vitales de la nación, manipulando dispositivos críticos o instalando en ellas 'software' maliciosos que pueden alterar, corromper o robar los activos de información requeridos para su correcto funcionamiento.

En esta dirección se avanzó en la formulación de un Modelo de Organización Cibernética para el Comando Cibernético Nacional, instancia que ha sido pensada para que, atendiendo al Anteproyecto de Ley Constitucional del Ciberespacio de la República Bolivariana de Venezuela, asuma la rectoría a nivel nacional en materia de Ciberseguridad, de manera tal de minimizar las vulnerabilidades que hoy emergen de la explotación del Ciberespacio.

Las consideraciones antes reseñadas ponen en evidencia que la Ciberseguridad del Estado Venezolano es hoy todo un desideratum, no solo por lo difuso y complejo del ciberespacio de la República Bolivariana de Venezuela, la distribución espacial y densidad poblacional, sino también por la capacidad de adaptación de los entes con los que hoy se cuentan para su garantía y los tiempos de reacción de los mismos ante la ubicuidad de potenciales ciberdelincuentes y los problemas que, producto de las novedosas y disruptivas ciberamenazas, deben enfrentar. Esta falta de funcionalidad y versatilidad compromete la estabilidad de las infraestructuras críticas que permiten la prestación de Servicios Públicos del Estado venezolano.

Lo señalado hasta aquí evidencia que no existe "salud organizacional" en las instituciones estatales dedicadas al tema de la ciberseguridad y ciberdefensa (llámese comandos, entes, organismos, consejos y comisiones) al no contarse con atributos claves como alineación estratégica, calidad en la ejecución y capacidad de renovación requeridos para minimizar situaciones organizacionales signadas por procesos burocráticos con señales de ineficiencia en el manejo de los talentos, infraestructuras y recursos disponibles, lo cual genera poca capacidad de adaptación ante las amenazas que provienen de un contexto interno y externo cada vez más politizado y radicalizado.

Formulación del problema

En el interés de que el problema de investigación quedase formulado del modo más explícito y comprensible posible, en las líneas que se presentan a continuación se delimita con precisión el objeto de estudio y los propósitos de la investigación; todo ello en la necesidad de que el problema y las preguntas asociadas a este tengan una respuesta adecuada al tipo de investigación que se realizó, y que las preguntas formuladas tengan valor o relevancia teórica, de ma-

nera que contribuyan al desarrollo y a la ampliación del conocimiento existente.

De esta forma, el problema de investigación quedó formulado de la siguiente manera:

¿Qué tipo de ciberamenazas se ciernen sobre la República Bolivariana de Venezuela y cuál es su procedencia?

¿Qué tan preparada está la República Bolivariana de Venezuela para enfrentar las ciberamenazas que sobre ella se ciernen?

¿Cuál ha de ser el modelo de creación de valor en materia de Ciberseguridad para enfrentar los desafíos que afronta a República Bolivariana de Venezuela?

¿Cuáles deberían ser las características de Modelo de Negocio del Comando Cibernético Nacional en la República Bolivariana de Venezuela?

¿Cuál ha de ser el modelo de organización del Comando Cibernético Nacional?

Las respuestas obtenidas a estas interrogantes orientaron de forma crítica una adecuada discusión que permitió identificar, comprender, describir y explicar un modelo teórico apropiado de organización del Comando Cibernético Nacional, en la búsqueda de la regulación y control de sus procesos y relaciones como organización eficiente, viable y sostenible en el contexto actual venezolano.

Objetivos de la investigación

Objetivo general

Proponer el Modelo de Organización Cibernética para el Comando Cibernético Nacional.

Objetivos específicos

Construir el Mapa de Ciberamenazas que se ciernen sobre la República Bolivariana de Venezuela.

Identificar los propósitos, capacidades y relaciones de la República Bolivariana de Venezuela para hacer frente a los desafíos relacionados con la Ciberseguridad.

Establecer elementos de creación de valor en materia de Ciberseguridad para enfrentar los nuevos desafíos que afronta a República Bolivariana de Venezuela.

Determinar el Modelo de Negocio del Comando Cibernético Nacional para la República Bolivariana de Venezuela.

Diseñar el Modelo de Organización Cibernética del Comando Cibernético Nacional para la República Bolivariana de Venezuela.

Justificación de la investigación

En general, los autores perciben el impacto de las amenazas a la ciberseguridad de la nación como un inexorable impulsor del cambio en la atomizada y fragmentada institucionalidad del Estado venezolano dedicada a esta materia; cambio que debe apuntar hacia un proceso de disrupción innovativo en lo institucional, basado en la combinación

del empleo de estructuras, gente y tecnologías de una forma más novedosa. Esto incentivó a reexaminar la manera como actualmente se organizan y relacionan las instituciones dedicadas a la ciberseguridad, no solo en el país, sino en naciones aliadas como China y Rusia, y también con el gran enemigo: los Estados Unidos, de forma tal de poder emular mejores prácticas en materia de organización de los servicios de ciberseguridad, con miras a garantizarle a la nación venezolana la necesaria adaptación, regulación y control ante eventuales amenazas a la ciberseguridad de la nación.

Esto tributó significativamente en la necesaria reflexión sobre nuevas fronteras para la creación de valor en materia de ciberseguridad, y con ello se pudo avanzar en la propuesta de organización cibernética del Comando Cibernético Nacional.

De allí que esta obra pretende ampliar el saber sobre un objeto de estudio que ha sido identificado como el Modelo de Organización Cibernética del Comando Cibernético Nacional para la República Bolivariana de Venezuela. En consecuencia, es un intento por aportar conocimiento nuevo u original al debate de la Seguridad y Defensa Integral de la Nación.

Para avanzar en este propósito, se explicitó un objetivo concreto que justificó la elección del objeto del estudio en referencia a la disciplina académica en que se inscribe, la cual no es otra que la Seguridad de la Nación.

Por otro lado, los autores buscaron y tomaron en cuenta toda la información accesible sobre el objeto de estudio, cuya selección respondió a criterios técnicos y políticos en razón del objetivo de la investigación.

De igual forma, a lo largo de esa obra se refleja de manera sistemática y consistente la fidelidad de las fuentes de las que se extrae la información, permitiendo así la posibilidad futura de contrastar estas últimas y validar los hallazgos a los que se arribó con la investigación.

Se recurrieron a referentes teóricos de alto nivel académico, mediante el empleo de índices bibliométricos que permitieron la ubicación de bibliografía académica para indagar y adquirir el conocimiento existente y hacer el esfuerzo académico de ampliarlo.

Por otro lado, se propone el desarrollo de argumentos lógicos y completos inspirados en el paradigma de la Cibernética Organizacional, que son expuestos ordenadamente de acuerdo con una estructura razonada e internamente consistente.

Finalmente, se logran conclusiones "robustas", pero susceptibles de evaluación crítica y revisión, en el entendido de que nunca serían indiscutibles o irrefutables.

Metódica que guió la investigación

Enfoque epistemológico

En virtud de la naturaleza de la realidad estudiada y en correspondencia con los objetivos antes indicados, la postura epistémica asumida por los autores para el abordaje de esta investigación fue la asociada con la escuela her-

menéutica, y en consecuencia, se tomó como referencia el enfoque cibernético para avanzar en la generación de la propuesta de creación del Modelo de Organización Cibernética para el Comando Cibernético Nacional de la República Bolivariana de Venezuela.

Con esta orientación epistémica, se plantea que el saber estratégico-gerencial en materia de ciberseguridad se adquiere por medio de la observancia de una serie de principios generales, a partir de los cuales se deducen sus instancias particulares. De este modo, el enfoque de sistemas hizo posible la validación de algunas reglas de inferencia que los estudiosos de la cibernética reconocen como principios generales, desde donde se deducen sus instancias particulares.

Una vez seleccionada la escuela de pensamiento y el enfoque para el abordaje de la investigación, se estableció la metodología a seguir, la cual estuvo en plena concordancia con los objetivos planteados; en este sentido, la investigación se realizó en base al método deductivo. Y esto fue así, pues el enfoque cibernético se ha asociado con el método deductivo de descubrimiento y comprobación, ya que se destaca el valor del conocimiento para llegar a la verdad, por lo cual se le confiere criterio de verdad a lo intelectual, a la razón y a los hechos (Camacho y Padrón, ob. cit.).

Tipo de investigación

Esta investigación buscó la descripción y explicaciones al fenómeno de cómo organizarnos de manera sistemática, coherente y lógica para ser eficaz y eficiente en la atenuación de las emergentes amenazas a la Ciberseguridad de la nación.

El tipo de investigación realizada determinó los niveles que fueron necesarios desarrollar, por lo que se alizó a nivel exploratorio, descriptivo y explicativo, ya que, descriptiva, explicativa, ya e "se centra en determinar los orígenes o las causas de un determinado conjunto de fenómenos complejos y delicados, en los que el riesgo de cometer errores es alto" (Palella y Martins, ob. cit.; p. 103).

Diseño de la investigación

En atención a los objetivos que guiaron la investigación, se justificó el diseño de esta como de campo (Tamayo y Tamayo, 2005; Hernández, Fernández y Baptista, 2006, Arias, 2006), en el hecho de que los datos e informaciones de interés se obtuvieron directamente de fuentes primarias involucradas con la realidad de los sujetos informantes, detallados más adelante, sin manipular variable alguna, mediante observación directa y aplicación de un instrumento diseñado para tal fin. En cuanto a la consideración que subyace a considerar que toda investigación de campo involucra un componente de tipo documental, se debe a que parte de la fuente de información fue secundaria, en tal sentido, fue obtenida de un arqueo teórico riguroso, focalizado en la aspiración de precisar aspectos, elementos y restricciones relacionadas con la temática investigada.

En consecuencia, no fue una investigación de carácter experimental, sino que se realizó en situaciones del contexto y dinámica de la vida organizacional, es decir, en los servicios de Ciberseguridad, el cual se circunscribe a la República Bolivariana de Venezuela.

Método de investigación

Dada la escuela de pensamiento y el enfoque adoptado para avanzar hacia el logro de los objetivos planteados, el método utilizado fue una combinación de los métodos cuantitativos con las metodologías cualitativas. En consecuencia, siguiendo a Hurtado (2000), estamos en presencia de una investigación multimétodos.

Población y muestra

En la tarea de diseñar una investigación en relación a un ámbito de la realidad, un fenómeno científico o un grupo en estudio, se hace necesario la definitoria de las tres coordenadas que lo especifican: el espacio en que se producen, el tiempo en que tienen lugar y el conjunto de unidades de observación o población que comprenden (Sierra Bravo, 2007). Por ello, fue una tarea del investigador fijar los límites espaciales o geográficos, la temporalidad y la población del fenómeno indagado.

En este sentido, para cumplir con dicho protocolo y darle forma al proceso de indagación, la población objeto de estudio quedó determinada por los siguientes grupos:

Población 1: Representantes de organismos e instituciones del Estado venezolano que tienen incidencia en el tema de la Ciberseguridad.

Población 2: Investigadores, académicos y expertos comprometidos institucionalmente y vinculados al debate de la Organización Cibernética.

No obstante, dado que es imposible estudiar todas las realidades poblacionales, se hizo necesario abarcar solo una parte de estas, de manera que se estimó conveniente seleccionar una cuidadosa y controlada colección de sujetos, tomando en consideración los criterios anteriormente mencionados. Por ejemplo, en cuanto a accesibilidad, para la población 1 se trabajó solo con un conjunto de doce (12) organizaciones, que a efectos de esta publicación, los autores han decidido mantener en la confidencialidad.

Para la población 2, dadas sus características de intelectualidad, conocimiento de la temática y disposición de acceso a recursos tecnológicos como la internet, los cuales permitieron una fluida y asincrónica comunicación con el investigador, se trabajó con una población que fue susceptible de ser ubicada en el Ciberespacio, por tener allí posibilidad de interacción síncrona y asíncrona con los miembros de esta población.

Es importante destacar que inicialmente algunas de las muestras poblacionales no estaban pre-especificadas, y en consecuencia, fue posible que evolucionaran una vez se inició el trabajo de campo. Algunas de las causas que se suscitaron en el transcurso de la investigación fueron: cambios ministeriales, hermetismo en torno a la temática de la Ciberseguridad, e importancia teórica de las producciones intelectuales de los actores, de las fuentes documentales e institucionales y de las observaciones realizadas en escenarios dinámicos propios del contexto organizacional que signa hoy la realidad venezolana, entre otras.

De esta forma, a medida que el estudio progresó se descartaron o seleccionaron casos adicionales a estudiar,

de acuerdo con el potencial para el desarrollo de nuevas intelecciones o para el refinamiento y la expansión de las ya adquiridas, lo cual implicó que algunas muestras se fueron ajustando con el avance de la investigación.

Para la selección de la muestra se utilizó la modalidad de *muestreo intencional no probabilístico* aleatorio estratificado, en tanto que permitió la posibilidad para la ubicación de sujetos de manera circunstancial, y es estratificado debido a la clasificación con la que se presentaron en la población, dividida en subpoblaciones a los fines de garantizar la representatividad de los sujetos seleccionados por cada estrato (Hernández, Fernández y Baptista, 2003), a partir de allí, los sujetos muestrales se consideraron en igualdad de condiciones para dar respuestas al instrumento de recolección de datos diseñado para tal fin.

La muestra determinada se constituyó, por lo tanto, en el referente a través del cual solicitar la opinión a dichos estratos mediante el instrumento que se diseñó para tal fin.

Protocolos técnicos

Fueron aquellos utilizados por los autores para recolectar u obtener la información necesaria en función de estudiar la problemática planteada. Sabino (2002) los define como "… cualquier recurso del que se vale el investigador para acercarse a los fenómenos y extraer de estos la información" (p. 143).

En consecuencia, debido a la forma en que se obtuvieron los datos y a la concepción del diseño de la investigación de campo, la recolección de datos e informaciones se realizó a través de varias modalidades:

Recolección documental y bibliográfica: Permitió obtener todos aquellos datos secundarios que se necesitaron para realizar un trabajo sistemático.

Observación directa no participante: Permitió a los autores visualizar, sin intervenir, instalaciones de ciberseguridad en el ejercicio de sus prácticas administrativas en la procura del cumplimiento de sus funciones, sus interacciones y procesos. De igual forma, implicó la visita a entes e instituciones gubernamentales involucradas en el tema de la ciberseguridad.

Este contacto hizo posible analizar y comprender la realidad de las organizaciones seleccionadas, en la búsqueda de una práctica, estructura y procesos que las conviertan en organizaciones adaptativas y viables en el complejo entorno donde operan y se desarrollan.

Cuestionario estructurado: Esta modalidad de encuesta se utilizó de forma escrita y a través de medios electrónicos mediante un instrumento o formato en contentivo de una serie de preguntas. Se le denominó cuestionario auto-administrado porque este fue llenado por el encuestado, sin intervención del encuestador (Arias, ob. cit.).

La información obtenida por las modalidades anteriormente citadas se organizó en forma sistemática y pertinente, y posteriormente fue analizada de manera profunda y reflexiva, en función de lograr la contrastación de las teorías con la realidad concreta expresada por los informantes a través del

instrumento de captura de información, en la búsqueda intelectual basada en la sistema-cibernética organizacional, a fin de formular un Modelo de Organización Cibernética del Comando Cibernético Nacional como organización compleja a partir de los principios de la Cibernética Organizacional.

Una vez obtenida la información y terminada la recolección de datos, se abordaron una serie de etapas que conducen a tratar, interpretar, relacionar y analizar los datos e informaciones recabados para gestar el Modelo de Organización Cibernética que aquí se propone.

El tratamiento y las técnicas de análisis de los datos e información que fueron recabadas guardaron estrecha relación y coherencia con el abordaje epistemológico y metodológico de la investigación. Por lo tanto, se estableció y cumplió un plan para el logro de los objetivos específicos planteados, de manera que todo ello tributó, finalmente, al objetivo principal.

Momento II

SABERES PARA CONSTRUIR EL MODELO

Presentado el planteamiento del problema dentro del contexto en el que se desarrollan los hechos, establecidos los objetivos de la investigación, así como la justificación de cómo ir al encuentro con la realidad, fue necesario un acercamiento a referentes teóricos y el posterior análisis de discurso, que permitieron establecer las consideraciones teóricas-conceptuales de mayor proximidad al contexto de estudio en relación a la Ciberseguridad, el Modelo de Organización Cibernética y la Seguridad de la Nación. Para ello, se estableció el entramado de saberes propios de la investigación, que sirvió como andamiaje para soportar teóricamente el desarrollo de la misma.

En este orden de ideas y a los fines de esta publicación, se presentan los referentes teóricos inherentes al estudio, los cuales emergen como saberes requeridos para la construcción del Modelo de Organización Cibernética del Comando Cibernético Nacional.

Una mirada al Ciberespacio y a la Ciberseguridad

En primer lugar, habría que destacar que el Diccionario de la Real Academia Española (DRAE) en su 22ª edición define Ciberespacio, en su única acepción, como el "ámbito artificial creado por medios informáticos". En realidad, entendemos que la RAE se está refiriendo a un entorno no físico creado por un equipo informático con el objetivo de interoperar en una Red. En consecuencia, el mayor ámbito del ciberespacio es Internet.

Existen numerosas definiciones de ciberespacio. Desde la más simple y ya vieja e histórica como «aquel espacio donde sucede una conversación telefónica», hasta una más práctica y actual: "El espacio o realidad virtual donde se agrupan usuarios, páginas web, chat, redes sociales, blogs y demás servicios de la web y de internet". En todo caso, y en virtud del tema central de este Trabajo de Grado, el ciberespacio es el nuevo campo donde pasamos gran parte de nuestras vidas los más de 1.000 millones de habitantes que hoy día tenemos acceso a internet; este es un gran campo social donde disfrutar, trabajar, pensar, vivir, pero también es un nuevo campo de batalla, debido a los riesgos y amenazas que su uso masivo plantea. En definitiva, es un nuevo campo de batalla en el siglo XXI, sin fronteras y asimétrico.

En relación al vocablo ciberseguridad, cabe destacar que el autor hizo una revisión documental exhaustiva de esta temática, concluyendo que el trabajo de Maurer y Morgus (2014) intitulado 'Cybersecurity' and Why Definitions Are Risky', recoge el estado actual de debate que sobre la materia dan organizaciones internacionales, organismos internacionales de normalización y comandos nacionales de ciberseguridad.

De allí que para un acercamiento al debate teórico requerido en esta investigación, los autores han elaborado la siguiente definición de ciberseguridad:

> "Conjunto de actuaciones orientadas a asegurar, en la medida de lo posible,

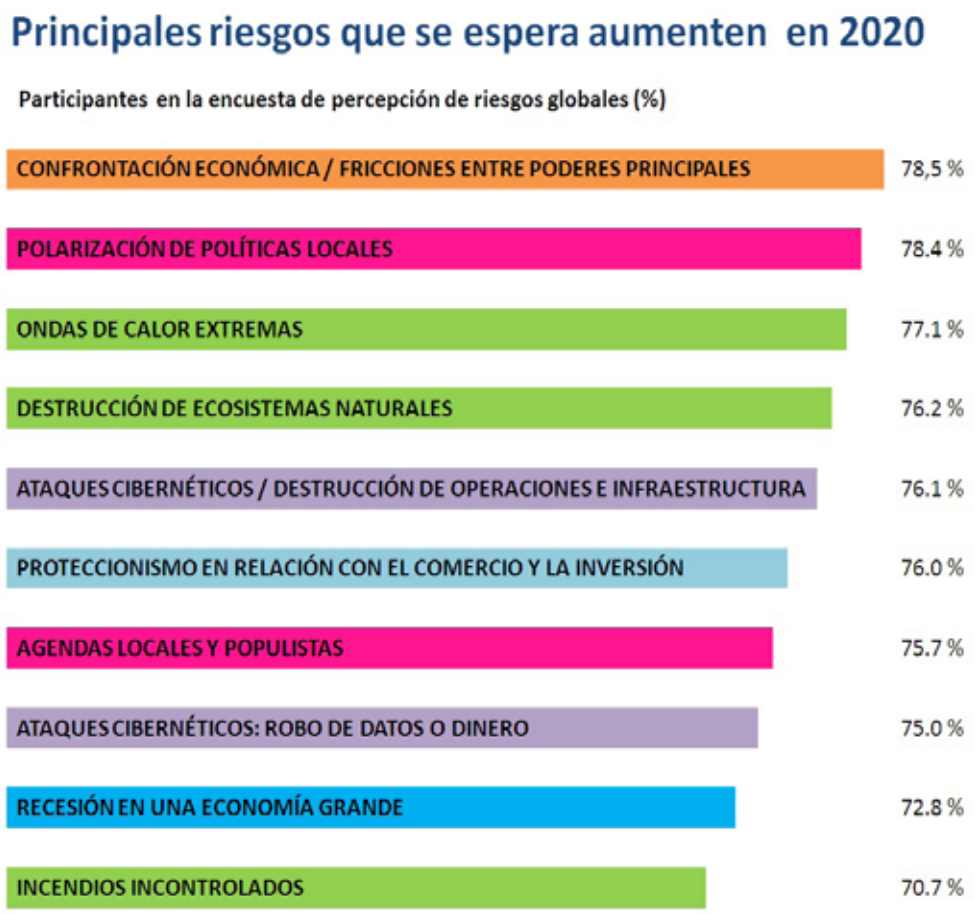
las redes y sistemas que constituyen el ciberespacio:

•Detectando y enfrentándose a intrusiones,
•Detectando, reaccionando y recuperándose de incidentes, y
•Preservando la confidencialidad, disponibilidad e integridad de la información".

La Ciberseguridad en el contexto de los riesgos globales

En primer lugar, se van a situar los ciberataques en perspectiva con otros riesgos globales. El Foro Económico Mundial ha publicado el estudio "Riesgos Globales 2019" en el que se ofrece un gráfico sobre la percepción del impacto y de la probabilidad de los riesgos globales, que denominado "el paisaje de riesgos globales en 2019". En dicho Foro de debatió que asistimos a un momento en que las oportunidades de las tecnologías emergentes exigen audacia y agilidad, un aumento en los ataques cibernéticos afiliados al Estado está agravando los puntos de falla en las operaciones de las empresas, la infraestructura, las cadenas de suministro y las interacciones con los clientes.

Gráfico Nro.1 Top Risks Expected to Increase 2020.

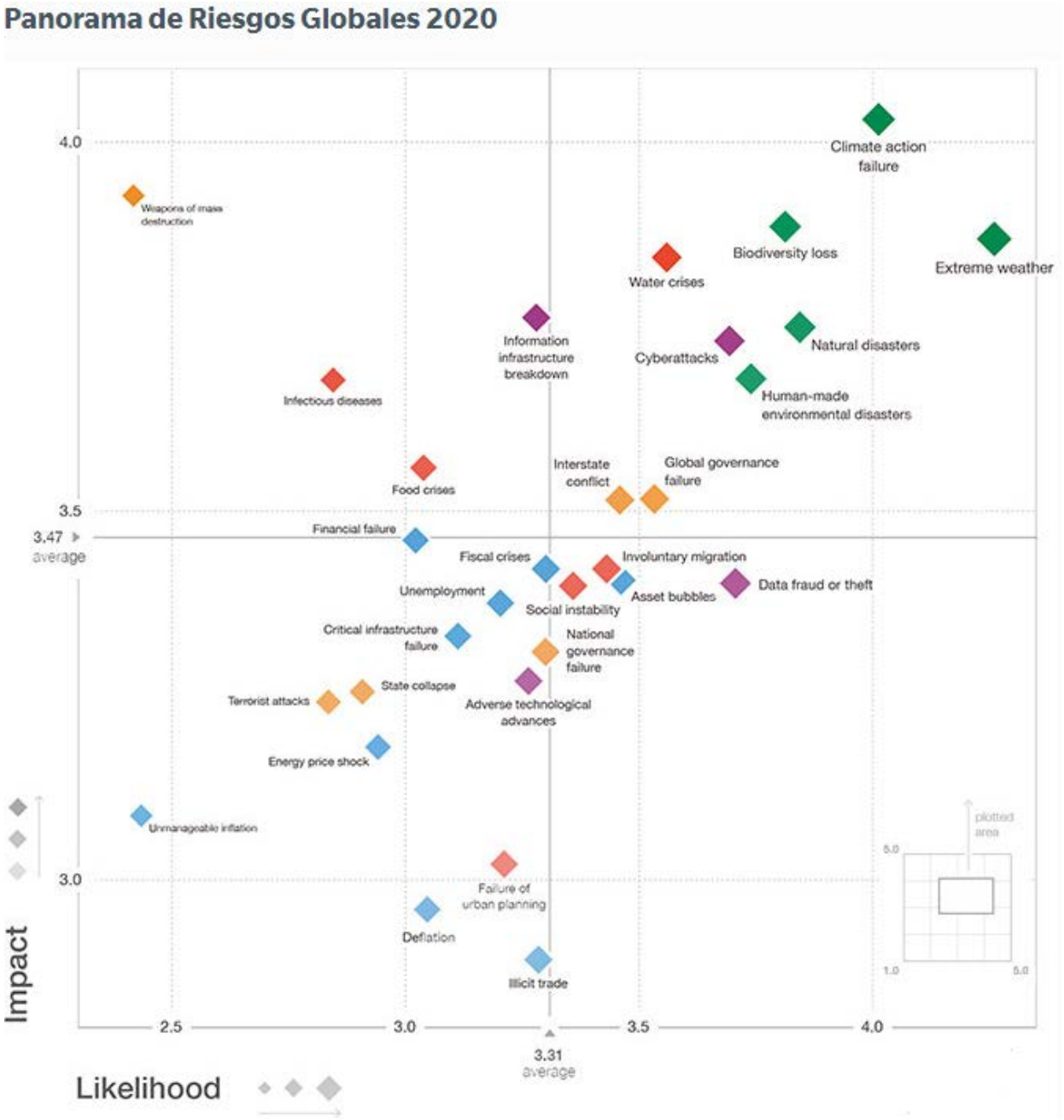


Fuente: Foro Económico Mundial.

El Gráfico anterior permite apreciar que la tecnología sigue desempeñando una función fundamental en la configuración del panorama global de riesgos. Las preocupaciones sobre los ataques cibernéticos y el robo de datos o dinero volvieron a ser prominentes, y también pone de relieve otras vulnerabilidades tecnológicas: alrededor de dos tercios de los encuestados esperan que los riesgos asociados con disrupción de operaciones e infraestructuras, mientras que tres quintas partes dijeron lo mismo sobre la pérdida de datos robo de dinero. En 2019 se produjeron nuevas filtraciones masivas de datos, se revelaron nuevas debilidades de hardware y la investigación señaló los usos potenciales de la inteligencia artificial para diseñar ciberataques más potentes. Durante el año 2018 también se demostró que los ciberataques plantean riesgos para las infraestructuras críticas, lo que llevó a los países a reforzar el control de las asociaciones transfronterizas por motivos de seguridad nacional.

Para el inicio del año 2020, los ciberataques tienen asignada una probabilidad de 3,6 y un impacto de 3,6 en base a 4,0. Los riesgos asociados a los ciberataques son superados solamente en relación a la combinación de ambos parámetros, por desastres ambientales generados por el hombre, desastres naturales, pérdida de biodiversidad, clima extremo y fracaso en la acción climática. De este paisaje de riesgos globales se desprende la percepción de la alta probabilidad y el elevado impacto de los ciberataques en comparación con el resto de riesgos globales.

Gráfico Nro. 2: El Paisaje de Riesgos Globales en 2020.



Fuente: World Economic Forum, 2020.

De igual forma, el informe "Riesgos Globales 2020" de igual forma analiza estos datos en un apartado específico dedicado a los riesgos tecnológicos, en un anexo titulado: "Riesgos Tecnológicos: Regreso al Futuro". En el análisis se recoge que el riesgo de ataques cibernéticos a gran escala se sigue considerando por encima del promedio en las dos dimensiones del impacto y la probabilidad, lo que refleja la creciente sofisticación de los ataques cibernéticos y el surgimiento de la hiperconectividad, con un número cada vez mayor de objetos físicos conectados a Internet, además de la vulnerabilidad que supone el almacenamiento de los datos personales en la nube. Aunado a esto, el "Internet de las cosas" (IoT en sus siglas en inglés) incrementará esta tendencia.

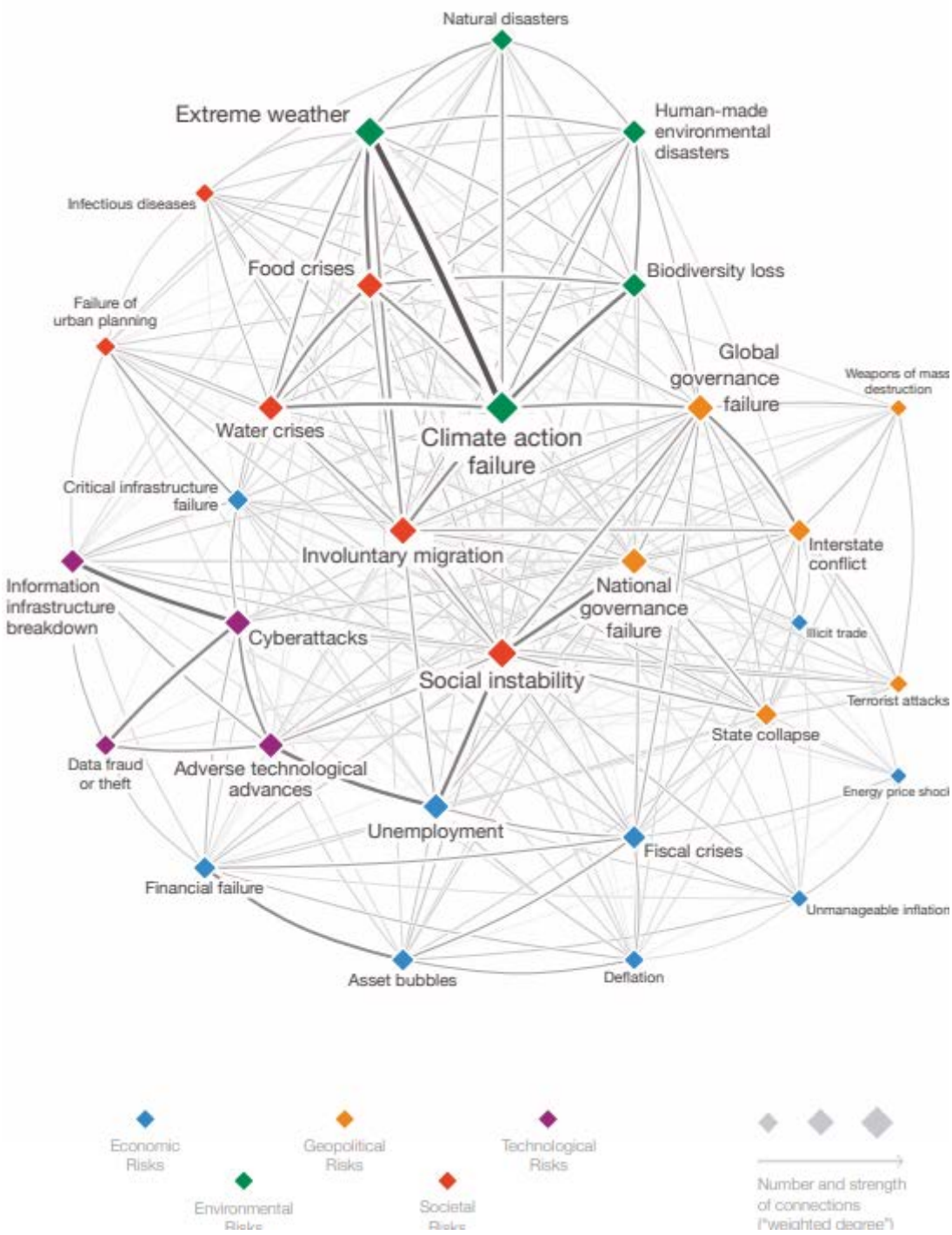
El mencionado informe, "Riesgos Globales 2020", ofrece también un mapa de interconexión de los riesgos, donde se puede observar la conexión directa de los ciberataques con otros riesgos tecnológicos como la ruptura de la infraestructura de información crítica, el mal uso de las tecnologías, el fraude y robo de datos. También existe un enlace directo con un riesgo que en el informe se asocia a la economía, el fallo de infraestructuras críticas. El resto de conexiones directas con otros riesgos caen en el ámbito de los riesgos denominados geopolíticos, ataques terroristas, fallo de la gobernanza nacional y conflictos entre Estados.

En el caso de los riesgos asociados al uso del ciberespacio, podemos observar al analizar el gráfico que las conexiones de segundo nivel alcanzan a otros riesgos que tienen unos niveles elevados tanto de probabilidad como de peligrosidad y que se incorporan a áreas económicas, sociales, ambientales y de riesgos geopolíticos.

Con esto nos enfrentamos a un nuevo campo de batalla dentro de la seguridad que es el ciberespacio, donde se producen comportamientos o fenómenos ya conocidos, pero empleando técnicas nuevas; y también fenómenos nuevos que surgen de la propia idiosincrasia del ciberespacio y en donde, en ocasiones, no están claras las fronteras entre activismo y delincuencia.

Mapa de interconexión de los riesgos 2020

Gráfico Nro. 3. Mapa de interconexiones de riesgos globales 2019.



Fuente: World Economic Forum 2020.

La vulnerabilidad estratégica que supone este tipo de amenazas comprende especialmente dos campos. Por un lado, los ataques contra los sistemas que regulan infraestructuras básicas para el funcionamiento de un país –como el sabotaje de los servicios públicos, la paralización de la red de telecomunicaciones, transporte aéreo o ferroviario, así como la interrupción de los sistemas de energía eléctrica– suponen un serio quebranto para la normalidad y la seguridad de una nación. En consecuencia, todas las infraestructuras básicas deben dotarse de elementos de protección suficientes para poder neutralizar este tipo de agresiones cuando su funcionamiento depende de complejos sistemas y plataformas informáticas y de telecomunicaciones.

Por otro lado, la eventual penetración a los sistemas de comando y control de las Fuerzas Armadas Nacionales, así como a las bases de datos de los servicios de inteligencia, permiten suponer una amenaza directa a la seguridad de la nación. Razón por la cual existen fundadas preocupaciones sobre las capacidades necesarias para impedir cualquier tipo de agresión cibernética que pueda amenazar la seguridad de la nación; con lo cual se evidencia que uno de los nuevos retos mundiales y principales amenazas a la seguridad de una nación, lo constituye el tema de la Ciberseguridad.

Pertinencia de Organizaciones Nacionales dedicadas a la Ciberseguridad

La tendencia dominante en el actual contexto de las organizaciones tanto públicas como privadas dedicadas a la Ciberseguridad, dan cuenta del acelerado crecimiento de sus umbrales de complejidad, producto del incremento acelerado de la rata de incidentes telemáticos que generan múltiples interacciones entre actores que no es fácil determinar su procedencia, en ocasiones ubicuos, altamente tecnificados y conocedores de los entornos con los cuales están inexorablemente vinculados.

Las prognosis más fundamentadas en este particular campo del saber, apuntan a que, en los próximos años, conducir una organización de ciberseguridad no importando su tamaño y naturaleza (pública o privada) implicará manejarse en un contexto cada vez más incierto y de complejidad en ascenso. Por ello sería ingenuo no prever un aumento exponencial de complejidad de sus actividades y una dinámica cada vez más acelerada de interrelaciones con los diferentes actores con los que, en ocasiones, interactúa a ciegas, para poder obtener y gestionar con eficacia, eficiencia y transparencia los recursos y talentos necesarios que le permiten dar respuestas acertadas y con la velocidad requerida, a las soluciones que demandan los múltiples problemas que en lo interno y externo le posibiliten garantizar la continua adaptación y supervivencia de las infraestructuras críticas que resguardan en el entorno donde estas materializan sus operaciones; a la vez que serán permeadas por los avances tecnológicos que modificarán, sin duda, aspectos básicos de los procesos asociados a la materialización de su misión.

En un contexto como el antes descrito, habría que añadir altos niveles de conflictividad ocasionado por variables asociadas a lo económico, político y social, que permiten imaginar la configu-

ración de un entramado caracterizado por alta incertidumbre. De esta forma, estaríamos en presencia de un relacionamiento con estructuras sociales y organizacionales dedicadas a la ciberdelincuencia y el ciberterrorismo no predecibles, tal como las imaginara en la década de los noventa Ilya Prigogine, premio Nobel de Química y fundador de la ciencia de la Inestabilidad.

En consecuencia, asistimos a un momento histórico de cambios que demanda de las organizaciones nacionales de ciberseguridad acuciosidad para reflexionar y repensar con seriedad no solo los problemas actuales que la pandemia del covid-19 ha ventilado en la materia, si no también avizorar los retos y desafíos que delinea la praxis en este campo del saber, ante las profundas mutaciones que enfrentarán las organizaciones para hacer frente a la explosión de complejidad que emerge de entornos cada vez más cambiantes.

En este contexto, los profesionales del campo de la ciberseguridad deberán dejar los métodos, metodologías y protocolos técnicos en la materia, signados por la más alta racionalidad y elusión de riesgos, para proceder a la indagación sobre nuevos mapas cada vez más difusos de ciberamenazas, de manera responsable, con enfoques holísticos que permitan cartografiar con mayor amplitud los actores, las armas y las infraestructuras críticas susceptibles de ser impactadas ante procesos de cambios que atraviesa la realidad con la cual interactúa.

De esta manera, los profesionales del campo de la ciberseguridad deberán asumir el trabajo incesante de bajar al campo y tener contacto directo con el contexto para captar las claves de la realidad, probablemente en muchos casos ignoradas por las metodologías de inteligencia en materia de seguridad tradicional.

Todas las cuestiones anteriores son especialmente críticas en la formulación de un Comando Cibernético Nacional para la República Bolivariana de Venezuela. De allí que esta obra viene a llenar un vacío existente en relación al cómo investigar en este campo del saber, desde donde surge la aspiración de que al concluir esta obra se podrá apreciar la emergencia de un modelo de Organización Cibernético del Comando Cibernético Nacional orientado a los reales problemas de Ciberseguridad que enfrenta el país, marcadamente disímil con respecto a los tradicionales enfoques, para afrontar el desafío que supone lograr las necesarias sinergias de las organizaciones existentes en este campo del saber, con el fin de garantizar la toma de decisiones, la gobernabilidad, la adaptación, regulación y control antes, durante y después de incidentes telemáticos.

En este contexto, la creación de un Comando Cibernético Nacional es el escenario de profundos cambios que actúan como referente de la transformación de las instituciones, procesos y métodos para hacerle frente a las ciberamenazas que se ciernen contra la República Bolivariana de Venezuela. Toda vez que la institucionalidad existente en materia de ciberseguridad, si bien han tenido una extendida aceptación debido a la necesidad cada vez más imperiosa de contar con métodos y protocolos técnicos para el abordaje de situaciones

derivadas de incidentes telemáticos, en los actuales momentos, a pesar de sus aportaciones, aparecen desligados de la problemática real hasta aquí expuesta. En muchas ocasiones dichas instituciones apuntan hacia un esquema de trabajo genérico o prefigurado por una orientación puramente cientificista y metodologicista.

Finalmente, lo que se desea resaltar es la fuerte relación que debe existir entre los problemas reales en materia de ciberseguridad, las formas de concebir y problematizar situaciones susceptibles de convertirse en amenazas, y la pluralidad y riqueza de métodos, metodologías y protocolos técnicos existentes en el campo de la ciberseguridad para ir al encuentro con dichas realidades, de forma tal de poder apuntar a la necesaria producción de soluciones, innovaciones o aportaciones teóricas que den cuenta de las demandas-exigencias de la sociedad en tiempo real.

Es así como desde esta obra los autores asumimos el reto de repensar las orientaciones prevalecientes en lo que respecta a la conformación de un Comando Nacional de Ciberdefensa, dirigiendo este esfuerzo intelectual a satisfacer las necesidades de fortalecimiento de la institucionalidad para que asuma el rol de rectorar las actividades relacionadas con la garantía del ciberespacio de la República Bolivariana de Venezuela.

A tono con lo que se afirma en las líneas anteriores, la pandemia de la covid-19 ha puesto de relieve la vida cotidiana del venezolano que, quiérase o no, gira alrededor de actividades cada vez más digitalizadas y, por consiguiente, más sensibles a amenazas cibernéticas. Actividades educativas, trabajo, pagos y transacciones financieras, trámites gubernamentales, servicios, telecomunicaciones, electricidad y así, un sinfín de actividades, operan en la actualidad a través de tecnologías digitales, pero, para la gran mayoría de los ciudadanos, las amenazas cibernéticas son desconocidas y sus efectos pasan prácticamente desapercibidos.

Por esto, la necesidad de garantizar el ciberespacio de la República Bolivariana de Venezuela y con ello, allanar este vacío institucional, es una tarea urgente. De allí que como una orientación estratégica básica en el proceso de cambios que vive hoy la sociedad venezolana, la creación de un Comando Cibernético Nacional se convierte en un verdadero motor de la reflexión intelectual, de la formación de especialistas en ciberseguridad, y de la calificación de investigadores en esta materia.

En esta dirección, la presente obra se convierte en una propuesta de acción académica que relaciona ámbitos complementarios: la Seguridad de la Nación, la Ciberseguridad y la Gerencia, en las cuales se realiza el inmenso esfuerzo transformador que orienta el modelo de desarrollo que organiza, moviliza y alinea la participación de actores en el proceso de cambio que hoy experimenta la sociedad.

La Cibernética Organizacional propuesta por Stafford Beer

Esta parte del trabajo contiene una breve introducción a las ideas fundamentales sobre La Cibernética Organizacional, y en especial sobre el que el Modelo de Sistemas Viables (VSM), con

el propósito de llamar la atención sobre una nueva forma de pensar acerca de las organizaciones, la cual es radicalmente diferente de los modelos tradicionales, a menudo jerárquicos. Todo ello en la dirección de dar el salto a nuevas formas de pensar las organizaciones utilizando un lenguaje nuevo y rico en metáforas, que convocan a reflexiona la forma en que el cerebro humano organiza el funcionamiento de los músculos y órganos. Esta estructura garante de la adaptación, regulación y control en los seres humanos, se corresponde con la que soporta el sistema nervioso central y autónomo para manejar el funcionamiento del sistema nervioso central de las personas, que ha demostrado ser exitoso al garantizar su capacidad de supervivencia, lo cual es posible emular en organizaciones creadas por el hombre.

No obstante, y parafraseando a Jhon Wlater: " …para que esto suceda, tienes que aprender a ver el mundo a través de ojos cibernéticos". (Opc, Pag 7)

De esta forma, la Cibernética es hoy entendida como ciencia que se encarga de las totalidades, y que estudia y explica la realidad organizacional a partir de las leyes que regulan el comportamiento universal de los sistemas naturales.

De allí que, la Cibernética Organizacional, y en particular el Modelo de Sistemas Viables (MSV) propuesto por Stafford Beer, constituye un modelo que apunta a obtener una mejor comprensión de la complejidad organizacional, aumentando la capacidad gerencial para interpretar y analizar situaciones muy complicadas, y así descubrir respuestas imaginativas en las organizaciones sociales para hacerles frente a los desafíos y a las oportunidades del medio ambiente.

En este orden, el Modelo de Sistemas Viables permite una recrear "estructuras organizacionales que se adaptan continuamente, teniendo la flexibilidad suficiente para involucrar a todas las áreas de complejidad relevantes para su desarrollo, de forma que pueda garantizarse la coordinación, la planeación y el control" (Pérez, ob. cit.; p.145).

De este modo, el Modelo de Sistemas Viables (MSV) intenta describir y explicar el funcionamiento del Sistema Nervioso Central, con base en los cinco sistemas que en el interactúan.

SISTEMA 1: Todos los músculos y órganos. Constituyen las actividades básicas encargadas de la garantía de la misión de la organización.

SISTEMA 2: El sistema nervioso simpático, que monitorea la músculos y órganos y asegura que su interacción se mantenga estable.

SISTEMA 3: El cerebro base, puente y médula que supervisa todo el complejo de músculos y órganos y optimiza el ambiente interior. Relacionado con la gerencia, la regulación interna y mejoramiento continuo. Tiene su parangón en las actividades de apoyo.

SISTEMA 4: El cerebro medio o diencéfalo, permite la conexión con el mundo exterior a través de los sentidos. Se asocia con el responsable de la planificación futura, proyecciones, y pronóstico.

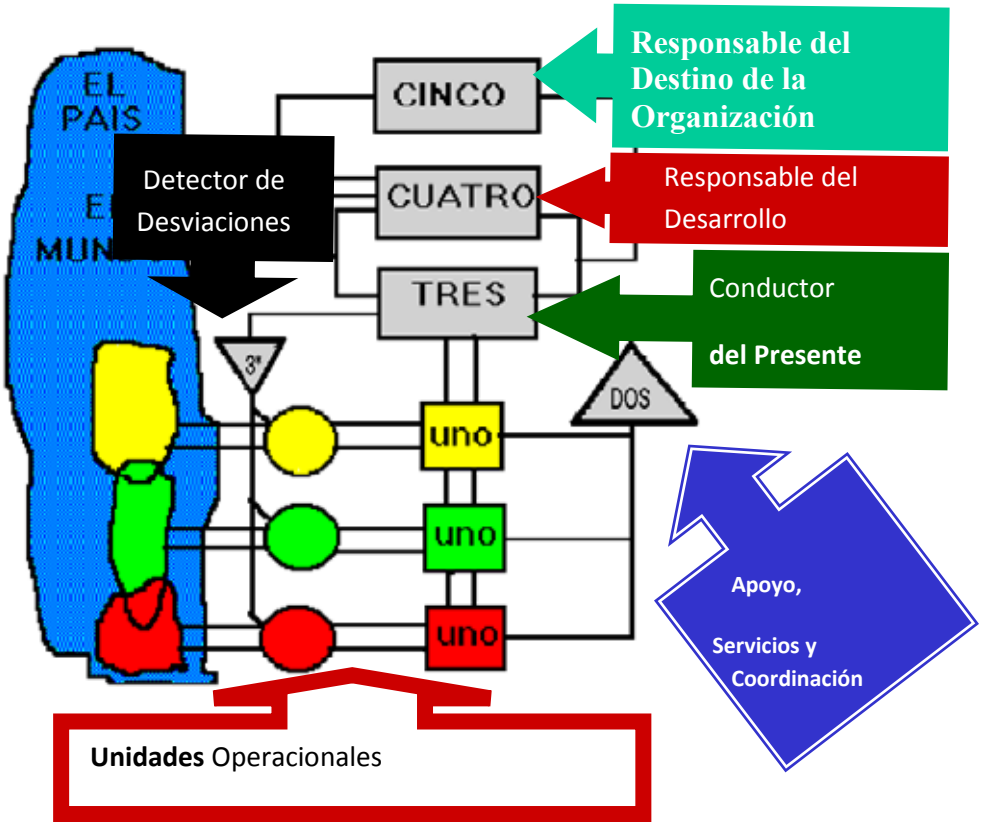
SISTEMA 5: La corteza cerebral, garante de las funciones cerebrales superiores. Se corresponde con la formulación de decisiones de política e Identidad.

Con esto se propicia la representación de la complejidad organizacional sobre la base de la imbricada coexistencia de cinco grandes funciones que se materializan en toda organización: Operativa, Coordinación, Gerencia, Inteligencia y Política; además de ser una poderosa herramienta para el diagnóstico, análisis y diseño organizacional a través de la cual es posible validar elementos conceptuales que apuntan a garantizar la eficacia y eficiencia necesarias para el fortalecimiento de la capacidad de adaptación, regulación y control organizacional.

La ilustración gráfica del Modelo de Sistemas Viables se muestra en la Figura 1 y en ella puede visualizarse que consta de 5 funciones o subsistemas:

1. Subsistema 1: Actividad Operativa.
2. Subsistema 2: Función de Coordinación.
3. Subsistema 3: Función de Gerencia, que incluye dentro de sí al Sistema de Monitoreo.
4. Subsistema 4: Función Inteligencia.
5. Subsistema 5: Función Política.

Figura 1. Modelo de Sistemas de Viables



Fuente: Adaptación propia de los autores, (2020).

Estos subsistemas o funciones representan los cinco criterios esenciales planteados por Beer, que agregados a los mecanismos que permiten la regulación, se deben tener en cuenta frente a cualquier conversación por el diseño del sistema autónomo que se quiera hacer viable (Narvarte, 2002), a saber:

Sistema Uno: Las Unidades Operacionales. Las actividades operacionales constituyen la razón de ser del sistema o institución, y es, precisamente por esta circunstancia, que el criterio de libertad y autonomía debe ser especialmente observado a este nivel. Esta autonomía solo debe estar restringida por las limitaciones propuestas por las funciones de coordinación y cohesión del Metasistema. Cada sistema uno debe ser capaz de operar, hasta donde le sea posible, con recursos propios, sin más limitaciones que los lineamientos y políticas establecidas por el Metasistema, los cuales deberán ser los mínimos necesarias para mantener la cohesión y estabilidad de la organización como un todo. Esta concepción hace que el sistema uno sea considerado por su Metasistema (dos, tres, cuatro y cinco) como un sistema viable. Los sistemas uno de una organización social, como los Servicios de Salud, son típicamente las áreas de atención primaria de generación de acciones tempranas para el logro de la garantía de la salud de los ciudadanos.

Sistema Dos: Coordinación. Es el dispositivo de regulación de la organización con respecto a las interacciones que ocurren entre los diferentes sistemas uno. No posee autoridad ni jerarquía sobre estos. Entre sus funciones típicas asociadas al manejo del talento humano, se encuentra asesoría legal, informática; relaciones industriales, las rutinas de presupuesto, los procesos administrativos en general y resolver conflictos de regulación mediante el ejercicio participativo de contraloría social, que incluye a la ciudadanía a través de Asociaciones de Vecinos y Consejos Comunales, quienes tienen la responsabilidad legal de realizar adecuadamente las funciones del sistema dos.

Sistema Tres: Conductor del Presente. Este sistema es el responsable del presente de la organización y, por ende, de la sinergia operativa de los sistemas uno. Da autonomía a sus unidades operativas, pero mantiene, al mismo tiempo, la cohesión del todo. Es, de este modo, el integrador de los sistemas uno. Las funciones del sistema tres de una organización de salud recaen usualmente en un director ejecutivo, o en un comité ejecutivo conformado por los directores funcionales tales como Director Médico, Administrador, etc.

El Sistema Tres Asterisco (3): Detector de las Desviaciones Operacionales (Calidad de Gestión)*. Es una función especializada del **Sistema Tres** que provee un canal complementario de comunicación entre el **Sistema Tres** y el **Sistema Uno**. El Sistema Tres permite detectar desviaciones operacionales del **Sistema Uno**, no identificadas por el **Sistema Dos**. El resultado de esta comunicación puede conducir a modificaciones procedimentales en el **Sistema Uno**. Usualmente conforman el **Sistema Tres*** las funciones realizadas por los departamentos de auditoría interna.

Sistema Cuatro: *El Responsable del Desarrollo*. Tiene como actividad básica promover la invención del futuro de la

organización. Para ello realiza estudios y evaluaciones del contexto global detectando oportunidades o perturbaciones del medio ambiente. Su principal rol está en el proceso de planificación estratégica a mediano y largo plazo, y entre sus funciones se pueden mencionar las siguientes: exploración de tendencias de nuevas demandas provenientes del entorno, investigación y desarrollo institucional, investigación de nuevos productos y tecnologías, planificación estratégica, pronósticos y desarrollo gerencial.

Los departamentos típicos que conforman este sistema son los de planificación estratégica y los relacionados con la inteligencia de negocios: investigación de mercados, productos y tecnología.

Sistema Cinco: *El Responsable del Destino de la Organización*, constituye el último sistema del modelo y su objetivo se materializa al lograr el cierre del sistema como un todo. Esto se alcanza estableciendo el equilibrio entre las necesidades del presente (Sistema Tres) y del futuro (Sistema Cuatro). Su plataforma decisional deberá provenir de sus Sistemas Tres y Cuatro. Este sistema lo conforma una organización típica: el presidente de la empresa y una junta directiva.

Esta elaboración permite entender que el desarrollo del Modelo de Sistemas Viables (MSV) propuesto por Stafford Beer, es una de las más relevantes aportaciones de la cibernética en el marco de la gerencia de las organizaciones, ya que son el producto del necesario equilibrio de sus procesos interactivos los cuales deben guardar, a su vez, un completo equilibrio interno y con el contexto. De allí que en esta investigación se considera el planteamiento conceptual planteado por Beer como parte fundamental de la plataforma teórica para asumir el reto investigativo de imaginar la concepción de la Organización del Comando Cibernético Nacional.

De esta manera, y para garantizar que las partes se interconecten para formar un sistema completo integrado, hay que concebir el Comando Cibernético Nacional bajo los siguientes términos:

1. En primer lugar, necesita unidades operacionales que garanticen su misión. Estas constituirían los Sistemas 1 (S1), que en las estructuras organizativas tradicionales se corresponden con las unidades que garantizan la operación. De esta manera los S1 constituyen los procesos que realmente transforman insumos en bienes y servicios. Son, en el caso del cuerpo humano, los músculos; en un buque, la sala de máquinas; en una fábrica, las máquinas; en una comunidad agraria, los productores del campo.

2. En segundo lugar, hay que asegurarse de que haya formas de abordar los intereses en conflicto que inevitable en las interacciones que ocurren cuando las partes de S1 interactúan y compiten por el otorgamiento de recursos que son finitos. La resolución de conflictos es el trabajo del Sistema 2 que también se encarga de garantizar la estabilidad.

3. Una vez que las interacciones de las unidades del Sistema 1 se vuelven estables, es esencial observar formas de optimizar estas interacciones. Este es el trabajo del Sistema 3. El Sistema

3 funciona con una descripción general de todo el complejo de unidades interactivas del Sistema 1, en la búsqueda de la eficiencia global, la cual en el modelo se llama sinergia. De esta forma el sistema 3 está ahí para regular el Sistema 1, su función es la optimización.

4. Una vez que existe un conjunto estable y optimizado de unidades operativas, hay que asegurarse de que se pueda sobrevivir en un entorno cambiante. Este es el trabajo del Sistema 4. El Sistema 4 mira hacia el mundo exterior, considera lo que ve, busca amenazas y oportunidades. De esta forma, está ahí para elaborar planes para asegurar la viabilidad a largo plazo.

5. Y finalmente, todo debe funcionar dentro de algún tipo de contexto general. Todos deben estar alineados en la misma dirección. Este es el trabajo del Sistema 5. Proporciona las reglas básicas y los medios de hacerlos cumplir para garantizar que el sistema esté completo. El Sistema 5 proporciona, por último, decisiones y autoridad.

Con la finalidad de profundizar el debate de la cibernética organizacional, a continuación, se encontrará una síntesis de autores cuya producción intelectual da cuenta del estado del arte en la materia, destacándose conceptualizaciones, características, ventajas y desventajas de la Organización Cibernética:

Otras voces relacionadas con la Cibernética Organizacional

Hoy en día, con la emergencia del ciberespacio como un nuevo campo de actuación, un movimiento general de virtualización, afecta no solo a la ciberseguridad, sino también al funcionamiento económico, a los marcos referenciales de muchas disciplinas y con ello al ejercicio de la administración y de la gerencia. De esta manera, el discurso gerencial está impregnado por un debate que alude a lo virtual: comunidades virtuales, empresas virtuales, democracia virtual, y otros.

La amplificación del ciberespacio juega un rol esencial en las transformaciones en curso, como si se tratase de un oleaje de fondo que inunda los saberes, que hasta ahora eran referencia inamovible.

Sin duda, el ciberespacio constituye la esencia o punto preciso de la transformación en marcha, que hacen posible un movimiento inédito de virtualización, que nos obliga a de aprehender, a repensar, a comprender lo que acontece en materia organizacional.

Lo virtual, tiene poco o nada que ver con lo falso, lo ilusorio o lo imaginario. No es en modo alguno, lo opuesto a lo real. Se trata del paso de lo posible a lo real. Y es en esta dirección que a continuación, el lector encontrará otras voces que desde el debate de frontera en materia organizacional, reconocen en la cibernética, la ciencia que aporta muchos conocimientos acerca de los sistemas reguladores, capaz de reflejar toda la complejidad de lo acontece en el contexto interno de una organización, así como en el contexto global donde esta materializa su misión.

De allí que, otras voces plantean que, para estar en condiciones de actuar en relación con estas cuestiones como el ciberespacio y la virtualización, necesitamos una apoyatura conceptual solida que permita dilucidar respecto de sus

características, ventajas y desventajas que permitan discernir luego sobre sus propósitos, capacidades y forma de relacionamiento; cuestión esta, que los modelos tradicionales de organización abordan con extrema superficialidad.

Por ello, en un intento por superar estos vacíos, consultamos la visión de autores que abordan el tema de la organización virtual, que utilizan la noción de estructura para referirse a la manera como este tipo de organización logra acoplarse con un entorno representado por el ciberespacio con el cual interactúa, y para ello proponen centrarse en categorías analíticas que permiten captar la complejidad de lo real que acontece en el ciberespacio. Destacando que, al conocer sobre estas categorías en materia organizacional, permite saber cuáles son las condiciones actuales y potenciales para la supervivencia organizacional en el contexto actual donde se desenvuelven.

A continuación, el lector encontrará desde la perspectiva de estos autores la Conceptualización, Características, Ventajas y Desventajas de la Organización Cibernética.

Cuadro Nro. 2 Categorías para el Análisis de la Organización Cibernética

Autor	Conceptualización	Características	Ventajas	Desventajas
Abbe owshowitz (2002) Índice h: 27 Citas: 4.114	"Es una forma de estructurar y administrar actividades orientadas a objetivos basado en una distinción categórica entre los requisitos de una tarea (requisitos abstractos) y los elementos capaces de satisfacerlos (satisfactores), de forma que sea independiente de los medios para su realización, operado bajo un sistema de supervisión denominado metamanagement".	- Punto de vista de procesos. - Actividad orientada a objetivos. - Depende completamente del modelo de la innovación. - En constante renovación. - No tiene límites espaciales ni temporales. - Alto grado de flexibilidad. - Genera conceptos como: red, equipos virtuales. - Estrechamente relacionada con la división del trabajo. - Estructuras de control centralizadas o descentralizadas.	- Mejor rendimiento mediante el uso sistemático de la conmutación. - Uso eficiente de los recursos. - Mejora la capacidad de respuesta organizacional y promueve la reflexión organizacional. - Simplificación de tareas que conlleva al ahorro en la mano de obra, disminución del desperdicio y una menor factura salarial. - Costos indirectos son pequeños en comparación con las ganancias. - Sin estructura de control particular, ni requiere arreglos espaciales o funcionales específicos.	- Alto requerimiento de información precisa y compleja, tecnologías de información y comunicaciones y talento humano calificado, cuyo valor pudiera superar a lo ahorrado por los procesos. - Se necesitan nuevas actividades de gestión para organizar la actividad de manera virtual con su relativo nuevo costo de transacción. - El cambio excesivo, puede aumentar los costos en lugar de reducirlos.
Luis M. amarinha-Matos, Hamideh Afsarmanesh y Martin Ollus (2005) Índice h: 46 Citas: 10.445	"Es una alianza temporal de empresas que se unen para compartir habilidades o competencias centrales y recursos a fin de proporcionar al mundo exterior un conjunto de servicios y responder mejor al oportunismo empresarial, y cuya cooperación es respaldada por redes informáticas, actuando como si fueran una sola organización".	- Punto de vista estructural: la Organización Virtual se considera un tipo de cooperación entre organizaciones, empresas, grupos o individuos. - Actividad orientada a objetivos. - Puede ser una configuración dinámica dependiendo de la función / servicio que se proporcionará en ese momento. - Respaldada por TIC. - Sin restricciones físicas, geográficas o estructurales. - Puede ser una configuración más estable con un lapso considerable y un conjunto estable de servicios y funciones.	- Desmaterialización: los productos se vuelven potencialmente inmateriales. - Delocalización: potencialmente independiente del espacio. - Asincronización: contribuye al desacoplamiento de las condiciones temporales y espaciales (virtualización). - Atomización integrativa: para cada tarea individual en la empresa, se puede encontrar un licitador especializado, que a menudo ofrece un estándar del mercado mundial. - Temporalización: relacionado con la limitación temporal de las organizaciones virtuales. - No institucionalización: Al renunciar a la sede y al aumentar la reubicación del trabajo de la oficina al teletrabajo, los atributos físicos típicos de una empresa se vuelven virtuales. - Individualización: combina producción en masa de bajo costo con la personalización de productos y servicios.	- La selección de socios y el establecimiento para fundar organizaciones puede ser costoso en términos de tiempo y esfuerzo; por lo tanto, la Organización Virtual puede incluso obstaculizar el objetivo de ser ágil. - La demanda de nuevas habilidades desafiará a los líderes, especialmente en las organizaciones tradicionales. - El espíritu y las capacidades humanas solo pueden ser diseñados por un sistema de recursos humanos adecuado. - Debido a la necesidad de la empresa de cooperar con otras empresas, la confianza puede verse como una clave para las interacciones. - Carece de un marco legal coherente para abordar los reclamos con la entidad.

John Byrne (1993) Índice h: 67 Citas: 17.753	"Es una red temporal de proveedores de compañías independientes, clientes e incluso rivales vinculados por la tecnología de la información para compartir habilidades, costos y acceso a los mercados globales y explotar las oportunidades de negocios que cambian rápidamente hasta que se logre un determinado objetivo comercial".	- Punto de vista estructural. - Fronteras vagas y flexibles. - Los equipos de personas en diferentes compañías trabajan juntas, concurrentemente y no secuencialmente. - Recursos y capacidades distintivos. - Dimensión temporal. - Estado de transformación constante. - Depende completamente de las TIC. - Competencias principales - Red de unidades legalmente independientes - Jerarquías más planas, más organizaciones basadas en red de asociaciones - Propósito comercial común - Riesgos, recursos, conocimiento compartido - Basado en la confianza y oportunismo.	- Brinda a las empresas pequeñas la oportunidad de mantener su independencia y al mismo tiempo, de mejorar su competitividad. - Flexibilidad, adaptabilidad, capacidad de respuesta, menores costos y una mejor utilización de los recursos necesarios para cumplir con sus objeticos. - Gastos inmobiliarios reducidos. - Aumento de la productividad. - Altas ganancias. - Mejor servicio al cliente. - Elimina la falta de acceso a expertos.	- Disfunción como el bajo compromiso individual, la sobrecarga de roles, la ambigüedad de roles, el ausentismo y la holgazanería social pueden exagerarse en un contexto virtual. - Los clientes pueden percibir una falta de permanencia, confiabilidad y consistencia en las formas virtuales. - La dificultad de la reunión: hacer que la gente se una es costosa. - Problemas con la tecnología. - La falta de interacción física. - El costo adicional requerido para equipar a un trabajador móvil o a domicilio.

Fuente: Elaboración propia de los autores, (2020).

Hasta aquí, hemos presentado los contenidos básicos que forman parte del marco de referencia que hemos empleado para el acercamiento conceptual al debate, que subyace a esta investigación.

Las ideas y conceptos que hemos presentado de forma introductoria, en este momento de la publicación, forman parte de un marco de referencia más amplio sobre el debate actual del ciberespacio, la ciberseguridad y la cibernética organizacional; en la aspiración de transmitir al lector elementos clave que peritan comprender el entramado conceptual que soporta la propuesta del Modelo de Organización Cibernética para el Comando Cibernético Nacional.

Cerramos este momento, invitando al lector a revisar, un glosario de definiciones y términos asociadas al debate del ciberespacio, los cuales han sido incorporados como Apéndice Nro. 1

Momento III

CONSTRUCCIÓN DEL MODELO DE ORGANIZACIÓN CIBERNÉTICA DEL COMANDO CIBERNÉTICO NACIONAL

Mapa de Ciberamenazas que se ciernen sobre la República Bolivariana de Venezuela

Si bien es cierto que las amenazas que se ciernen sobre el ciberespacio de la República Bolivariana de Venezuela son precisas en sí mismas, también es cierto que el proceso de su aprehensión no se puede considerar como un mecanismo (programado), o un organismo (natural) sino como un sistema complejo, donde entran en interacción dinámica diferentes actores, con sus propósitos, las capacidades presentes y las contradicciones existentes, dada su orientación social, política y técnica. Dicha complejidad, sin duda, es la resultante que en ellas operen múltiples lógicas y diversidad de fuerzas encontradas, que no hacen del ciberespacio de la República Bolivariana de Venezuela un todo armónico, estable y predecible.

Y en tal sentido, la Organización para enfrentar los retos y desafíos de la Ciberseguridad, como unidad de análisis, es decir, como objeto específico de estudio, es un fenómeno complejo de reciente data. Considerarla desde este enfoque, pasa por una contrastación exhaustiva con la teoría Cibernética, la Teoría de las organizaciones Virtuales y la llamada Cuarta Revolución, ubicadas todas en su contexto histórico-social particular lo que influyó directa y sustantivamente en el propio proceso de construcción de conocimiento, el cual lleva esencialmente implícito la actividad, innovación, evolución y el cambio.

El paradigma clásico de la organización tradicional, enfoca la atención en el cumplimiento de objetivos de sus áreas funcionales que determinan su dinámica, en el logro efectivo de dichos objetivos. La teoría Cibernética Organizacional evalúa constantemente el entorno alrededor de los parámetros deseables, vale decir de la adaptación, la regulación y el control de la misma forma que frente a los procesos de comunicación y flujos de información.

Las Organizaciones dedicadas a la Ciberseguridad asumen su inserción en un entorno con características multidimensionales donde concurren factores y actores interesados en este novedoso tipo de amenaza compleja no tradicional, lo cual requirió de un marco de comprensión que involucró una perspectiva interpretativa y comprensiva. Los elementos anteriores son fundamentales para expresar, que esta investigación, parte de una realidad que no es lineal ni estable, la cual está marcada por la incertidumbre, divergencias, paradojas y la disrupción tecnológica que impulsó a fijarnos tanto en los procesos como en las situaciones, con el fin de lograr respuestas.

La construcción del mapa ciberamenazas que se ciernen sobre la República

Bolivariana de Venezuela, constituyó el enfoque inicial exploratorio y de apertura mental ante el problema investigado: en este sentido, se abordó esta problemática utilizando técnicas fenomenológicas y hermenéuticas, como la observación participante e interpretación inicial, para otear la posible bibliografía que sirviera como muestra teórica, y autores que fungieran como informantes clave que permitieron acercamiento a ese mundo de la seguridad nacional no tradicional. Una participación intensa de los autores en el medio social estudiado, evitó descontextualizar los datos, aislándolos de su entorno natural, recogiendo la información en la forma más completa posible.

Para ello, se empleó la técnica de investigación con énfasis la participación de informantes clave, conocida como el focus group. En esta parte la investigación con el apoyo institucional del Observatorio Nacional de Ciencia, Tecnología e Innovación (ONCTI), se organizó un grupo focal donde participaron informantes de 12 organismos que representan 3 estratos del sector público nacional (Organismos, Universidades y Centros de Investigación, Desarrollo e Innovación), lo que permite afirmar que dicha muestra aunque no contiene una representatividad de los distintos sectores nacionales; lo cierto, es que la situación ocasionada por la pandemia de la Covid-19, ha dificultado que estas instituciones logren equilibrar dos prioridades para responderle a la calamidad: protección contra nuevas amenazas cibernéticas y mantener la continuidad operacional con el empleo del teletrabajo, ante lo cual, un aspecto a destacar es el grado de preparación para atender una calamidad.

A continuación, se sistematizan los resultados obtenidos del focus group:

Cuadro Nro 3. Principales resultados por tipo de institución

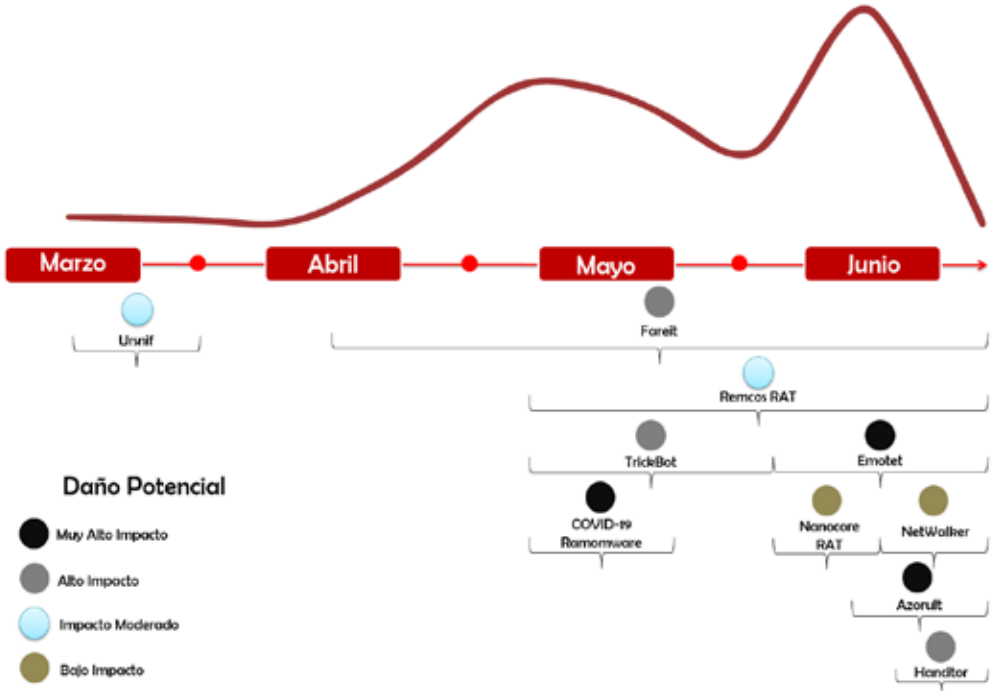
Organismos	Universidades	Centros De I+D+I
En el 75 % no existe una única área responsable de la ciberseguridad.	En el 100 % no existe una única área responsable de la ciberseguridad.	En el 50 % no existe una única área responsable de la ciberseguridad.
En el 100 % existen más de dos (2) niveles jerárquicos entre el CEO y el máximo responsable de la seguridad digital.	En el 100 % existen más de dos (2) niveles jerárquicos entre el CEO y el máximo responsable de la seguridad digital.	En el 50 % existe un (1) nivel jerárquico entre el CEO y el máximo responsable de la seguridad digital.
El 25 % cuenta con un equipo de trabajo conformado por 1-5 miembros.	El 100 % no cuenta con un equipo de trabajo conformado para la seguridad digital.	El 100 % cuenta con un equipo conformado por 1-5 miembros.
El 75 % no está implementando herramientas, controles o procesos usando tecnologías digitales emergentes.	El 100 % no está implementando herramientas, controles o procesos usando tecnologías digitales emergentes.	El 75 % no está implementando herramientas, controles o procesos usando tecnologías digitales emergentes.
El 100 % fue objeto de ataques o incidentes cibernéticos.	El 100 % fue objeto de ataques o incidentes cibernéticos.	El 100 % fue objeto de ataques o incidentes cibernéticos.
El 50 % identificó ocurrencia de eventos de malware diariamente	El 25 % identificó ocurrencia de eventos de malware diariamente.	El 50 % identificó ocurrencia de eventos de malware diariamente.
El 100 % fue objeto durante el mes de abril, de una campaña aprovechando los correos electrónicos de phishing que hacen referencia a los términos COVID-19.	El 25 % fue objeto durante el mes de abril, de una campaña aprovechando los correos electrónicos de phishing que hacen referencia a los términos COVID-19.	El 100 % fue objeto durante el mes de abril, de una campaña aprovechando los correos electrónicos de phishing que hacen referencia a los términos COVID-19.
El 25 %, durante el mes de mayo, fueron objeto de robo de información por medio de herramientas de acceso remoto (RAT) y del malware Trickbot	El 25 %, durante el mes de mayo, fue objeto de robo de información por medio de herramientas de acceso remoto (RAT) y del malware Trickbot	El 50 %, durante el mes de mayo, fue objeto de robo de información por medio de herramientas de acceso remoto (RAT) y del malware Trickbot
El 25 %, durante el mes de mayo, reporta surgimiento de ransomware COVID-19.	El 100 %, durante el mes de mayo, reporta surgimiento de ransomware COVID-19.	El 50 %, durante el mes de mayo, reporta surgimiento de ransomware COVID-19.

El 50 %, durante el mes de mayo, reporta correos electrónicos de phishing para promocionar un sitio web falso, con un mapa global de infección por coronavirus (malware Azorult y Hancitor).	El 25 %, durante el mes de mayo, reporta correos electrónicos de phishing para promocionar un sitio web falso, con un mapa global de infección por coronavirus (malware Azorult y Hancitor).	El 75 %, durante el mes de mayo, reporta correos electrónicos de phishing para promocionar un sitio web falso, con un mapa global de infección por coronavirus (malware Azorult y Hancitor).
El 75 % reporta archivo malicioso llamado "CORONAVIRUS_COVID-19.vbs", producto del ransomware Netwalker.	El 25 % reporta archivo malicioso llamado "CORONAVIRUS_COVID-19.vbs", producto del ransomware Netwalker.	El 25 % reporta archivo malicioso llamado "CORONAVIRUS_COVID-19.vbs", producto del ransomware Netwalker.
El 25% realizó una evaluación de ciberseguridad y está adelantando las acciones correspondientes.	El 100% no realizó una evaluación de ciberseguridad y no está adelantando las acciones correspondientes.	El 50% realizó una evaluación de ciberseguridad y está adelantando las acciones correspondientes.
El 25 % ofrece un mecanismo para que sus usuarios reporten incidentes a la entidad.	El 100 % no ofrece un mecanismo para que sus usuarios reporten incidentes (ataques exitosos) sufridos a la entidad.	El 100 % no ofrece un mecanismo para que sus usuarios reporten incidentes a la entidad.
El 100 % no cuenta con un plan de comunicaciones para informar a sus usuarios cuando la información de la institución se haya visto comprometida.	El 100 % no cuenta con un plan de comunicaciones para informar a sus usuarios cuando la información de la institución se haya visto comprometida.	El 50 % cuenta con un plan de comunicaciones para informar a sus usuarios cuando la información de la institución se haya visto comprometida.
El 25 % reporta los incidentes sufridos ante Suscerte, autoridad de aplicación de la ley.	El 100 % no reporta los incidentes sufridos ante Suscerte, autoridad de aplicación de la ley.	El 50 % reporta los incidentes sufridos ante Suscerte, autoridad de aplicación de la ley.
El 100 % manifestó que no existe un presupuesto para ciberseguridad.	El 100 % manifestó que no existe un presupuesto para ciberseguridad.	El 75 % manifestó que no existe un presupuesto para ciberseguridad.
El 100 % manifestó que el impacto de respuesta y de recuperación ante incidentes de ciberseguridad es alto.	El 100 % manifestó que el impacto de respuesta y de recuperación ante incidentes de ciberseguridad es alto.	El 100 % manifestó que el impacto de respuesta y de recuperación ante incidentes de ciberseguridad es alto.

Fuente: Elaboración propia de los autores, (2020).

De esta consulta participativa, emerge un primer hallazgo, la elaboración de la línea de tiempo de los ciberataques en tiempo de pandemia en la República Bolivariana de Venezuela, la cual se ilustra en la Figura Nro. 2.

Figura Nro.2. Línea de tiempo de Ciberataques reportados durante la pandemia de la covid-19 en Venezuela



Fuente: Estudio de impacto de los ciberataques en tiempos de pandemia a la seguridad de la nación ONCTI 2020.

Una vez puestos en perspectiva las informaciones obtenidas sobre los riesgos relacionados con la ciberseguridad, a continuación, se construyó el Mapa de ciber amenazas que se ciernen sobre la República Bolivariana de Venezuela.

La valoración de las amenazas actuales y futuras es una parte importante de la evaluación de las prioridades a tener en cuenta en las crecientes medidas de seguridad.

Es de suma importancia la necesidad de tener presente la prevención, detección, respuesta, mitigación y recuperación junto con la cooperación internacional en su caso.

Por ello, a continuación, describiremos brevemente algunas de las amenazas que se han hecho más «populares» en los últimos tiempos por las repercusiones e impacto que han tenido en aquellos lugares y equipos donde se han producido. De allí que, se identifican los orígenes o agentes de la amenaza, las víctimas u objetivos que pueden verse atacados y los efectos que se esperan conseguir por los generadores de los ataques.

Cuadro Nro 4. Mapa de Cibe amenazas que se ciernen sobre la República Bolivariana de Venezuela

Origen de la amenaza	Estado/Sector es Energético – Comunicaciones – Banca y Finanzas – Transporte – Salud - Fuerzas Armadas - Educación	Privado/Sectores Comunicaciones – Banca y Finanzas – Transporte – Salud - Educación	Ciudadanos
Actores Estadales	Vulneración de infraestructuras críticas Interrupción de sistemas y aplicaciones Operaciones de información	Vulneración de infraestructuras críticas Interrupción de sistemas y aplicaciones Operaciones de información	Operaciones de información
	Neutralizar capacidades ofensivas y defensivas	Neutralizar capacidades ofensivas y defensivas	
Terroristas	Vulneración de infraestructuras críticas Interrupción de sistemas y aplicaciones Operaciones de información	Vulneración de infraestructuras críticas Interrupción de sistemas y aplicaciones Operaciones de información	Operaciones de información
	Neutralizar capacidades ofensivas y defensivas	Neutralizar capacidades ofensivas y defensivas	
	Toma de control de procesos	Toma de control de procesos	
Profesionales del ciberdelito	Interrupción de sistemas y aplicaciones	Interrupción de sistemas y aplicaciones	Interrupción de sistemas y aplicaciones
	Toma de sistemas y aplicaciones	Toma de control de sistemas y aplicaciones	Toma de control de sistemas y aplicaciones
	Sustracción, publicación, venta y manipulación de información	Sustracción, publicación, venta y manipulación de información	Sustracción, publicación, venta y manipulación de información
Cibervándalos y script kiddies	Interrupción de sistemas y aplicaciones	Interrupción de sistemas y aplicaciones	Sustracción, publicación, venta y manipulación de información
	Sustracción, publicación, venta y manipulación de información	Sustracción, publicación, venta y manipulación de información	
Hacktivistas	Sustracción y divulgación de información sustraída	Sustracción y divulgación de información sustraída	
	Desfiguraciones en páginas web	Desfiguraciones en páginas web	
	Interrupciones de sistemas/ Toma de control	Interrupciones de sistemas/ Toma de control	
Actores internos	Desinformación Interrupciones de sistemas / Toma de control	Desinformación Interrupciones de sistemas / Toma de control	
	Sustracción, publicación, venta y manipulación de información	Sustracción, publicación, venta y manipulación de información	
Ciber investigadores	Recibir y publicar información	Recibir y publicar información	
	Sustracción de información (Espionaje digital)	Sustracción de información (Espionaje digital)	
Organizaciones privadas	Recibir y publicar información	Recibir y publicar información	Uso, abuso y reventa de información
		Sustracción de información	

Bajo	No se han observado nuevas amenazas o se dispone de medio suficientes para neutralizarlas, o no ha habido incidentes especialmente significativos
Medio	Se han observado nuevas amenazas o tendencias, se dispone de medios (parciales) no suficientes para neutralizarlas, los incidentes detectados no han sido especialmente significativos
Alto	Se han presentados nuevas amenazas o tendencias, no se dispone de medios suficientes para neutralizarlas, los incidentes detectados han sido especialmente significativos

Fuente: Elaboración propia de los autores, (2020).

De esta manera, el lector podrá apreciar que la presente sistematización recoge en una matriz de amenazas globales la correlación entre los orígenes de la amenaza y sus víctimas, identificando los ámbitos de las agresiones y los efectos a conseguir:

Desde el punto de vista de Seguridad de la Nación, se destaca uno de los mayores problemas, el cual se encuentra en las infraestructuras críticas asociadas a la continuidad de los servicios públicos que garantizan la estabilidad de la sociedad venezolana.

Su desinformación o desconocimiento ante estos, riesgos ponen en peligro la Seguridad de la Nación; y la falta de una organización, que cumpla funciones de detección, exploración, neutralización, ciberdefensa y ciberataque, hacen vulnerable al Estado Venezolano y sus instituciones a los ojos de actores internos y externos, que en rol de ciberdelincuentes explotan las oportunidades ,que en esta materia brinda este nuevo campo de batalla o teatro de operaciones: el ciberespacio.

Propósitos, Capacidades y Relaciones de la República Bolivariana de Venezuela para hacer frente a los desafíos relacionados con la ciberseguridad

Para el logro de este objetivo de la investigación que apuntaba en la dirección de generar una contextualización sobre las Organizaciones del Estado Venezolano dedicadas al tema de la ciberseguridad, se adoptó como estrategia, la investigación documental, relacionada con las nueve (9) Instituciones públicas con competencia en la materia, a saber: Superintendencia de Servicios de Certificación Electrónica (SUCERTE), Sistema Nacional de Gestión de Incidentes Telemáticos (VENCERT), Centro Nacional de Informática Forense (CENIF), Centro Nacional de Tecnologías de Información (CNTI), Comisión Nacional de Tecnologías de Información (CONATI), Comisión Nacional de Telecomunicaciones (CONATEL), Centro Nacional de Desarrollo e Investigación en Tecnologías Libres (CENDITEL), Consejo Superior de Ciberdefensa, Dirección Conjunta de Ciberdefensa de la Fuerza Armada Nacional Bolivariana (DICOFANB). En tal sentido, se realizó una búsqueda a través de la Web de los sitos oficiales de estas instituciones.

Cuadro Nro 5.- Relaciones, Propósitos y Capacidades de la República Bolivariana de Venezuela para hacer frente a los desafíos relacionados con la ciberseguridad

Organismo	Relaciones	Propósitos	Capacidades
Superintendencia de Servicios de Certificación Electrónica (SUCERTE)	Ministerio del Poder Popular para las Telecomunicaciones y la Informática (MPPTI) - Ministerio del Poder Popular de Ciencia y Tecnología (MPPCT), - Proveedores de Servicios de Certificación públicos o privados.	- Desarrollar y promover los Sistemas Nacionales de Seguridad de Información, Certificación Electrónica y Gestión de Incidentes Telemáticos, como herramientas habilitadoras del desarrollo tecnológico nacional, favoreciendo la inclusión del soberano en los servicios de gobierno electrónico y fortaleciendo los Sistemas de Información de los Órganos y Entes del Poder Público	- Coordinar e implementar el modelo jerárquico de la infraestructura Nacional de Certificación Electrónica -Acreditar, supervisar y controlar a los Proveedores de Servicios de Certificación (PSC) y ser el ente responsable de la Autoridad de Certificación Raíz del Estado Venezolano, posee una infraestructura de Claves Públicas y Privadas (PKI) -Infraestructura de Claves Públicas y Privadas (PKI) -Generar los Certificados para que Proveedores de Tiempo generen el servicio para los documentos y transacciones electrónicas.
Sistema Nacional de gestión de Incidentes Telemáticos (VENCERT)	- Ministerio del Poder Popular para las Telecomunicaciones y la Informática. (MPPTI) - Ministerio del Poder Popular de Ciencia y Tecnología (MPPCT), - Superintendencia de Servicios de Certificación Electrónica (SUCERTE) - Instituciones del Estado	- Centralizar y coordinar los esfuerzos para el manejo de incidentes que afecten los recursos informáticos de la Administración Pública de Venezuela, así como difundir información de como neutralizar sucesos y tomar precauciones para las amenazas de virus y gusanos informáticos, que puedan comprometer la disponibilidad y confiabilidad de las redes del Estado.	- Manejo de incidentes que afecten o puedan afectar los recursos informáticos de la Administración Pública; así como difundir información de cómo neutralizar incidentes, tomar precauciones para las amenazas de virus que puedan comprometer la disponibilidad y confiabilidad de las redes. -Aplicación de técnicas científicas y analíticas especializadas a infraestructuras tecnológicas que permiten realizar los procesos de Preservación, Colección, Análisis y Presentación de evidencia digital, de acuerdo a procedimientos Técnico-Legales preestablecidos, como apoyo a la Administración de Justicia en la resolución de un caso Legal.
Centro Nacional de Informática Forense (CENIF)	Superintendencia de Servicios de Certificación Electrónica (SUCERTE) -Instituciones del Estado	Laboratorio de informática forense para la adquisición, análisis, preservación y presentación de las evidencias relacionadas a la tecnologías de información y comunicación, con el objeto de prestar apoyo a los cuerpos de investigación judicial órganos y entes del Estado que así lo requieran.	- Apoyo técnico de todos los cuerpos y órganos del Estado con competencia en materia de experticias digitales.
Centro Nacional de tecnologías de Información (CNTI)	- Ministerio del Poder Popular de Ciencia y Tecnología (MPPCT),	- Impulsar y respaldar actividades de docencia, investigación y desarrollo científico y tecnológico...	-Facilitar la interconexión que permita utilizar los servicios de telecomunicación para el intercambio de información. -Implementación de planes y programas educativos, tales como: cursos de alfabetización tecnológica para operar computadoras y adiestrarse en el uso de herramientas Web; producción de Software Educativo y capacitación en aplicaciones libres a través de la Academia de Software Libre
Comisión Nacional de tecnologías de Información (CONATI)	- Ministerio del Poder Popular de Ciencia y Tecnología (MPPCT), - Cooperación a gran escala entre organizaciones que responden ante ciertos incentivos de mercado, se basan en el aprovechamiento de oportunidades y son siempre temporales. - Relaciones de comunicación con proveedores, distribuidores y detallistas, lo que implica nivel de información compartida. - Basado en la confianza.	- El proceso de desarrollo de productos mediante el uso de diseño y simulación por ordenador, la utilización de equipos de diseño y la consideración de clientes y proveedores como recursos. - El proceso de producción caracterizado por la flexibilidad, equipos de trabajo, la mejora continua, la producción "justo-a-tiempo", el control de la calidad total, la participación de proveedores y clientes y la producción instantánea y descentralizada.	- Los recursos complementarios que existen en las empresas que cooperan se dejan en su lugar, pero se integran para respaldar un esfuerzo de producto en particular mientras sea económicamente justificable hacerlo. - Las redes informativas ayudarán a las organizaciones remotas a vincularse y trabajar juntas, y las asociaciones se basarán en contratos electrónicos. - Cada socio aporta su competencia central al esfuerzo.

Comisión Nacional de Telecomunicaciones (CONATEL)	- Presidencia de la República - Ministerio del Poder Popular de Comunicación e Información. Radio, Televisión y Medios Electrónicos	Socializar el uso y aplicación de las telecomunicaciones y democratizar su acceso hasta convertirlas en plataforma habilitadora de desarrollo para consolidar la República. Monitorizar los mensajes difundidos por los prestadores de servicios de radio y televisión, y verificar el cumplimiento de leyes como la de Responsabilidad Social en Radio, Televisión y Medios Electrónicos.	- Estaciones de trabajo creadas para monitorizar las diferentes zonas espectrales del país, investigar interferencias perjudiciales; registrar las señales y analizar los parámetros de las emisiones radioeléctricas de los prestadores de servicio. Cuentan con el apoyo de Unidades Móviles y equipos portátiles que permiten la comprobación técnica de las emisiones en un rango de frecuencias entre 10 Khz y 18 Ghz, para que las Gerencias de Conatel puedan sustentarse de esta información y determinar sus planes a seguir. Los CAC están constituidos por seis (6) estaciones ubicadas en Distrito Capital, Lara, Monagas, Nueva Esparta, Táchira y Zulia. Cada una de ellas con responsabilidades asignadas sobre una de las seis (6) Zonas Espectrales en las que se divide el territorio nacional.
Centro Nacional de Desarrollo e Investigación en Tecnologías Libres (CENDITEL)	- Ministerio del Poder Popular de Ciencia y Tecnología (MPPCT), Centros, Grupos y Laboratorios de Investigación, Empresas públicas y privadas, PyMES, Emprendedores,	- Impulsar a nivel nacional las tecnologías de información y comunicación con estándares libres, promoviendo la investigación y el desarrollo de productos innovadores que conduzcan a la soberanía tecnológica del país	- Investigación, desarrollo y apropiación de Tecnologías Libre - Consultoría de Tecnologías Libres - Cursos de Formación En Línea -Diseño de Dispositivos de control tipo PLC
Consejo Superior de Ciberdefensa		-Configuración de las políticas públicas de un sector vital como lo es la ciberseguridad y ciberdefensa	
Dirección Conjunta de Ciberdefensa de la Fuerza Armada Nacional Bolivariana (DICDFANB)	Ministerio popular para la Defensa (MPPD)	Planificar, proteger, neutralizar, sincronizar y conducir las Operaciones de Ciberdefensa con el fin de asegurar la integridad de las Redes de Sistemas Informáticos y de Telecomunicaciones del Comando Estratégico Operacional, así como también responder a los posibles ciberataques, amenazas y agresiones que puedan afectar a los sistemas de mando y control, infraestructura crítica, sistemas de armas y la seguridad de la información de la Fuerza Armada Nacional Bolivariana y demás organismos de interés estratégico nacional, asegurando el uso del ciberespacio y negándolo al enemigo.	-Redes sociales; -Operaciones de ciberdefensa -Gestión de seguridad informática -Investigación y desarrollo y por supuesto -Gestión administrativa.

Fuente: Elaboración propia de los autores, (2020).

Seguidamente se presentan los hallazgos obtenidos como producto de la realización de entrevistas focalizadas a tres (3) informantes de alto nivel, autores de obras relacionadas con el tema de la organización Cibernética.

Para esto, los investigadores contactaron a los entrevistados vía correo electrónico materializando una conversación previa donde se les planteó la intencionalidad del trabajo investigativo, que da origen a esta publicación, solicitándole que confirmaran su disposición a colaborar a través de una entrevista focalizada relacionada con los objetivos de la investigación, quienes a la brevedad respondieron agradeciendo la consideración del investigador hacia ellos y poniéndose a la orden para colaborar en la medida de sus posibilidades.

Los autores que participaron en calidad de informantes, fueron seleccionados en virtud de su Índice h. El índice h es un sistema propuesto por Jorge Hirsch, de la Universidad de California, para la medición de la calidad profesional de científicos, en función de la cantidad de citas que han recibido sus artículos científicos. Así, la elección de estos informantes se justificó principalmente por ser autores relevantes en el eje temático de la Organización cibernética. Dichos informantes fueron:

a.- *Dr. Abbe Mowshowitz*. Profesor de Ciencias de la Computación en el City College de la Universidad de New York, Estados Unidos, quien además es profesor invitado en la Escuela de Gerencia de Rotterdam. Su pensamiento y obras han estado orientados al campo social y organizacional en el área de la computación desde los años 70 hasta nuestros días. Su libro Virtual Organization. Toward a theory of societal transformation stimulated by information technology (Organización Virtual. Hacia una teoría de transformación social estimulada por la tecnología de información) fue publicado 2002 en Westport, Estados Unidos de América por la Editorial Quorum Books. Su índice bibliométrico (índice h) es de 27 sobre 4.114 citas.

b.- *Dr. John Byrne*, escritor, productor de televisión norteamericana, columnista de ABC News, editor de la revista tecnológica Wired y del website Edgelings.com, sitio en la red enfocado en noticias en las áreas de gerencia y tecnología en Silicon Valley, California (EE.UU.). Su obra The futurists who fathered the ideas (Los futuristas que engendraron las ideas), publicado en febrero de 1993 en la revista Business Week en Estados Unidos de América. Su índice bibliométrico es 67 sobre 17.753 citas.

c.- *Dr. Luís Camarinha Matos*, líder del Grupo de Robótica y Manufactura Integrada en la Nueva Universidad de Lisboa en Portugal y líder de Sistemas Distribuidos y Redes Colaborativas en el mismo instituto. Director Científico del Proyecto integrado ECOLEAD, iniciativa europea para colaboración en redes cuyas áreas incluyen: Organización Virtual, comunidades virtuales, sistemas multiagentes, entre otros. Ha editado varios libros, donde destaca Virtual Organizations: Systems and practices (Organizaciones virtuales: sistemas y practices) publicado en 2005 en New York, Estados Unidos de América por la editorial Springer y cuyos autores son los Doctores: Luis M. Camarinha Matos (Nueva Universidad de Lisboa, Portugal), Dra. Hamideh Afsarmanesh (Universidad de Amsterdam, Países Bajos) y Dr. Martin Ollus (VTT Automation, Finlandia). Su índice bibliométrico (índice h) es de 46 sobre 10.445 citas. El resultado de estas entrevistas con la definición de relaciones, propósitos y capacidades de una organización cibernética se presentan a continuación:

Cuadro Nro 6.- Teoría Organizacional: Relaciones, Propósitos y Capacidades

Autor	Relaciones	Propósitos	Capacidades
Abbe Mowshowitz (2002)	- Estructuras de control centralizadas o descentralizadas. - Acoplamiento entre las multinacionales y sus proveedores.	- Estructurar y administrar actividades orientadas a objetivos basado en una distinción categórica entre los requisitos de una tarea (requisitos abstractos) y los elementos capaces de satisfacerlos (satisfactores).	- Separación de conceptualización de la ejecución de tareas. - Uso de criterios objetivos para la asignación de recursos. - Confiar en la idea de separar las necesidades de los modos de satisfacción como un principio general, aplicable a todas las funciones de gestión. - La asignación de satisfactores a los requisitos, se basa en el concepto de asignación de recursos en la investigación de operaciones. - Uso de la conmutación para facilitar el uso eficiente de los recursos.
John Byrne (1993)	- No existe un socio central, por lo que existe igualdad entre los socios y liderazgo compartido. - Cooperación a gran escala entre organizaciones que responden ante ciertos incentivos de mercado, se basan en el aprovechamiento de oportunidades y son siempre temporales. - Relaciones de comunicación con proveedores, distribuidores y detallistas, lo que implica nivel de información compartida. Basado en la confianza.	- El proceso de desarrollo de productos mediante el uso de diseño y simulación por ordenador, la utilización de equipos de diseño y la consideración de clientes y proveedores como recursos. - El proceso de producción caracterizado por la flexibilidad, equipos de trabajo, la mejora continua, la producción "justo-a-tiempo", el control de la calidad total, la participación de proveedores y clientes y la producción instantánea y descentralizada	- Los recursos complementarios que existen en las empresas que cooperan se dejan en su lugar, pero se integran para respaldar un esfuerzo de producto en particular mientras sea económicamente justificable hacerlo. - Las redes informativas ayudarán a las organizaciones remotas a vincularse y trabajar juntas, y las asociaciones se basarán en contratos electrónicos. - Cada socio aporta su competencia central al esfuerzo.
Luis M. Camarinha-Matos, Hamideh Afsarmanesh y Martin Ollus (2005)	Una Organización Cibernética se compone de entidades semiindependientes con competencias básicas separadas, que se unen para lograr un objetivo empresarial prescrito o suscrito, respaldado por tecnologías de información y comunicación.	Proporcionar al mundo exterior un conjunto de servicios y responde mejor al oportunismo empresarial. - Orientada para lograr objetivos.	- La cooperación es respaldada por redes informáticas, actuando como si fueran una sola organización. - Utiliza la tecnología de información para unir dinámicamente a personas, activos e ideas, que a menudo surge de una red de empresas que se unen rápidamente para explotar oportunidades continuamente cambiantes. - Se comparten recursos y capacidades básicas para incrementar el tamaño aparente o la cobertura geográfica que un competidor puede ofrecer a un cliente.

Fuente: Elaboración propia de los autores, (2020).

De igual forma, para el abordaje del tema de la Ciberseguridad se realizaron entrevistas focalizadas a informantes de alto nivel, dos (2) de ellos autores de obras relacionadas con esta temática. Para este caso, se replicó el procedimiento explicado con anterioridad. Destacando que, de igual forma, que la selección de los autores atendió al criterio del Índice h. Dichos informantes solicitaron que garantizáramos su anonimato:

a.- El primero de ello es el investigador para asuntos políticos y de seguridad del Centro de Estudios de Asia de la Fundación Heritage. Se especializa en la política exterior y militar china, y ha escrito extensamente las implicaciones tecnológicas del programa espacial y los problemas de "doble uso" asociados con la infraestructura industrial y científica de China.

b. El segundo, es consultor internacional de seguridad, Postgraduado en las áreas de seguridad pública y privada, defensa comunicaciones. Dedicado por más de 30 años a la Consultoría e Ingeniería de Seguridad y Defensa por más de 20 países como asesor para asuntos aeroportuarios, puertos, cárceles hospitales, entidades bancarias, museos, transporte ferroviario, servicios de Correos y puertos.

Seguidamente se presenta la síntesis de los hallazgos obtenidos producto de entrevistas a profundidad a tres (3) de los cinco (5) especialistas en el tema de la Ciberdefensa. Las entrevistas in extenso el lector las encontrará en el apéndice Nro.3

Cuadro Nro. 7.- Hallazgos de las entrevistas a especialistas en Ciberdefensa

Informante	Misión Comando Cibernético Nacional	Actividades reguladoras de un Comando Cibernético Nacional	Resolución de Conflictos	Detección de amenazas / oportunidades provenientes del exterior en un Comando Cibernético Nacional	Propósitos	Capacidades
Nro.1	El uso de la tecnología para reunir inteligencia en el campo de batalla, coordinar las operaciones conjuntas de diferentes recursos militares y ayudar en la selección de sus objetivos, sino también, su uso para influir en la opinión pública de ciertos países, llevar a cabo actividades de espionaje y acceder a las ciberinfraestructuras militares y civiles de los que considera sus adversarios.	-Un Gobierno debe controlar e influenciar la totalidad del flujo de información hacia sus adentros, lo cual implica moldear las estructuras internacionales que administran ese flujo de información.	- Los intereses políticos, económicos y de seguridad de un estado están ahora cada vez más conectados con la ciberseguridad. Sin embargo, Internet es un arma de doble filo, es decir, no solo ofrece enormes beneficios, sino también numerosos riesgos, desafíos y amenazas. Por lo tanto, dada la naturaleza sin fronteras, transnacional y única del ciberespacio, se ha convertido en una nueva frontera para la gobernanza global.	- Mmplazado una 'Gran Muralla Cortafuegos ' y desplegado un número de censores en el orden de los centenares de miles, a los efectos de limitar la amenaza informativa.	- Estructurar y administrar actividades orientadas a objetivos basado en una distinción categórica entre los requisitos de una tarea (requisitos abstractos) y los elementos capaces de satisfacerlos (satisfactores).	- Separación de conceptualización de la ejecución de tareas. - Uso de criterios objetivos para la asignación de recursos. - Confiar en la idea de separar las necesidades de los modos de satisfacción como un principio general, aplicable a todas las funciones de gestión. - La asignación de satisfactores a los requisitos, se basa en el concepto de asignación de recursos en la investigación de operaciones. - Uso de la conmutación para facilitar el uso eficiente de los recursos.

Nro. 2	- La razón de ser hoy día de un Comando Cibernético Nacional ante las emergentes amenazas en materia de ciberseguridad, es la lograr la adecuada transición de un modelo de ciberseguridad de carácter preventivo y defensivo, hacia un esquema que incorpore elementos de mayor fuerza disuasoria en un contexto global de mayor competencia geopolítica.	- El adecuado desarrollo de un Comando Cibernético Nacional, exige trabajar con un enfoque multidisciplinar en todos los sentidos, que englobe aspectos más allá de los básicamente técnicos, vale decir de consolidación dela infraestructura tecnológica necesaria; del monitoreo, registro y control de ciberataques; o de la ubicación y empleo adecuado del factor humano, que en estos momentos es paradójicamente escaso ero altamente demandado.	La gestión de las situaciones de crisis en cualquier ámbito, que por su transversalidad o dimensión, desborden las capacidades de respuesta de los mecanismos recursos habituales es responsabilidad ineludible de un CEOC.	Un Comando Cibernético Nacional, tiene sentido para apoyar al Consejo de Seguridad Nacional y asiste al Presidente del Gobierno en la dirección y coordinación de la política de Seguridad Nacional en el ámbito de la ciberseguridad. De esta manera fomenta las relaciones de coordinación, colaboración y cooperación entre Administraciones Públicas y entre estas y el sector privado, ante situaciones que por su transversalidad o dimensión, desborden las capacidades de respuesta de los mecanismos recursos habituales con que cuenta el ecosistema de ciberseguridad nacional.	Proporcionar al mundo exterior un conjunto de servicios y responde mejor al oportunismo empresarial. - Orientada para lograr objetivos.	- La cooperación es respaldada por redes informáticas, actuando como si fueran una sola organización. - Utiliza la tecnología de información para unir dinámicamente a personas, activos e ideas, que a menudo surge de una red de empresas que se unen rápidamente para explotar oportunidades continuamente cambiantes. - Se comparten recursos y capacidades básicas para incrementar el tamaño aparente o la cobertura geográfica que un competidor puede ofrecer a un cliente.

Fuente: Elaboración propia de los autores, (2020).

Elementos de creación de valor en materia de ciberseguridad para enfrentar los nuevos desafíos que afronta la República Bolivariana de Venezuela

A continuación, el lector encontrará la definición del cómo el Comando Cibernético Nacional creará valor para la República Bolivariana de Venezuela. En consecuencia, no se trata solo del producto / servicio, sino de todos los factores, alrededor del mismo, que aportan algún valor a la sociedad venezolana.

La propuesta de valor que a continuación se presenta, se compone por 6 cuadrantes:

1. Lo que usuarios están intentando solucionar o prevenir y que se constituye en un problema.

2.- Las frustraciones o emociones negativas antes, durante o después de las tareas.

3.- Los beneficios y lo que va a recibir el usuario por nuestros producto o servicio.

4.- Aquellas características de nuestra propuesta de valor que reducen las frustraciones de los usuarios.

5.- Cómo los productos o servicios crean valor, es decir, cómo generan beneficios para los usuarios.

6.- La oferta de productos y servicios.

A continuación, se presentan de manera sistematizada los resultados de un focus group realizado en las instalaciones de la Fundación Muronto: "Centro de Investigación y Desarrollo de la Fuerza Armada Nacional Bolivariana" con ocho (8) especialistas del área de Ciberseguridad, pertenecientes a Instituciones del Estado dedicadas a procesos de Ciberseguridad, quienes identificaron de manera colegiada los elementos de creación de valor que describen de manera lógica, la forma en que una organización dedicada a la Ciberseguridad de la Nación debe crear, entregar y capturar valor.

La Figura Nro. 3 muestra la Propuesta de Creación de Valor, resultante del 1er. ejercicio asociado al focus group:

Fuente: Elaboración propia de los autores, (2020).

Modelo de Negocios del Comando Cibernético Nacional para la República Bolivariana de Venezuela

Seguidamente, y como otro producto del ejercicio de focus group antes indicado, se presenta el Modelo de Negocios del Comando Cibernético Nacional para la República Bolivariana de Venezuela.

En su elaboración se siguió la siguiente metodología:

1.-Segmentar los usuarios, para conocer el nicho de demandantes y las oportunidades de prestación de servicio.

2- Definir bien la propuesta de valor, en otras palabras, saber por qué el Comando Cibernético Nacional constituye una propuesta innovadora y qué lo diferencia de las actuales instituciones dedicadas a la ciberseguridad y nos acerca a potenciales usuarios.

3- Delimitar los canales de comunicación, distribución y de estrategia comunicacional que se adoptará, para fortalecer la idea de un Comando Cibernético Nacional.

4.- Establecer la relación que mantendremos con los usuarios.

5.- Determinar las fuentes de financiamiento del Comando Cibernético Na-

cional, un aspecto fundamental si queremos tener éxito en su implementación.

6.- Identificar los activos y recursos clave que se requieren como piezas imprescindibles en el engranaje de la creación del Comando Cibernético Nacional.

7.- Conocer las actividades clave que darán valor al Comando Cibernético Nacional, y saber las estrategias necesarias para potenciarlas.

8.- Tener en cuenta los socios clave con los que establecer contactos y alianzas para el Comando Cibernético Nacional. En otras palabras, definir las estrategias de networking con potenciales socios o proveedores, entre otras figuras importantes.

9.- Marcar las estructuras de costes, para llegar a saber el precio que tendrá que pagar los usuarios por la prestación del servicio que ofrecerá el Comando Cibernético Nacional.

Nótese que la oferta de valor está en el lado derecho del esquema, donde se ve cuál es el mercado objetivo. Luego, entre la oferta de valor y el mercado objetivo, están los canales de distribución y la comunicación con los usuarios. En el lado izquierdo está toda la infraestructura que se requiere para hacer la oferta de valor. Están las redes con los aliados. De esta manera al determinar la población objetivo, el lector podrá comprender al usuario potencial, sus necesidades y preferencias. Y así saber cómo comunicarse con éste y cuáles serán los canales de distribución más adecuados porque han sido determinadas sus preferencias.

El cuadro Nro. 8 muestra el Modelo de Negocio resultante del 2do. ejercicio asociado al focus group:

Modelo de Negocio del Comando Cibernético Nacional

Socios clave:

- *Investigadores*
- *Empresas públicas y privadas*
- *DCCDFANB*
- *MPPCTI y sus entes adscritos*
- *MPPRI y sus entes adscritos*
- *Centros de investigación nacionales e internacionales (Müröntö, etc.)*
- *Consejo Científico Tecnológico Nacional*
- *Entes con capacidad ya instalada para la Ciberdefensa.*

Actividades clave:

- *Identificación de Ciberamenazas*
- *Protección contra Ciberataques*
- *Detección de Ciberamenazas*
- *Respuesta a tiempo a Ciberataques*
- *Recuperación de los Servicios en caso de Ciberataques*

Recursos clave:

- *Infraestructura Tecnológica robusta*
- *Talento Humano Especializado*
- *Centro de Operaciones corporativas*
- *Sistema de detección de Alertas tempránas.*

Propuesta de valor:

- *Consolidación del Comando Cibernético Nacional.*
- *Plan Estratégico Nacional en Materia de Cibersegridad*
- *Fortalecimiento de Infraestructuras Críticas*

Relaciones con los clientes:

- *Relacionamiento proactivo con organizaciones públicas y privadas, y con investigado-res del sector Ciberseguridad*
- *Política Pública en materia de Ciberseguridad.*

Canales:

- *Actividades de detección de Ciberamenazas.*
- *Portal WEB, RRSS y correo electrónico.*
- *Red de investigación en materia de Ciberseguridadcon alcance nacional.*

Clientes:

- *Estado (quien nos crea)*
- *Industrias o empresas públicas y privadas*
- *Investigadores*
- *Comunidades (usuarios de los servicios vitales)*
- *Entes de investigación del sector Ciberseguridad.*

Estructura de costos:

- *Pago de nóminas (Especialista/administrativos/obreros)*
- *Consolidación de la infraestructura propia, bajo un concepto arquitectónico y espacial propio.*
- *Plataforma tecnológica*
- *Gastos de funcionamiento*

Fuentes de ingreso:

- *Aportes del Ejecutivo nacional*
- *Sistema de producción para la autogestión*
- *Aportes de otros entes públicos y privados.*

Fuente: Elaboración propia de los autores, (2020).

A continuación, se conceptualizan los componentes del Modelo de Negocio antes presentado:

Clientes. El objetivo fue agrupar a los clientes con características homogéneas en segmentos definidos y describir sus necesidades.

Propuestas de valor. El objetivo fue definir el valor que deberá ser creado para cada segmento de clientes describiendo los productos y servicios que se ofrecerán. Estas primeras dos partes son el núcleo del modelo de negocio.

Canales. Se indica la manera en que se establece contacto con los clientes.

Relación con el cliente. Aquí se identificaron cuáles recursos de tiempo y monetarios se utiliza para mantenerse en contacto con los clientes. Por lo general, si un producto o servicio tiene un costo alto, entonces los clientes esperan tener una relación más cercana con nuestra empresa.

Fuentes de ingresos. Este paso tiene como objetivo identificar que aportación monetaria hace cada grupo y saber de donde vienen las entradas (ventas, comisiones, licencias, etc.). Así se podrá tener una visión global de cuáles grupos son más rentables y cuáles no.

Recursos clave. Después de haber trabajado con los clientes, hay que centrarse en la empresa. Para ello, hay que utilizar los datos obtenidos anteriormente, seleccionar la propuesta de valor más importante y la relacionarse con el segmento de clientes, los canales de distribución, las relaciones con los clientes, y los flujos de ingreso. Así, saber cuáles son los recursos clave que intervienen para que la empresa tenga la capacidad de entregar su oferta o propuesta de valor.

Actividades clave. En esta etapa es fundamental saber qué es lo más importante a realizar para que el modelo de negocios funcione. Utilizando la propuesta de valor más importante, los canales de distribución y las relaciones con los clientes, se definen las actividades necesarias para entregar la oferta.

Asociaciones claves. Fundamental es realizar alianzas estratégicas entre empresas, Joint Ventures, gobierno, proveedores, y otros. En este apartado se describe a los proveedores, socios, y asociados con quienes se trabaja para que la empresa funcione. ¿Qué tan importantes son? ¿se pueden reemplazar? ¿pueden convertir en competidores?

Estructura de costos. Aquí se especifican los costos de la empresa empezando con el más alto (marketing, R&D, CRM, producción, etc.). Luego se relaciona cada costo con los bloques definidos anteriormente, evitando generar demasiada complejidad. Posiblemente, se intente seguir el rastro de cada costo en relación con cada segmento de cliente para analizar las ganancias.

Modelo de Organización Cibernética del Comando Cibernético Nacional para la República Bolivariana de Venezuela

De acuerdo a Mariña (1994), repensar nuevas expresiones del Poder Público Nacional, supone moverse en la idea del isomorfismo cibernético de la naturaleza, lo cual implica replicar esquemas de

comportamiento y de los principios que rigen el universo y los sistemas que en él interactúan a todos sus niveles, para tratar de validar las leyes de la naturaleza en la definición de tales actividades que el engloba, ofreciéndose así una morfología organizacional, que recoja la complejidad de la realidad estudiada, y que permita diseñar los mecanismos para su adaptación, regulación y control.

En este contexto, la organización del Comando Cibernético Nacional constituye un caso de estudio ideal, para que desde el paradigma Cibernético, se explore la posibilidad de repensar su andamiaje organizativo, de forma de poder emular mecanismos de adaptación, regulación y control, que siendo exitosos en los seres vivos, para alcanzar máxima eficacia y eficiencia, puede servir como plataforma conceptual para coadyuvar en la creación de una organización dedicada a la ciberseguridad y ciberdefensa nacional.

El modelo de organización propuesto estará centrado en procesos decisionales, sustantivos y de apoyo, elementos de conformidad con lo pautado en la Ley Orgánica de la Administración Pública.

De allí que, la estructura organizativa del Comando Cibernético Nacional puede concebirse como una estructura organizacional recursiva, constituida por distintos niveles de recursión, que contienen unidades organizacionales que hoy existen y que pasarán a formar parte de ésta, que la vez estará contenidas en un sistema mayor. Esta concepción de cómo estructurar una institución, ofrece la posibilidad de asumir una estructura que apunte hacia la garantía del logro de la necesaria adaptación, regulación y el control de la organización, que permite que quien "Dirige" o quien "Comanda", pueda estar al tanto de lo que está sucediendo en el contexto interno y externo con el cual se interactúa.

Contextos estos, que en el caso del Comando Cibernético Nacional Venezolano, hoy se materializan en espacios dinámicos, abiertos y complejos representados hoy por la metáfora de la nube o el ciberespacio, donde como ya se ha reseñado, se generan nuevos tipos de amenazas que demandan a los entres responsables de garantizar la Seguridad de la Nación, la incorporación de mecanismos de atenuación y amplificación de variedad, con sus homeostatos respectivos, que le permitan mantener el monitoreo permanente de variables claves que habrán de redefinirse en términos de "variedad" y que son susceptibles de ser medidas, de forma que se puedan generar las señales de alerta temprana ante la ocurrencia de amenazas que atenten contra la estabilidad requerida y aprovechar las potencialidades para su atenuación, neutralización y/o ataque como un factor crítico de éxito.

En consecuencia, al concebir cibernéticamente al Comando Cibernético Nacional, delineando su misión, visión, valores y objetivos estratégicos es delinear una estructura centrada en procesos, estableciendo sus complejas interconexiones internas y externas y sus diferentes niveles de recursión, como un complejo andamiaje de unidades organizacionales, que de forma cohesionada y dada sus características propias, constituyen el la propuesta del Comando Cibernético Nacional quien deberá rectorizar las acciones de Ciberseguridad y Ciberdefensa, para que el Estado

Venezolano garantice la operatividad de las Infraestructuras críticas que soportadas en Tecnologías de Información son requeridas para la Defensa Integral de la Nación.

Teniendo estas orientaciones como telón de fondo, a continuación, se presenta de una manera esquemática la propuesta de la creación del Comando Cibernético Nacional.

Concepción Estratégica

Visión

Institución del Estado Venezolano, responsable de garantizar el uso pacífico del ciberespacio de la república Bolivariana de Venezuela, mediante las acciones de Ciberseguridad y Ciberdefensa, que garanticen la operatividad de las Infraestructuras de Criticas que soportadas en Tecnologías de Información son requeridas para la Defensa Integral de la Nación.

.

Misión

Garantizar el uso pacífico del ciberespacio de la República Bolivariana de Venezuela, mediante la detección, exploración y neutralización de ciberamenazas, así como la ciberseguridad y ciberdefensa que son requeridas para la Defensa Integral de la Nación,

Valores

Garantizar la operatividad de las Infraestructuras de Críticas del Estado Venezolano que son soportadas en Tecnologías de Información; implica el ejercicio de derechos consagrados en la Constitución de la República Bolivariana de Venezuela y leyes nacionales y por tanto los valores que deben regir para garantizarlo son:

- El libre acceso del ciberespacio
- El uso seguro del ciberespacio
- El uso responsable del ciberespacio

Mapa Estratégico

El Mapa de procesos muestra de manera gráfica los objetivos estratégicos que se aspiran alcanzar para dar cumplimiento a la misión y visión. El Grafico Nro. 4 ilustra el Mapa Estratégico del Comando Cibernético Nacional.

Fuente: Elaboración propia de los autores, (2020).

Mapa de Procesos

El Mapa de procesos muestra de manera gráfica los procesos medulares, estratégicos y de apoyo, requeridos para garantizar el logro de los objetivos estratégicos el Gráfico Nro. 5 ilustra el Mapa Procesos del Comando Cibernético Nacional.

Fuente: Elaboración propia de los autores, (2020).

Organización Cibernética

En atención al mapa de procesos antes presentado, se desprende la morfología organizativa propuesta el para Comando Cibernético Nacional, derivado de los principios de la teoría Cibernética, y que con el auxilio del Modelo de Sistemas Viables (MVS) permite diagramar la relación de los diferentes sistemas que lo conforman.

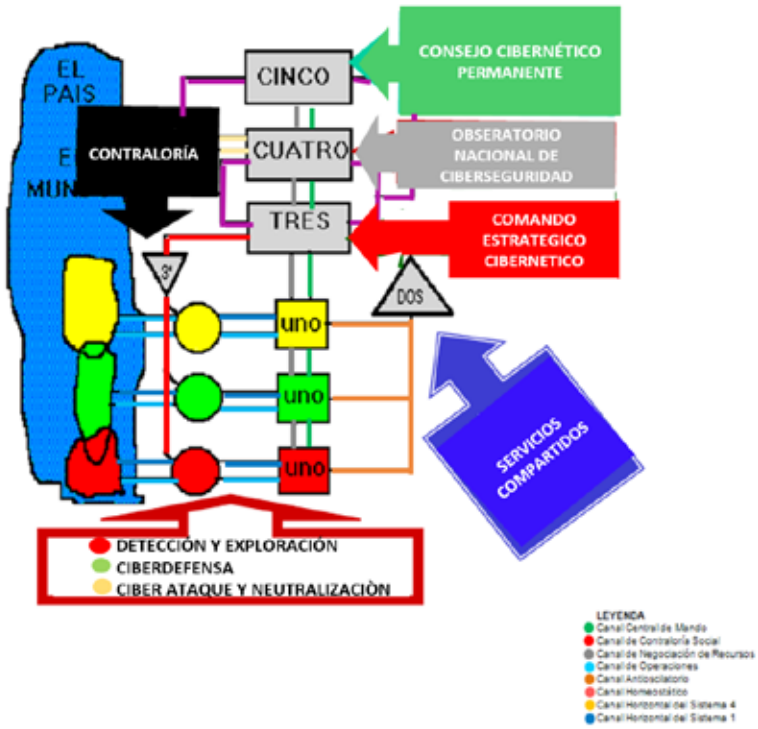
Las Figuras que a continuación se presentan, emergen como el resultado de la aplicación del planteamiento de la Cibernética Organizacional para la desagregación del sistema, estudiado en distintos niveles recursivos:

Para una mejor comprensión, por parte del lector, habría que recordar que en todas las figuras que se muestran a continuación, los rectángulos identificados en el plano vertical como UNO-TRES-CUATRO-CINCO, se corresponden con procesos denominados: Operativos, de Gerencia, Planificación y de Decisión respectivamente. Los triángulos que se muestran a mano derecha en el mismo plano vertical identificados como DOS, corresponden a procesos de apoyo.

Tanto los rectángulos como los triángulos están interconectados por flechas. Las conexiones indicadas por fechas en el plano vertical corresponden a flujos dinámicos de información que circulan entre las partes. Las conexiones en el plano vertical implican relación de amplificación o atenuación de elementos provenientes del entorno (léase "Variedad"). El entorno está simbolizado por la figura parecida a una amiba, dibujada a mano izquierda en repetidas ocasiones. Los círculos representan actividades operativas asociadas a los procesos operativos o de producción.

En consecuencia, en un primer nivel de recursión que se corresponde con el Nivel Corporativo del Comando Cibernético Nacional se muestran los 5 Sistemas que se comentan a continuación:

Figura Nro.4. Primer Nivel de Recursión del Modelo de Organización Cibernética del Comando Cibernético Nacional para la República Bolivariana de Venezuela



Fuente: Elaboración propia de los autores, (2020).

Esta particular concepción del Comando Cibernético Nacional, supone la presencia de 5 grandes Sistemas, a saber:

Sistema 5: Representado por el Consejo Cibernético Permanente, alta dirección del Comando Cibernético Nacional.

Sistema 4: Representado por el Observatorio de Ciberseguridad, quien es órgano facultado para el monitoreo y análisis permanente del entorno, detección de capacidades y necesidades, desarrollo de actividades propias de inteligencia, que habrá de concretarse en una sala situacional para la producción permanente de señales de alerta temprana.

Sistema 3: Representado por el Comando Estratégico Cibernético (CEC), quien asumirá la gerencia estratégica y conducción de Operaciones de ciberseguridad y ciberdefensa. Instancia encargada de la planificación, dirección y coordinación de los procesos medulares del Comando Cibernético Nacional en base de la orientación y de las normas dictadas por el órgano superior.

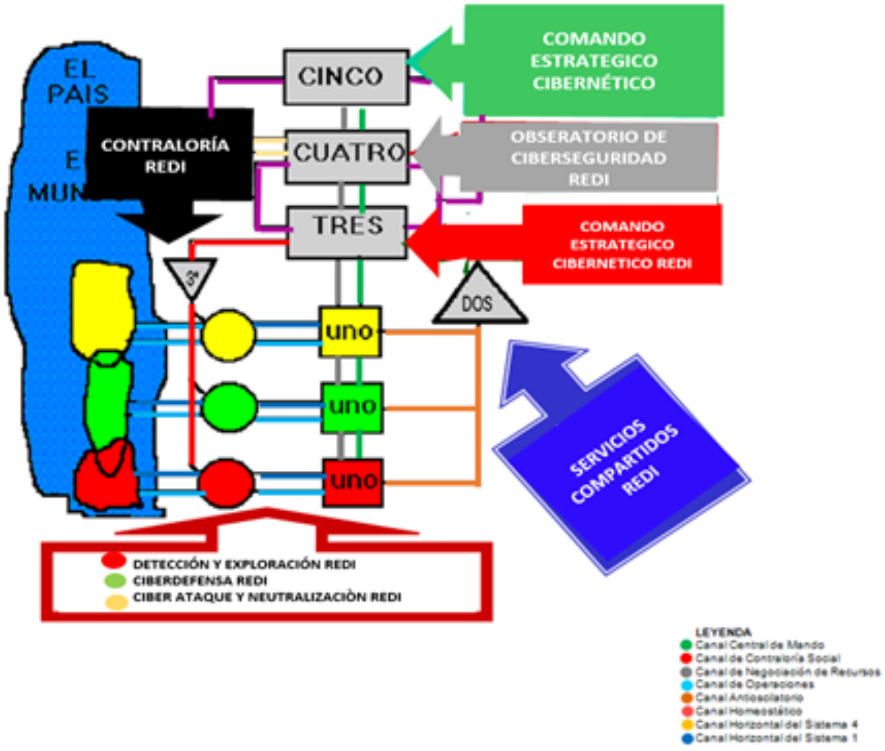
Sistema 2: Representado por las Gerencia de Servicios Compartidos, servicios que sirven de Apoyo a los procesos medulares del Comando Cibernético Nacional, poniendo a disposición de estos los recursos de toda clase, destina-

dos a apoyar los procesos, que en ellos se despliegan.

Sistemas 1: Representado por las unidades operacionales básicas o procesos medulares del Comando Cibernético Nacional que están facultadas para llevar a cabo actividades relacionadas con la Exploración y Detección de amenazas, la Ciberdefensa, la Neutralización y Ciberataques en sus respectivas jurisdicciones territoriales, de acuerdo a la división del territorio nacional para la garantía de la Seguridad y Defensa de la Nación. Vale decir en las Regiones de CiberDefensa Integral (RECDI), en las Zonas de CiberDefensa Integral (ZOCDI) y en las áreas de CiberDefensa Integral (ACDI).

El Modelo propuesto se habrá de replicar a niveles de Regiones de Defensa Integral (REDI), en las Zonas de Defensa Integral (ZODI) y en las áreas de Defensa Integral (ADI). Con lo cual el Comando Cibernético Nacional podría desplegar todo su potencial a través de 4 niveles de recursión que se ilustran a continuación:

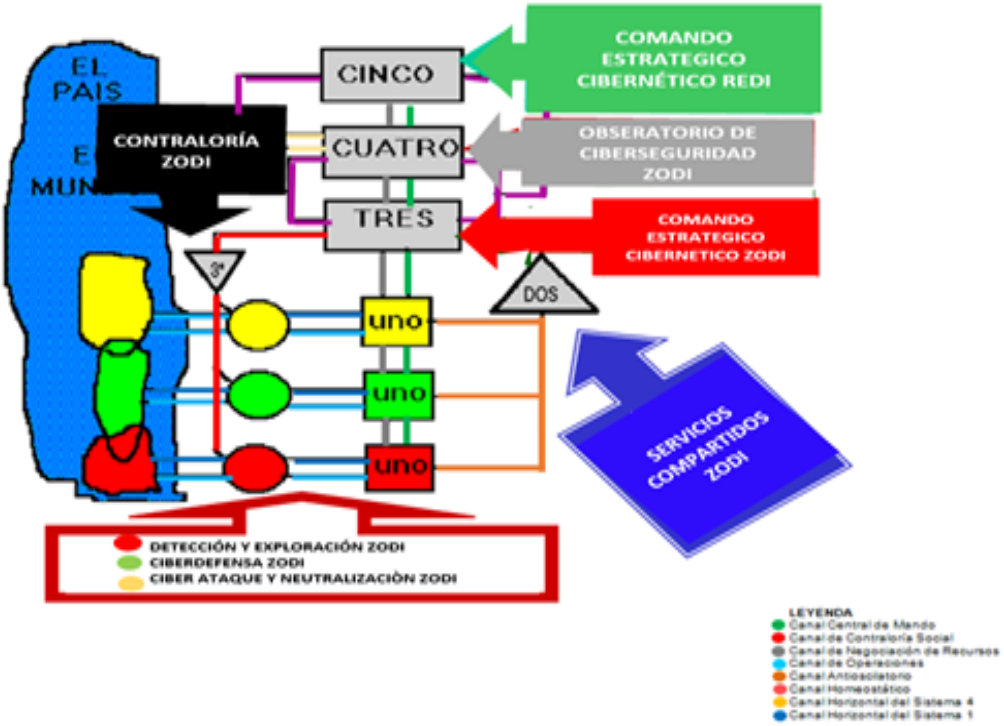
Figura Nro.5. Segundo Nivel de Recursión del Modelo de Organización Cibernética del Comando Cibernético Nacional para la República Bolivariana de Venezuela.



Fuente: Elaboración propia de los autores, (2020).

Sistema 5: Representado por el Comando Estratégico Cibernético.
Sistema 4: Representado por el Observatorio de Ciberseguridad de la REDI.
Sistema 3: Representado por el Comando Estratégico Cibernético de la REDI.
Sistema 2: Representado por las Gerencia de Servicios Compartidos de la REDI.
Sistemas 1: Representado por las unidades operacionales básicas o procesos medulares del Comando Cibernético Nacional que están facultadas para llevar a cabo actividades relacionadas con la Exploración y Detección de amenazas, la Ciberdefensa, la Neutralización y Ciberataques en las Regiones de Defensa Integral (REDI).

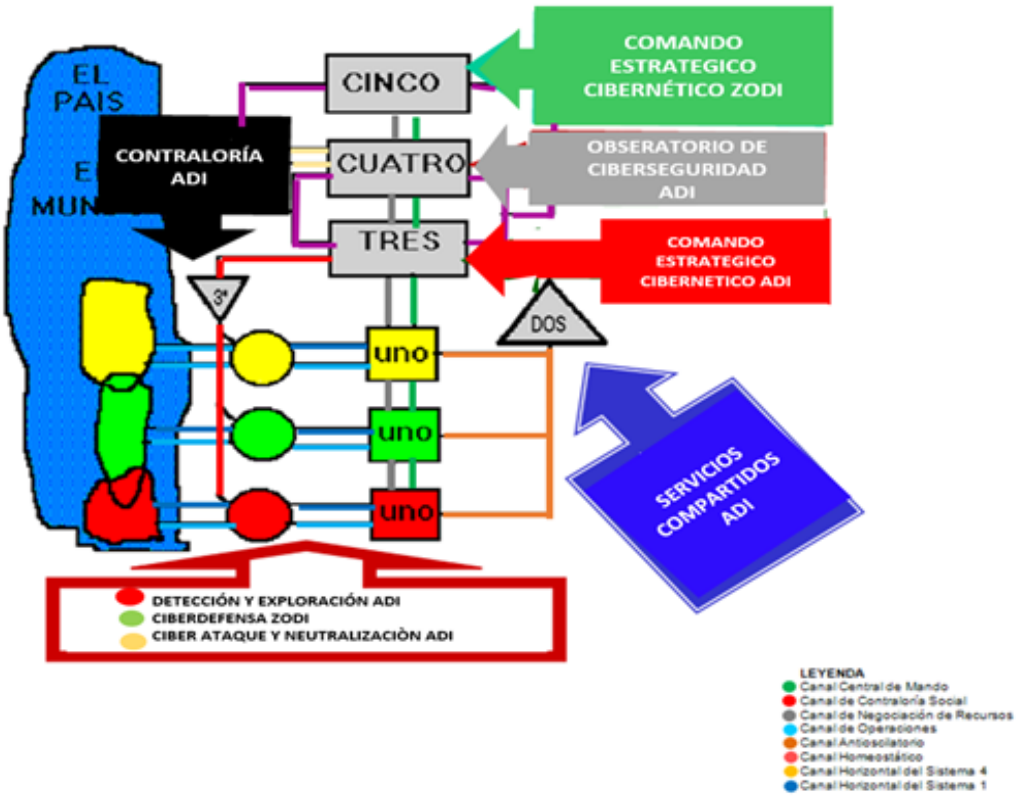
Figura Nro 6. Tercer Nivel de Recursión del Modelo de Organización Cibernética del Comando Cibernético Nacional para la República Bolivariana de Venezuela



Fuente: Elaboración propia de los autores, (2020).

Sistema 5: Representado por el Comando Estratégico Cibernético REDI.
Sistema 4: Representado por el Observatorio de Ciberseguridad de la ZODI.
Sistema 3: Representado por el Comando Estratégico Cibernético de la ZODI.
Sistema 2: Representado por las Gerencia de Servicios Compartidos de la ZODI.
Sistemas 1: Representado por las unidades operacionales básicas o procesos medulares del Comando Cibernético Nacional que están facultadas para llevar a cabo actividades relacionadas con la Exploración y Detección de amenazas, la Ciberdefensa, la Neutralización y Ciberataques en las Zonas de Defensa Integral (ZODI).

Figura Nro.7. Cuarto Nivel de Recursión del Modelo de Organización Cibernética del Comando Cibernético Nacional para la República Bolivariana de Venezuela



Fuente: Elaboración propia de los autores, (2020).

Sistema 5: Representado por el Comando Estratégico Cibernético ZODI.
Sistema 4: Representado por el Observatorio de Ciberseguridad de la ADI.
Sistema 3: Representado por el Comando Estratégico Cibernético de la ADI.
Sistema 2: Representado por las Gerencia de Servicios Compartidos de la ADI.
Sistemas 1: Representado por las unidades operacionales básicas o procesos medulares del Comando Cibernético Nacional que están facultadas para llevar a cabo actividades relacionadas con la Exploración y Detección de amenazas, la Ciberdefensa, la Neutralización y Ciberataques en las Área de Defensa Integral (ADI).

Estos últimos niveles de recursión, obtenidos al aplicar el Modelo de Sistemas Viables al caso del Comando Cibernético Nacional, nos indica que es posible imaginar una Organización Estratégica del Estado Venezolano, que en su nivel recursivo inferior, está compuesta por el conjunto de diversas Unidades de Organización Básica, que confluyen en un espacio territorial, para compartir recursos e información sobre ciberamenazas locales, lo que permitiría materializar a ese nivel recursivo la razón del Comando Cibernético Nacional que no es otra que la Neutralización y Ciberataques, Ciberdefensa, Exploración y De-

tección de amenaza en sus respectivas jurisdicciones territoriales y así alanzar objetivos estratégicos establecidos.

Esta particular concepción del Comando Cibernético Nacional, habrá de concretar su accionar logrando la sinergia con el resto de las Instituciones con las que el Estado Venezolano cuenta hoy para el abordaje de la problemática de la Ciberseguridad. En tal sentido la propuesta implica que en la práctica el modelo se concrete asumiendo la estructura matricial por procesos que se que muestra a continuación en el Gráfico N° 6:

Gráfico Nro. 6. Estructura Matricial del Comando Cibernético Nacional para la República Bolivariana de Venezuela.

Fuente: Elaboración propia de los autores, (2020).

Momento IV
A MANERA DE COLOFÓN

Conclusiones

Una primera conclusión a la que hemos arribado los autores, es que la infraestructura digital de la República Bolivariana de Venezuela, debe ser considerada como "un activo estratégico nacional". Esta afirmación proviene de los hallazgos hasta aquí reportados. que vienen a confirmar las proposiciones de Richard Clarke, quien prevé un fallo catastrófico (breakdown) que podría en un país en vías de desarrollo, ocasionar la caída de los sistemas de mensajería de video, voz y texto, así como los servicios de correo civil electrónico y con ello el colapso de los sistemas de telecomunicaciones, el sistema de suministro de energía eléctrica, los servicios de la banco comercial, los sistemas de pago electrónico, el control automático de refinerías y oleoductos, los sistemas de control de tráfico aéreo; los trenes de pasajeros y de carga así como y los metros de las principales ciudades; las órbitas de los satélites quedarán fuera de control. Y lo que es peor de todo, la identidad del atacante puede ser un misterio; con lo cual se ratifica la idea de que para el Comando Cibernético Nacional debe con un mandato claro "conducir las operaciones de amplio espectro para defender el ciberespacio de la República Bolivariana de Venezuela y estar preparado para atacar si fuera necesario a los sistemas e infraestructuras críticas de otros países". De allí que, el Comando Cibernético Nacional, nace esencialmente, de la necesidad de lograr la adaptación, regulación y control del ciberespacio de la República Bolivariana de Venezuela, ante la magnitud de las amenazas y la finitud de los talentos y recursos disponibles.

No obstante, dicho Comando Cibernético Nacional operará con efectividad si todos sus integrantes, sin ambigüedad, conocen su ubicación ante una amenaza específica, sus funciones y cómo se relacionan estas últimas con las de sus compañeros para lograr el objetivo o resultado.

En consecuencia, la estructura de la Organización propuesta del Comando Cibernético Nacional ha sido diseñada de manera que sea perfectamente claro para todos, quién es el ente rector con competencia en materia del Ciberespacio de la República Bolivariana de Venezuela, al que le corresponderá establecerá e implementar las políticas y estrategias para la protección del ciberespacio en el país.

Con esto, se aspira reducir y/o eliminar las dificultades que en el pasado, los ataques cibernéticos han ocasionado, como consecuencia de la imprecisión en la asignación de responsabilidades. Por ello, se aspira que su implementación tribute en el logro de una comunicación y toma de decisiones adecuada con los objetivos de la Seguridad de la Nación, toda vez que la estructura en un medio del que se sirve la Nación para conseguir sus objetivos con eficacia.

A partir de su creación y reconociendo la emergencia de nuevas amenazas a la Seguridad de la Nación, será posible avanzar en la formulación de su arquitectura estratégica, que permita el abordaje integrado de la problemática de la Ciberseguridad Nacional, desde tres (3) grandes dominios que marcaran su direccionalidad estratégica, a saber, el dominio de los "Propósitos", el de las "Capacidades" y el de las "Relaciones":

Gráfico Nro.7 . Comando Cibernético Nacional: Propósitos, Capacidades y Relaciones

Fuente: Elaboración propia de los autores, (2020).

El dominio de los "Propósitos" refleja los deseos y aspiraciones que en materia de Ciberseguridad, fueron plasmados por el Presidente Nicolás Maduro Moros, en el proceso permanente de reflexión estratégica que se suscitó con motivo de los ciberataques al Sistema Eléctrico Nacional y que marcan la ruta que desde la Asamblea Nacional Constituyente se le imprime en los actuales momento al debate del Anteproyecto de Ley Constitucional del Ciberespacio de la República Bolivariana de Venezuela, para saldar las heridas de la Guerra Cibernética a la que el país en su conjunto y con ella sus infraestructuras crítica ha estado sometido.

El dominio de las "Capacidades" agrupa los aspectos que determinan recursos existentes, de cualquier clase para poder avanzar hacia el logro de los "Propósitos". Aquí, se enfatizan tanto las estructuras, los procesos como las tecnologías presentes y requeridas por el Comando Cibernético Nacional, que determinan los modos de funcionamiento y criterios para la elección de cursos de acción.

Es por ello que este dominio indica "el que tan preparado se está para" y no simplemente los recursos materiales, financieros y tecnológicos disponibles para la ejecución con calidad del os procesos relacionadas con la Exploración y Detección de amenazas, la Ciberdefensa, la Neutralización y Ciberataques en sus respectivas jurisdicciones territoriales, de acuerdo a la división del territorio nacional para la garantía de la Seguridad y Defensa de la Nación. Vale decir en las Regiones de Defensa Integral (REDI), en las Zonas de Defensa Integral (ZODI) y

en las áreas de Defensa Integral (ADI). Adicionalmente se incluyen explícitamente lo relativo a las competencias presentes en la fuerza laboral, así como a los valores y creencias.

El dominio de las relaciones refiere a las formas de relacionamiento e interconexión de todos los actores internos y externos que determinan la existencia de antagonismos y conflictos que se resuelven a través de las relaciones de poder tanto con actores nacionales e internacionales, las cuales coadyuvan u obstaculizan la implementación exitosa del Comando Cibernético Nacional.

Al relacionar los dominios de "Propósitos, Capacidades y Relaciones" con el Modelo de Negocio y la Estructura Organizativa del Comando Cibernético Nacional, es posible avanzar hacia la concreción de la Propuesta de Valor aquí diseñada, que deberá desplegar el Comando Cibernético Nacional, para tributar con el logro de las aspiraciones plasmadas en el Plan de la Patria 2019-2025.

Recomendaciones

Haciendo nuestras las inquietudes de los especialistas en materia de Ciberseguridad consultados durante la realización de este trabajo de Investigación, a continuación, se presentan las siguientes de recomendaciones:

1.- Decretar la creación del Comando Cibernético Nacional.

2.- Ordenar una revisión inmediata de todas las defensas y vulnerabilidades cibernéticas de la República Bolivariana de Venezuela, con énfasis en la infraestructura crítica.

3.- Formular el Plan de desarrollo Institucional del Comando Cibernético Nacional.

4- Elaborar el Manual de Organización y Funcionamiento del Comando Cibernético Nacional.

5.- Diseñar un plan para la formación, capacitación y actualización permanente, en materia de Ciberdefensa, de personal civil y militar que estando hoy adscrito a los diferentes entes con competencia en la materia, pasarían a formar parte del Comando Cibernético Nacional.

6.- Fortalecer la infraestructura tecnológica de los entes con competencia en la materia, para garantizar la integridad, seguridad y disponibilidad de la información ante la presencia de ataques cibernéticos internos y externos.

7- Crear una fuerza de tarea especializada para combatir a lo interno y externo a los hackers.

8.- Promover por la vía del estímulo, la investigación e innovación, el desarrollo de capacidades defensivas y ofensivas necesarias para impedir ciberataques estatales en la República Bolivariana de Venezuela y, de ser necesario contar con las capacidades para responder apropiadamente.

REFERENCIAS BIBLIOGRÁFICAS

Alcalà, C. (2010). *Arquitectura Estratégica para para gerenciar la movilización Militar en caso de declararse estado de Excepción*. Universidad Nacional Experimental de la Fuerza Armada Nacional Bolivariana

Beer, S. (1971). *Cibernética y administración*. México: Conti-nental.

Beer, S. (1977). *Diseñando la libertad*. España: Fondo de Cultura Económica.

Beer, S. (1979). *The Heart of Enterprise*. Gran Bretaña: John Wiley & Sons.

Beer, S. (1981). *Brain of the Firm*. (2da ed). Gran Bretaña: John Wiley & Sons.

Beer, S. (1982). *Decisión y control: El Significado de la investigación de operaciones y administración cibernética*. Colombia: Fondo de Cultura Económica.

Beer, S. (1985). *Diagnosting The System for organizations*. Gran Bretaña: John Wiley & Sons.

Beer, S. (1996). The culpabliss error. [Transcripción en línea]. Disponible: http://www.staffordbeer.com/papers/Culpabliss.pdf. Traducción libre. [Consulta: 2010, abril 9].

Bernal, C. (2000). *Metodología de la investigación*. México: Prentice Hall.

Bertalanffy, L. (1976). *Teoría general de los sistemas. fundamento, desarrollo, aplicaciones*. España: Fondo de Cultura Económica.

Bertalanffy, L. (2000). *Teoría general de los sistemas*. (2da ed). Colombia: Fondo Cultural Económica.

Byrne, J. (1993). The futurists who fathered the ideas [Los futuritas que engendraron las ideas]. Business Week, 8 (febrero): 41.

Camarinha, L., Afsarmanesh, H. y Ollus, M. (2005) Virtual Organizations: systems and practices [Organizaciones virtuales: sistemas y prácticas]. New York, United States of America: Springer.

Camacho, H. y Padrón, J. (2000). ¿Qué es investigar? Una respuesta desde el enfoque epistemológico del racionalismo crítico. *En Telos. Revista de Estudios Interdisciplinarios* de la Universidad Rafael Belloso Chacín, (Vol. 2, Nº 2, pp. 314-330).

Castro, B. (2007). Análisis organizacional desde la teoría general de sistemas. Tesis Doctoral en Ciencias de la Educación, Universidad de la Serena, Chile.

Cibernética Organizacional Software [Sofware en línea]. Disponible: http://www.ciberneticaorganizacional.org/vsmod. [Consulta: 2011, marzo 11].

Centro Nacional de Ciberseguridad de los Países Bajos (2018). *Evaluación de la Ciberseguridad en los Países Bajos*.

Chean, Deng (2012). China's Evolving

Space Capabilities: Implications for U.S. Interests.

Chean, Deng (2016). Cyber Dragon: Inside China's Information Warfare and Cyber Operations (Praeger Security International). Edición Kindle

Chean, Deng (2018). China's Cyber Warfare: The Evolution of Strategic Doctrine. Edición Kindle

Córdova, V. y Zavarce, C. (2009). *Socialismo: Modos de vida y nuevas tecnologías de información*. Venezuela: Armada Bolivariana, Comando Naval de Educación, Escuela Superior de Guerra Naval.

Espejo, R. y Hernández, R. (1989). The viable system model: Interpretations and applications of Stafford Beer`s VSM. Gran Bretaña: John Wiley & Sons.

Etkin, J. y Schvarstein, L. (1989). La Identidad de las Organizaciones: Invariancia y Cambios. Buenos Aires, Argentina. Editorial Paidós.

Fayol, H. (1916). Principios y elementos de administración. Buenos Aires. El Ateneo, 1972.

Franje, U. (2002). Managing virtual web organizations in the 21st century: issues and challenges [Gerenciando organizaciones virtuales web en el siglo XXI: problemas y desafios]. London, England: Idea Group Publishing.

Jaramillo, L. (2000). *¿Qué es la epistemología?* [Artícu-lo en línea]. Disponible: http://www.biblioteca.ucn.edu.co/repositorio/Psicologia/ Epistemologia-dela-Psicologia/documentos/Que%20es%20Epistemologia.htm. [Consulta: 2010, enero11].

La Historia del Proyecto Cibersyn (2007). [Transcripción en línea]. Disponible: http://www.atinachile.cl/content/view/37449/La-Historia-del-Proyecto-Cybersyn-cuando-Chile-fue-pionero-de-las-redes-mundiales.html. [Consulta: 2010, marzo 24].

Leal, J. (2009). *Viabilidad del modelo cibernético gerencial para el Instituto Universitario Politécnico del Estado Trujillo*. Universidad Valle de Momboy, Valera, Venezuela.

Losada, R. y Casas, A. (2008). Enfoques para el análisis político. Historia, epistemología y perspectivas de la ciencia política. Bogotá: Pontificia Universidad Javeriana.

Luhmann, N. (1998). Sistemas Sociales: lineamientos para una teoría general (vol. 15). Barcelona: Anthropos-UIA-CEJA.

Mariña, M. (1985). *Gerencia y planificación cibernética*. Comisión de Estudios Administrativos de Postgrado, Facultad de Ciencias Económicas y Sociales, Universidad Central de Venezuela. Venezuela: Publicaciones.

Mariña, M. (1995). *Organización, complejidad y privatización*. Cuadernos de Postgrado 11. Temas de Fronteras en el Campo de la Gerencia. Compilador Carlos Zavarce. Comisión de Estudios de Postgrado, Facultad de Ciencias Económicas y Sociales, Universidad Central de Venezuela.: Tropykos.

Mariña, M. (2000). *Cibervenez*. Postgrado en Ciencias Administrativas. Universidad Central de Venezuela.

Mariña,M y Zavarce C. (2014) El Modelo de Sistema Viable para la Seguridad, Defensa y Desarrollo Integral de la Nación. Ediciones de Pdvsa Gas Comunal.

Maurer, T y Morgus, R:. (2014). Compilation of Existing Cybersecurity and Information Security Related Definitions, New America,. http://www.giplatform.org/sites/default/files/Compilation%20of%20Existing%20Cybersecurity%20and% 20Information%20Security% 20Related%20Definition.pdf consulta: 22 de Mayo de 2015.

Minztberg, H. (1988). Strategy Formation in an Adhocracy [La formación de la estrategia en una adhocracia]., Administrative Science Quarterly, v. 30(2), 160-197. Recuperado de: https://eric.ed.gov/?id=EJ323593.

Morin, E. (2007). *Introducción al pensamiento complejo*. España: Gedisa.

Mowshowitz, A. (1986). Social Dimensions of Office Automatisation [Dimensiones sociales de la automatización de oficinas]. En: Advances in Computers, 25. Jg., Nr. 1, 1986, p. 335-404.

Mowshowitz, A. (2002). Virtual Organization. Toward a theory of societal transformation stimulated by information technology [Organización Virtual. Hacia una teoría de transformación social estimulada por la tecnología de información]. Westport, United States of America: Quorum Books

Narvarte, P. (2002). *Bases teórico-metodológicas para el diagnostico y diseño de organizaciones*. [Transcripción en línea]. Disponible: http://www.comenius.usach.cl/.../DIAGNOSTICO%20Y%20DISEÑO%20ORGANIZACIONAL1.doc. [Consulta: 2010, marzo 21].

Padrón, J. (2007). *Tendencias epistemológicas de la investigación científica en el siglo XXI*. [Transcripción en línea]. Disponible: http://www.padron.entretemas.com. [Consulta: 2010, noviembre 20].

Palella, S. y Martins, F. (2006). Metodología de la investigación cuantitativa. (2a ed.) Caracas, Venezuela: FEDUPEL,

Pérez, O. (2011). *La cibernética organizacional en la regulación de las actividades espaciales venezolanas*. Tesis Doctorado en Ciencias Gerenciales, Universidad Nacional Experimental Politécnica de la Fuerza Armada Nacional, Caracas, Venezuela.

Pérez Ríos, J. (2005). *Aplicaciones de la cibernética organizacional al estudio de la viabilidad de las organizaciones*. Patologías Organizativas Frecuentes. Parte 1. [Transcripción en línea]. Disponible: http://www.herramientas.ateneagrupogid.org/guardados/Introduccion Cibernetica1de2.pdf. [Consulta: 2010, junio 25 y 2011, marzo 16].

Pérez Ríos, J. (2005). *Aplicaciones de la cibernética organizacional al estudio*

de la viabilidad de las organizaciones. Patologías Organizativas Frecuentes. Parte 2 y Final. [Transcripción en línea]. Disponible: http://www.herramientas.ateneagrupogid.org/guardados/IntroduccionCibernetica2de2(Patologias).pdf. [Consulta: 2010, junio 26, 2011, marzo 16 y 2011, abril 14].

Pérez Ríos, J. (2008). Vol. 83, nº 5: 265-281 DYNA, [Revista en línea] Disponible: http://www.herramientas.ateneagrupogid.org/guardados/ IntroduccionCibernetica1d. [Consulta: 2010, junio 28, 2011, abril 16 y 2011, abril 25].

Pérez Ríos, J. (2009). *Diseño y diagnóstico de organizaciones viables. Un enfoque sistémico"*. Iberfora 2000. E-Book. ISBN: 978-84-613-4861-9.

Popper, K. Racionalismo Crítico (s.f). [Transcripción en línea]. Disponible: http://www.gestiopolis.com/canales7/fin/racionalismo-critico-en-contabilidad-karl-popper.htm. [Consulta: 2010, marzo 16].

Puche, J., Pérez, J., Sánchez, P. (2006). *Aplicación de la cibernética organizacional mediante el MSMod al estudio de un proyecto software* [Transcripción en línea]. Disponible: http://www.adingor.es/ Documentacion/CIO/cio2006/docs/000116_final.pdf. [Consulta: 2010, junio 26 y 2011, abril 28].

Sabino, C. (2002). *El proceso de investigación*. Caracas, Venezuela: Panapo.

Sanchez Manuel (2018). Seguridad Corporativa: Nuevo Retos,Nuevas Exifgencias. España: Gedisa.

Sanchez Manuel (2016). Manual para el Director de seguridad. España: Gedisa.

Tamayo y Tamayo, M. (2001). *Proceso de la investigación científica*. (3ª ed). México: Limusa.

Ugas, G. (2006). *La complejidad: Un modo de pensar*. Táchira, Venezuela: Taller Permanente de Estudios Epistemológicos.

Universidad Nacional Experimental Simón Rodríguez (2007). *Proyecto Ciber Robinson*.

Universidad Nacional Experimental Simón Rodríguez (2007). *Proyecto Simón de los Pueblos*

Weber, M. (1947). The theory of social and economic organization [La teoría de la organización social y económica]. (T. Parsons, Trans). New York, NY: Oxford University Press.

World Economic Forum (2019). Global Riskc Lanscape

Zavarce, C. (1994). *Un modelo de organización cibernética para soportar la gerencia de pre-crisis*. Tesis Doctorado Ciencias Sociales Universidad Central de Venezuela, Caracas, Venezuela.

Zavarce, C. (1995). *Sistemas de información bajo enfoque cibernético*. Trabajo de Ascenso. Comisión de Estudios Administrativos de Postgrado, Facultad de Ciencias Económicas y

Sociales, Universidad Central de Venezuela. Venezuela: Publicaciones.

Zúñiga, F. (2010). *Modelo de sistema viable. Modo diagnóstico. Empresa Agrosuper*. Universidad Santiago de Chile. [Transcripción en línea]. Disponible: http://www.buenastareas.com/ensayos/Modelo-De-Sistema-Viable-Modo-Diagnostico/1300246.html. [Consulta: 2010, diciembre 20].

APÉNDICES

Apéndice 1: Glosario de Términos

Amenaza:

Es una causa potencial de un incidente no deseado, el cual puede resultar en daño a un sistema o a los activos de seguridad del Ciberespacio de la República Bolivariana de Venezuela.

Ciberespacio de la República Bolivariana de Venezuela:

Es el espacio global conformado por elementos tangibles e intangibles, que se generan durante el tiempo de interconexión, interrelación e interoperabilidad en infraestructuras Tecnológicas; redes, sistemas, equipos y usuarios, el cual permite el acceso, producción, transmisión y almacenaje de datos e información, e interacción a través de redes de información o comunicaciones, por cualquier dispositivo tecnológico, óptico, magnético entre otros; así como también cualquier forma de actividad que se realice en ellos que tengan efectos o repercusiones dentro o para la República Bolivariana de Venezuela.

Ciberdefensa:

Es el conjunto de acciones estratégicas, herramientas técnicas y legales, operaciones activas y/o pasivas desarrolladas por las Fuerzas Armadas Nacionales, en el ámbito de las a las infraestructuras tecnológicas, redes, sistemas, equipos, enlaces y usuarios de estos recursos a fin de asegurar el cumplimiento de los servicios para los que fueran concebidos, garantizando el libre acceso al ciberespacio de interés militar y permitir el desarrollo eficaz de las operaciones militares, tendentes a minimizar o neutralizar toda acción que genere o produzca riesgos, amenazas y agresiones a las infraestructuras críticas, la estabilidad económica, política y social que afecten la paz interna, la independencia, defensa, seguridad y soberanía, que tengan efectos o repercusiones dentro o para la República Bolivariana de Venezuela y el Ciberespacio venezolano.

Ciberseguridad:

Es el conjunto de acciones, herramientas, políticas, prácticas, tendentes a proteger los dispositivos tecnológicos, usuarios, servicios/aplicaciones, sistemas de comunicaciones, comunicaciones, y la totalidad de la información transmitida y/o almacenada que constituyen el ciberespacio.

Ciberterrorismo:

Ataques cometidos mediante la utilización de tecnologías de información y comunicación, con la finalidad de producir terror en la sociedad, desestabilización económica, política y social que afecten la paz interna.

Ciberterrorista:
Sujeto activo que ejecuta acciones terroristas mediante uso de tecnologías de información y comunicación.

Ciberguerra:
Conjunto de acciones desplegadas por motivos políticos, por uno o más Estados, mediante la utilización de tecnologías de información y comunicación para declarar y ejecutar acciones masivas en el ciberespacio contra Infraestructuras Críticas de otros Estados con la finalidad de producir terror en la sociedad, desestabilización económica, política y social que afecten la paz interna, la independencia, defensa, seguridad y soberanía de un gobierno y su población.

Cibercrimen:
Conducta típica antijurídica que emplea Tecnologías de Información y Comunicación como medio o como fin para la comisión de un hecho punible.

Cibercultura:
Conjunto de actividades que educan y sensibilizan a los usuarios en el buen uso del ciberespacio.

Ciberespionaje:
Obtención, o divulgación no autorizada de data o información privada o confidencial, contenida en un sistema que utilice tecnologías de información o comunicación o en sus componentes.

Dato:
Hechos, conceptos, instrucciones o caracteres representados de una manera apropiada para que sean comunicados, transmitidos o procesados por seres humanos o por medios automáticos, a los cuales se les asigna un significado.

Datos sensibles:
Son aquellos datos referidos a la intimidad de una persona que revelan origen racial, étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

Dispositivo tecnológico:
Cualquier elemento electrónico, óptico, magnético o de otra índole, bien sea físico, lógico o su combinación, utilizado directa o indirectamente por uno o más usuarios que permite ejecutar las siguientes acciones: entrada, procesamiento, salida, difusión de datos o información e interacción por cualquier medio.

Hardware:
Equipos o dispositivos físicos considerados en forma independiente de su capacidad o función, que conforman un computador o sus componentes periféricos, conexiones, componentes y partes.

Incidente de Seguridad:
Es todo aquel evento inesperados o no solicitados, que comprometa la operación de la gestión amenace la Seguridad de Información, atente contra la confidencialidad, disponibilidad, integridad o la normal operación, que constituya una amenaza para quebrantar los mecanismos de seguridad.

Infraestructura crítica:
Es aquella Infraestructura Tecnológica cuyo funcionamiento es indispensable y no permite soluciones alternativas, están conformadas por las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales de la Nación, empleada en el desarrollo de sectores protegidos en virtud de su repercusión en los ámbitos de Seguridad y Defensa, Salud, Banca, Finanzas, Energía, Petróleo, Comunicaciones, Telefonía y cualquier otra infraestructura tecnológica que cumpla funciones de interés, cuya afectación pueda perjudicar gravemente el orden interno, económico, desarrollo estratégico, soberanía y seguridad, independientemente de la naturaleza pública o privada del órgano responsable de su gestión.

Infraestructura tecnológica:
Conjunto de medios tecnológicos y sistemas en los cuales se soportan las bases para brindar servicios.

Información:
Conjunto de datos agrupados que representa algo significativo para el usuario.

Informática Forense:
Es una rama auxiliar de la ciencia forense la cual mediante la aplicación de técnicas científicas y analíticas especializadas permite identificar, preservar, analizar y presentar evidencias digitales que sean válidos dentro de un proceso legal.

Internet:
Sistema global de redes interconectadas en el dominio público.

Medios Tecnológicos:
Cualquier componente de software, hardware, instalaciones, dispositivos tecnológicos, redes de comunicaciones y demás elementos de las Tecnologías de Información y Comunicación.

Proveedores de Servicios de Difusión de Mensajes:
Entidad pública o privada que mediante tecnologías de información y comunicación prestan servicios para la difusión de mensajes.

Proveedores de Servicios de Internet:
Entidad pública o privada que utilizan tecnologías para brindar un servicio de conexión de Internet a sus usuarios.

Proveedores de Servicios de Tecnología de Comunicación e Información:

Entidad pública o privada que ofrezca a los usuarios servicios tecnologías de información y comunicación.

Redes de comunicaciones:

Constituye un medio para la conexión entre dos o más dispositivos tecnológicos para intercambio de datos e información.

Servicios de Tecnología de Comunicación e Información:

Serie de funcionalidades ofrecidas por un proveedor para satisfacer las necesidades de los usuarios en el ámbito de las TIC, como servicios de telefonía móvil, fija, Internet, radio, televisión, correo electrónico, entre otros.

Software:

Información organizada en forma de programas, procedimientos y documentación asociados, para realizar la operación de un sistema.

Software Malicioso (Malware):

Software con características o capacidades para amenazar o causar daño directa o indirectamente a infraestructura tecnológica.

Tratamiento de datos:

Operaciones sistemáticas, efectuadas mediante procedimientos manuales o automatizados aplicados a los datos, que permitan la recolección, conservación, ordenación,' almacenamiento, modificación, relacionamiento, evaluación, bloqueo,-destrucción, posesión, acceso, manejo y en general el procesamiento de datos, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

Tecnología de Información:

Rama de la tecnología que se dedica al estudio aplicación y procesamiento de datos.

Usuario:

Persona que se conecta directa o indirectamente a una red de comunicaciones utilizando uno o más dispositivos tecnológicos para hacer una determinada operación o acción.

APÉNDICE 2

Guión de entrevista a los informantes clave en el área de organización

1. ¿Cómo explica la teoría sobre la Organización su comportamiento y validez en la sociedad contemporánea?

2. ¿Qué elementos sustantivos caracterizan la teoría sobre la organización?

3. ¿Qué teorías (inventario) sobre la Organización incorporan propósitos, capacidades y relaciones como factores de éxito claramente definidos?

4. ¿Cuáles son los arquetipos de las organizaciones que marcan el debate contemporáneo?

5. ¿Qué desafíos afrontan las teorías actuales sobre la organización?

6. ¿Cuáles son los factores críticos de éxito de una organización?

APÉNDICE 3

Entrevista focalizada a los informantes clave expertos en el área de rganización

ENTREVISTA 1
(Idioma original inglés)

1. How does the theory about organization explain its behavior and validity in contemporary society?

According to my "theory of change" of the organization, one would expect companies to change providers more frequently than in the past, make greater use of outsourced workers and exhibit less loyalty to the flag and the country, and This behavior is demonstrable.

2. What substantive elements characterize the theory about organization?

You are familiar with my model, so I will not repeat the arrests here. Just keep in mind that the most common features such as "organizations without walls", "greater dependence on advanced information and transportation technologies", etc. they are consequences, instead of defining characteristics, of the fundamental changes in the organization.

3. What theories about the Organization incorporate purposes, capacities and relationships as clearly defined success factors?

Again, the purposes, capabilities and relationships are inherent in my "theory of commutation", since the theory presupposes clearly defined objectives in the change from one satisfactory to another.

4. What are the archetypes of organizations that mark the contemporary debate?

The first companies to exhibit the characteristics of the diferent organization were the large multinationals of the 1970s. These companies still have many activities organized virtually, but the field has been expanded by Internet-based marketing opportunities. Now, most Internet-based businesses function as virtual organizations.

5. What challenges do current theories about organization face?

An important challenge is to explain the connection between virtual organization and increase fragmentation and mistrust in the world of politics.

6. What are the critical success factors of a l organization?

As for any organization, companies aim to make profits, governments aim to achieve effective social control. The virtual organization offers new tools to achieve these objectives.

ENTREVISTA 1
(Traducido al español)

1. ¿Cómo explica la teoría sobre la Organización su comportamiento y validez en la sociedad contemporánea?

De acuerdo con mi "teoría de cambio" de la organización, no esperaría que las empresas cambien de proveedor con mayor frecuencia que en el pasado, hagan un mayor uso de los trabajadores subcontratados y exhiban menos lealtad a la bandera y el país, y este comportamiento es demostrable.

2. ¿Qué elementos sustantivos caracterizan la teoría sobre la organización?

Usted está familiarizado con mi modelo, así que no repetiré las detenciones aquí. Solo tenga en cuenta que las características más comunes como "organizaciones sin paredes", "mayor dependencia de tecnologías avanzadas de información y transporte", etc. son consecuencias, en lugar de definir características, de los cambios fundamentales en la organización.

3. ¿Qué teorías (inventario) sobre la Organización incorporan propósitos, capacidades y relaciones como factores de éxito claramente definidos?

Una vez más, los propósitos, las capacidades y las relaciones son inherentes a mi "teoría de la conmutación", ya que la teoría presupone objetivos claramente definidos en el cambio de uno satisfactorio para otro.

4. ¿Cuáles son los arquetipos de las organizaciones que marcan el debate contemporáneo?

Las primeras compañías en exhibir las características de la organización virtual fueron las grandes multinacionales de la década de 1970. Estas empresas todavía tienen muchas actividades organizadas virtualmente, pero el campo se ha ampliado por las oportunidades del marketing basado en Internet. Ahora, la mayoría de las empresas basadas en Internet funcionan como organizaciones virtuales.

5. ¿Qué desafíos afrontan las teorías actuales sobre la organización?

Un desafío importante es explicar la conexión entre la organización y aumentar la fragmentación y la desconfianza en el mundo de la política.

6. ¿Cuáles son los factores críticos de éxito de una organización?

Igual que para cualquier organización, las empresas apuntan a obtener ganancias, los gobiernos apuntan a lograr un control social efectivo. La organización virtual ofrece nuevas herramientas para lograr estos objetivos.

ENTREVISTA 2
(Idioma original inglés)

1. How does the theory about organization explain its behavior and validity in contemporary society?

The emergence of the Cibernetics Enterprise / Virtual Organization paradigm is within the natural sequence of restructuring processes in the traditional industrial approaches dependent on the data supply chain associated with an economy of platforms, which are enabled by the advances of the information and communication technologies. Parallel to the trend towards subcontracting, the transformation observed in large companies is their organization as a federation of relatively autonomous departments that lead to transformations that place emphasis on networking and partnership-cooperation and that have aroused great interest in new disciplines such as the theory of coordination, the theory of organization and the sociology of industrial organizations, bringing as an unavoidable consequence, the "reinvention of the work force".

2. What substantive elements characterize the theory about organization?

In my opinion, the substantive element that characterizes the theory about now organization is the process of System Integration. For example, consider the context of companies where systems integration can be addressed and instantiated at different levels of complexity and abstraction; that is, from a "cellular" level (level of basic resources, to inter and intra-enterprise levels). In addition, there is the challenge of the need for a new level of integration, which emphasizes the roles and opportunities for network collaboration environments. The inclusion of processing capabilities is that many components extend across all living environments, both in the professional environment and at home, leading to the idea of widespread or ubiquitous computing. Work methods change, which makes it possible to carry out professional activities from different places obtaining a true "results economy". The paradigm of the Virtual Organization and the most generic collaboration networks appear then in this sequence of "systems integration", which addresses the more complete scope of integration of autonomous, heterogeneous and distributed entities (associated with the revolution of the platforms) .

3. What theories (inventory) about the Organization incorporate purposes, capacities and relationships as clearly defined success factors?

Each partner organization focuses its purpose on its core competency and uses the resources of other companies for other tasks, usually based on a long-term relationship. According to this vision, operations are more efficient both in proportion to costs and time, and to contribute to the accumulation of knowledge. Other clearly defined commercial reasons are for example: customer orientation, flexibility, agility and risk reduction. The term "reproduction environment" used for the network expresses the idea of creating an environment, where organizations can develop, acquire knowledge and potentially grow in cooperation.

However, the purposes of the companies participating in an alliance are not identical; There are always multiple objectives, some of which may be contradictory and this is the case within an organization, where the objectives of different sectors or departments may be different. In addition, the short- and long-term objectives can be conflicting. Although in an ideal network or Virtual Organization, the objectives of the partners are aligned with each other, in practice the situation is rarely so simple. Normally, the vision of a Virtual Organization manager is different from the vision of a partner. Although all partners are affected in part for the same purposes, the importance of them is not the same for each organization. One reason may be that an organization participates simultaneously in several alliances.

4. What are the archetypes of organizations that mark the contemporary debate?

The Cibernetics Organizationo or Virtual Organization can be considered as a system for delivering solutions for the client temporarily enabled by a complex information and communication technology and subject to constant reconfiguration of its core competencies thanks to the complex dynamics of its structure associated with automated processes.

5. What challenges do current theories about organization face?

Virtual Organizations are a response to the strictest requirements of profitability, time and quality, especially in a global environment. In addition, collaboration within the Virtual Organizations contributes to flexibility, agility, customer orientation and risk reduction. However, these goals are not achieved automatically. The management of independent organizations for individual purposes, sometimes even contradictory, is a difficult task that contains a certain degree of uncertainty. The inter-organizational distribution of processes and activities can lead to high coordination costs, delays in deliveries, quality problems, information leaks and loss of knowledge. To prevent problems, proactive management of this type of organization is needed.

On the other hand, the management of information and its integration in the phases of the product life cycle has received a lot of attention during the last years. Standardization and other initiatives have been initiated to solve related problems. The information adds a substantial value to the physical product. In the Virtual Organization environment, the management of this information becomes even more challenging and complex when the steps of the life cycle involve interoperability among the cooperating organizations.

6. What are the critical success factors of a organization?

The critical success factors of the Organization can be postulated as a shared purpose, a relationship of trust, the willingness to share the risk and a mutual benefit that is derived from the existence of the Virtual Organization. Therefore, a successful Virtual Organization is based largely on the idea that mutual benefit for the parties involved is derived through timely and appropriate initiation and the formation of partnerships to take advantage of potentially ephemeral business opportunities. But for alliances to work effectively and provide benefits to all stakeholders, the management activity must achieve the required level of shared vision and purpose, a high degree of trust among the members and an acceptance and understanding that the risk should be shared among those who are to benefit.

ENTREVISTA 2
(Traducido al español)

1. ¿Cómo explica la teoría sobre la Organización su comportamiento y validez en la sociedad contemporánea?

La aparición del paradigma de Empresa Cibernetical/Organización Virtual se encuentra dentro de la secuencia natural de los procesos de reestructuración en los enfoques industriales tradicionales dependientes de la cadena de suministros de datos asociados a una economía de plataformas, que son habilitados por los avances de las tecnologías de información y comunicaciones. Paralelamente a la tendencia hacia la subcontratación, la transformación observada en las grandes empresas es su organización como una federación de departamentos relativamente autónomos que conllevan a transformaciones que ponen énfasis en la creación de redes y la asociación-cooperación y que han despertado un gran interés por nuevas disciplinas como la teoría de la coordinación, la teoría de la organización y la sociología de las organizaciones industriales trayendo como consecuencia ineludible, la "reinvención de la fuerza de trabajo".

2. ¿Qué elementos sustantivos caracterizan la teoría sobre la organización?

A mi juicio, el elemento sustantivo que caracteriza la teoría sobre la organización es el proceso de Integración de Sistemas. Por ejemplo, considere el contexto de las empresas donde la integración de sistemas se puede abordar e instanciar en diferentes niveles de complejidad y abstracción; es decir, desde un nivel "celular" (nivel de recursos básicos, hasta niveles inter e intra empresarial). Además, existe el desafío de la necesidad de un nuevo nivel de integración, que enfatice los roles y oportunidades para los entornos de colaboración en red. La inclusión de capacidades de procesamiento consiste en que muchos componentes se extienden por todos los entornos de vida, tanto en el entorno profesional como en el hogar, lo que lleva a la idea de la computación generalizada o ubicua. Los métodos de trabajo cambian, lo que hace posible realizar actividades profesionales desde diferentes lugares obteniendo una verdadera "economía de resultados". El paradigma de la Organización Virtual y las redes de colaboración más genéricas, aparecen entonces en esta secuencia de "integración de sistemas", que aborda el alcance más completo de integración de entidades autónomas, heterogéneas y distribuidas (asociado a la revolución de las plataformas).

3. ¿Qué teorías (inventario) sobre la Organización incorporan propósitos, capacidades y relaciones como factores de éxito claramente definidos?

Cada organización aliada enfoca su propósito en su competencia central y utiliza los recursos de otras empresas para otras tareas, generalmente basadas en una relación a largo plazo. Según esta visión, las operaciones son más eficientes tanto en proporción a los costos y el tiempo, como para contribuir a la acumulación de conocimiento. Otros motivos comerciales claramente definidos son por ejemplo:

orientación al cliente, flexibilidad, agilidad y disminución de riesgos. El término "entorno de reproducción" utilizado para la red expresa la idea de crear un entorno, donde las organizaciones puedan desarrollar, adquirir conocimiento y potencialmente crecer en una cooperación.

Sin embargo, los propósitos de las empresas que participan en una alianza no son idénticos; siempre hay múltiples objetivos, algunos de los cuales pueden ser contradictorios y este es el caso dentro de una organización, donde los objetivos de diferentes sectores o departamentos pueden ser diferentes. Además, los objetivos a corto y largo plazo pueden ser conflictivos. Aunque en una red u Organización Virtual ideal, los objetivos de los socios están alineados entre sí, en la práctica la situación rara vez es tan simple. Normalmente, la visión de un gerente de la Organización Virtual es diferente a la visión de un socio. Aunque todos los socios se ven afectados en parte por los mismos propósitos, la importancia de ellos no es la misma para cada organización. Una razón puede ser que una organización participa simultáneamente en varias alianzas.

4. ¿Cuáles son los arquetipos de las organizaciones que marcan el debate contemporáneo?

La Organización Virtual se puede considerar como un sistema de entrega de soluciones para el cliente habilitado temporalmente por una compleja tecnología de información y comunicaciones y sujeto a constantes reconfiguraciones de sus competencias centrales gracias a la compleja dinámica de su estructura asociados a procesos automatizados.

5. ¿Qué desafíos enfrentan las teorías actuales sobre la organización?

Las Organizaciones son una respuesta a los requisitos más estrictos de rentabilidad, tiempo y calidad, especialmente en un entorno global. Además, la colaboración dentro de las Organizaciones Virtuales contribuye a la flexibilidad, agilidad, orientación al cliente y disminución de los riesgos. Sin embargo, estos objetivos no se logran automáticamente. La gestión de organizaciones independientes con propósitos individuales, a veces incluso contradictorios, es una tarea difícil que contiene cierto grado de incertidumbre.

La distribución interorganizativa de procesos y actividades puede llevar a altos costos de coordinación, retrasos en las entregas, problemas de calidad, fugas de información y pérdida de conocimiento. Para prevenir los problemas, se necesita una gerencia proactiva de este tipo de organización.

Por otro lado, la gestión de la información y su integración en las fases del ciclo de vida del producto ha recibido mucha atención durante los últimos años. Se han iniciado la estandarización y otras iniciativas para resolver problemas relacionados. La información agrega un valor sustancial al producto físico. En el entorno de la Organización Virtual, la gerencia de esta información se vuelve aún más desafiante

y compleja cuando los pasos del ciclo de vida implican la interoperabilidad entre las organizaciones que cooperan.

6. ¿Cuáles son los factores críticos de éxito de una organización l?

Los factores críticos de éxito de la Organización pueden ser postulados como un propósito compartido, una relación de confianza, la disposición a compartir el riesgo y un beneficio mutuo que se deriva de la existencia de la Organización Virtual. Por lo tanto, una Organización Virtual exitosa se basa en gran medida en la idea de que el beneficio mutuo para las partes involucradas se deriva a través del inicio oportuno y apropiado y la formación de alianzas para aprovechar las oportunidades comerciales posiblemente efímeras. Pero para que las alianzas funcionen de manera eficaz y brinden beneficios a todos los interesados, la actividad de gestión debe alcanzar el nivel requerido de visión y propósito compartidos, un alto grado de confianza entre los miembros y una aceptación y comprensión de que el riesgo debe ser compartido entre quienes están para beneficiarse.

ENTREVISTA 3
(Idioma original inglés)

1. How does the theory about organization explain its behavior and validity in contemporary society?

It could be said that in the developed world, most of the successful companies have been "virtualized", very few traditionally hierarchical and vertical organizations have prevailed. So complete has this transformation been that few people today think about it. However, when companies use websites to sell their products and services, they recruit customers to help them create the products they buy, reduce management layers by replacing them with data management, allowing workers to work at home, etc. they behave like Virtual Corporations. The dominant companies of our time, Apple, Facebook, Google, Amazon, were designed to be virtual from the start.

2. What substantive elements characterize the theory about organization?

Fundamentally, we realized that computer and network technologies had reached the point where they could replace administrative and operational functions at key levels in the traditional organizational model. In particular, the information no longer had to increase and the decisions are no longer reduced, the intermediate administration of several levels. In contrast, with technology, decisions could be made much faster and closer to the problem. This flattened the organization, empowered the employees and greatly accelerated the decision cycle.

Secondly, we realized that, also thanks to computers and networks, it was now possible to realize the dream of "mass customization", that is, not to force customers to buy standardized products, but to modify those products specifically to them. And those companies that adopted this model first would quickly dominate their industries, which is exactly what happened.

3. What theories about the Organization incorporate purposes, capacities and relationships as clearly defined success factors?

My theory includes:

a. Maximize communications with suppliers, employees and customers.

b. The ability to change direction or scale quickly, usually through the use of strategic partners, technology and loyal customers.

c. Make the employee feel part of the organization through the ability to respond to their needs, providing design tools, social networks, enlist them in the creation, manufacture and service of products.

d. Implement the latest digital technologies.

e. Virtualize where you can, that is, do everything digital you can at any time.

4. What are the archetypes of organizations that mark the contemporary debate?

The biggest question facing modern companies is: who owns information? How should non-employees be treated in terms of privacy, ownership of their data, con-

tributions to the company's product, etc.? Free software, which seemed like a good idea at that time, has become dangerous in terms of turning users into products that can be sold to third parties.

5. What challenges do current theories about organization face?

Looking back, my biggest mistakes we made were these:

a. We do not anticipate the Internet (in particular, the Web). My book was based on the advances that took place in computers and networks. Being in Silicon Valley, he obviously knew about the Internet, but he could not predict how fast he would take over the world. Therefore, although it seems that the virtual revolution would take 20 years, in fact it only took around 3 years.

b. I did not explain certain aspects of human nature. If you take virtualization to its logical conclusion, companies basically send everyone home and evaporate into smart, fully networked organizations. But it turns out that people need to interact physically and feel part of something real to build trust. Therefore, I generated the theory of the Protean Organization, with a traditional nucleus of a few long-term employees, surrounded by a cloud of part-time workers, contractors, etc. In other words, a small core of a fixed company surrounded by many, more employees less attached.

ENTREVISTA 3

(Traducido al español)

1. ¿Cómo explica la teoría sobre la Organización su comportamiento y validez en la sociedad contemporánea?

Se podría decir que en el mundo desarrollado, la mayoría de las empresas exitosas han sido "virtualizadas", muy pocas organizaciones tradicionalmente jerárquicas y verticales han prevalecido. Tan completa ha sido esta transformación que pocas personas hoy en día piensan en ello. Sin embargo, cuando las empresas usan sitios web para vender sus productos y servicios, reclutan clientes para ayudarlos a crear los productos que compran, reducen las capas de administración reemplazándolas con administración de datos, permitiendo que los trabajadores trabajen en casa, etc., se comportan como Corporaciones Virtuales. Las compañías dominantes de nuestro tiempo, Apple, Facebook, Google, Amazon, fueron diseñadas para ser virtuales desde el principio.

2. ¿Qué elementos sustantivos caracterizan la teoría sobre la organización?

Fundamentalmente, nos dimos cuenta de que las tecnologías de computación y redes habían llegado al punto en que podían reemplazar las funciones administrativas y operativas en niveles clave en el modelo organizacional tradicional. En particular, la información ya no tenía que aumentar y las decisiones ya no se reducen, la administración intermedia de varios niveles. En cambio, con la tecnología, las decisiones podrían tomarse MUCHO más rápido y de manera más cercana al problema. Esto aplanó la organización, empoderó a los empleados y aceleró enormemente el ciclo de decisión.

En segundo lugar, nos dimos cuenta de que, también gracias a las computadoras y las redes, ahora era posible realizar el sueño de "personalización masiva", es decir, no obligar a los clientes a comprar productos estandarizados, sino modificar esos productos específicamente para ellos. Y esas empresas que adoptaron este modelo primero dominarían rápidamente sus industrias, que es exactamente lo que sucedió.

3. ¿Qué teorías (inventario) sobre la Organización incorporan propósitos, capacidades y relaciones como factores de éxito claramente definidos?

a. Maximice las comunicaciones con proveedores, empleados y clientes.

b . Capacidad de cambiar de dirección o escalar rápidamente, generalmente a través del uso de socios estratégicos, tecnología y clientes leales.

c. Hacer que el empleado se sienta parte de la organización a través de la capacidad de respuesta a sus necesidades, proporcionándoles herramientas de diseño, redes sociales, alistarlos en la creación, fabricación y servicio de productos.

d.Implementar las últimas tecnologías digitales.

e. Virtualizar donde pueda, es decir, haga todo lo digital que pueda en cualquier momento.

4. ¿Cuáles son los arquetipos de las organizaciones que marcan el debate contemporáneo?

La mayor pregunta que enfrentan las empresas modernas es: ¿quién posee información? ¿Cómo se debe tratar a los no empleados en términos de privacidad, propiedad de sus datos, contribuciones al producto de la compañía, etc.? Software libre, que parecía una buena idea en ese momento, se ha vuelto peligroso en términos de convertir a los usuarios en productos que pueden venderse a terceros.

5. ¿Qué desafíos enfrentan las teorías actuales sobre la organización l?

Mirando hacia atrás, mis mayores errores cometimos fueron estos:

a. No anticipamos Internet (en particular, la Web). Mi libro se basó en los avances que tuvieron lugar en computadoras y redes. Al estar en Silicon Valley, obviamente sabía de Internet, pero no podía predecir qué tan rápido se apoderaría del mundo. Por lo tanto, aunque parece que la revolución virtual demoraría 20 años, de hecho solo tomó alrededor de 3 años.

b. No expliqué ciertos aspectos de la naturaleza humana. Si lleva la virtualización a su conclusión lógica, las empresas básicamente envían a todos a casa y se evaporan en organizaciones inteligentes totalmente conectadas en red. Pero resulta que las personas necesitan interactuar físicamente y sentirse parte de algo real para generar confianza. Por lo tanto, generé la teoría de la Organización Protean, con un núcleo tradicional de unos pocos empleados a largo plazo, rodeado de una nube de trabajadores a tiempo parcial, contratistas, etc. En otras palabras, un pequeño núcleo de una empresa fija rodeada de muchos, más empleados menos apegados.

6. ¿Cuáles son los factores críticos de éxito de una organización?

a. Disposición para cambiar los productos, el modelo comercial, los clientes y los proveedores, tan rápido como lo demande el mercado, y no se apegue al status quo.

b. Reconocimiento de que cualquier proceso comercial que pueda hacer digital pone esa operación bajo la Ley de Moore (La ley de Moore expresa que aproximadamente cada dos años se duplica el número de transistores en un microprocesador) y le permitirá acelerar más allá de la competencia.

c. Permita que los clientes definan el producto final que les entrega, no forzándolos a aceptar su versión.

d. Prepare a sus empleados para un cambio continuo y rápido.

e. Digitalice cada función comercial y cada nivel de supervisión tan rápido como pueda.

Mantente al tanto de la innovación tecnológica, no solo en tu campo, sino también en otros. La nueva invención que amenazará la existencia de su empresa es tan probable que provenga de otra industria como de la suya. Mire la enorme industria de impresión establecida, y cómo fue destruida casi de la noche a la mañana por la autoedición en computadoras personales. Las impresoras nunca lo vieron venir, porque no estaban mirando allí.

APÉNDICE 4

Guión de entrevista a informantes clave en ciberseguridad

1. ¿Qué opinión le merece el tema de la Ciberseguridad hoy día?

2. ¿Cuáles son las mayores amenazas de seguridad cibernética de hoy, y qué deberían estar haciendo las organizaciones vinculadas con el Estado para reaccionar ante ellas?

3. ¿Existen estrategias universales que hayan demostrado ser particularmente eficaces para la seguridad cibernética, o es más importante ser flexibles y adaptarse conforme las amenazas evolucionan?

4. ¿Qué papel desempeñan los profesionales de nivel gerencial en la ciberseguridad?

5. ¿Cómo las regulaciones en materia de Seguridad se acercan a la ciberseguridad?

6. ¿Cuál ha de ser la misión de un Comando Cibernético Nacional? Vale decir, sus propósitos y las actividades que la hacen viable.

7. ¿Qué actividades reguladoras deben estar al servicio de las actividades tecnológicas de las que dependerá la viabilidad de un Comando Cibernético Nacional?

8. ¿De quién dependerá la Resolución de Conflictos y el logro de la estabilidad organizacional de un Comando Cibernético Nacional?

9. ¿Cómo se lograría la sinergia entre los organismos y empresas del sector público y privado con competencias en materia de ciberseguridad en una Nación?

10. ¿De qué manera un Comando Cibernético Nacional buscará y detectará amenazas/oportunidades provenientes del exterior?

11. ¿Cómo producir la planificación que asegure la viabilidad de largo plazo? ¿Quién estará a cargo de la Adaptación y la anticipación?

12. ¿Quién proporcionará las directrices de la organización y cuál será el medio para hacerlas cumplir? ¿Quién asumirá la Autoridad Última, diseñará la política y garantizará identidad organizacional?

APÉNDICE 5

Entrevista focalizada a los expertos clave en el área de ciberseguridad

ENTREVISTA ESPECIALISTA 1

(Idioma original inglés)

1. What is your opinion on cybersecurity today?

The turn of the century was accompanied by two historically significant phenomena. One was the emergence of computer networks as a vital component of advanced militaries and interdependent global economic systems. The second concerned China's rise on the global stage through economic reforms that led to sustained growth and military modernization. At the same time, Chinese government policies and actions have drawn international criticisms including persistent allegations of online espionage, domestic Internet censorship, and an increased military capability, all of which utilize computer networks. These threat perceptions are heightened by a lack of transparency. Unlike the United States or the North Atlantic Treaty Organization, China does not articulate its strategic doctrine. Further, open source material on this topic is often contradictory, cursory, and unclear due, in part, to the absence of consensus on cyber-related terminology and the infancy of this field.

2. ¿What are today's biggest cybersecurity threats, and what should state-related organizations be doing to react to them?

The People's Republic of China (PRC) has made significant progress in its cybersecurity program and is emerging as a power in cyberspace. By preserving its monopoly on power as a primary objective, the Chinese Communist Party (CPC) strengthens its legitimacy through achievements in cyberspace. The Chinese military manages China's cyberspace program, and there is a significant overlap between mutually reinforcing civilian and military cybernetic operations. An increasingly sophisticated industrial and R&D facility supplies the People's Liberation Army (EP) with military cybernetic systems. The PLA General Armaments Department (GAD) appears to oversee the acquisitions and operations of cyber systems. Other major organizations in the cyber program include Chinese Cybernetics Science and Technology Corporation (CASC) and China Cibernetics Science and Industry Corporation (CASIC). As a rough counterpart of the NSA, China's National Cybernetic Administration (CNSA) facilitates international exchanges and cooperation programs with other nations affecting cyberspace

3. ¿What should be the mission of a National Cyber Commando? That is, its purposes and the activities that make it viable.

The democratization of ICTs also means that potential adversaries can have unprecedented access to the national economy of other states, as well as to their

national citizens and leaders, extending threats beyond the boundaries of networks – such as attacks on social media – and computational components – such as malware – and making information a threat in itself.

Therefore the mission of a Cyber Command should be to use technology to gather intelligence on the battlefield, coordinate joint operations of different military resources and assist in the selection of its objectives, but also, its use to influence public opinion in certain countries, conduct espionage activities and access the military and civilian cyber-infrastructures of what it considers its adversaries.

6. ¿What regulatory activities should be at the service of technological activities on which the feasibility of a National Cyber Command will depend?

In the Information Age, information is the vital resource that empowers all those spheres of power.

At the same time, however, the free flow of information constitutes a direct and very serious threat. For example, in the case of China, it has placed the 'Great Firewall Of China' and deployed a number of censors in the order of hundreds of thousands, in order to limit the information threat against the regime.

But all of this is insufficient to put Beijing's concerns aside. Ideally, a government must control and influence the entire flow of information inwards, which involves shaping the international structures that manage that flow of information.

So on whose conflict resolution will depend and achieving stability in the face of the Cyber Threats facing China as a Nation State?

After land, sea, air and outer space, many people have called cyberspace the fifth domain for human activities, with multiple implications for a state. Simply put, a state's political, economic and security interests are now increasingly connected to cybersecurity. However, the Internet is a double-edged weapon, i.e. it offers not only enormous benefits, but also numerous risks, challenges and threats. Therefore, given the borderless, transnational and unique nature of cyberspace, it has become a new frontier for global governance. China attaches great importance to the development of the Internet and has made tremendous progress in this regard. However, as a newcomer to this field, China faces several challenges and has been one of the main victims of cyberattacks. Looking to the future, China is ready to fight for peaceful, safe, open and cooperative cyberspace alongside the international community. At the international level, there are many doubts about China's policies and practices in its Internet development due to misunderstandings, prejudices, lack of knowledge. , and even ignorance on one side. On the other hand, there is a growing demand to understand China's policies and practices in this domain.

5.¿How will a National Cyber Command search for and detect threats/opportunities from abroad?

Cyberdefense has become, in the last five years, an important issue on the international stage. A Cyber Command, by the place it occupies, is the subject of attention: it is observed, criticized and designated by many states as an important player in national cybersecurity, building its cyber defense strategy against what is called the "cybercyber threat." It is therefore important to better understand the current cyber-dimension challenges in relation to the rise of conflicts. The contributions of international researchers provide cross-insight into these, their strategies and policies for cybersecurity and cyberdefense. These issues have now gained a great strategic dimensión.

ENTREVISTA ESPECIALISTA 1

(Traducido al español)

1. ¿Qué opinión le merece el tema de la Ciberseguridad hoy día?

El cambio de siglo estuvo acompañado por dos fenómenos históricamente significativos. Uno de ellos fue el surgimiento de las redes informáticas como un componente vital de los ejércitos avanzados y los sistemas económicos mundiales interdependientes. El segundo se refería al ascenso de China en el escenario mundial a través de reformas económicas que condujeron a un crecimiento sostenido y a la modernización militar. Al mismo tiempo, las políticas y acciones del gobierno chino han sustraído críticas internacionales, incluidas las persistentes denuncias de espionaje en línea, la censura interna en Internet y una mayor capacidad militar, todas las cuales utilizan redes informáticas. Estas percepciones de amenaza se ven acentuadas por la falta de transparencia. A diferencia de los Estados Unidos o de la Organización del Tratado del Atlántico Norte, China no articula su doctrina estratégica. Además, el material de código abierto sobre este tema es a menudo contradictorio, superficial y poco claro debido, en parte, a la ausencia de consenso sobre la terminología cibernética y la infancia de este campo.

2. ¿Cuáles son las mayores amenazas de seguridad cibernética de hoy, y qué deberían estar haciendo las organizaciones vinculadas con el Estado para reaccionar ante ellas?

La República Popular China (PRC) ha hecho avances significativos en su programa de ciberseguridad y está emergiendo como una potencia en el ciberespacio. Con la preservación de su monopolio del poder como objetivo primordial, el Partido Comunista Chino (PCC) refuerza su legitimidad a través de logros en el ciberespacio. El ejército chino gestiona el programa ciberespacial de China y hay una superposición significativa entre las operaciones ciberneticas civiles y militares, que se refuerzan mutuamente. Un establecimiento industrial y de I+D cada vez más sofisticado suministra al Ejército Popular de Liberación (EP) sistemas cibernéticos militares. El Departamento General de Armamentos de PLA (GAD) parece supervisar las adquisiciones y operaciones de sistemas cibernéticos. Otras organizaciones importantes en el programa cibernético incluyen china Cibernetics Science and Technology Corporation (CASC) y China Cibernetics Science and Industry Corporation (CASIC). Como contraparte aproximada de la NSA, la Administración Cibernetica Nacional de China (CNSA) facilita los intercambios internacionales y los programas de cooperación con otras naciones que afectan al ciberespacio.

3. ¿Cuál ha de ser la misión de un Comando Cibernético Nacional? Vale decir, sus propósitos y las actividades que la hacen viable.

La democratización de las TIC significa también que potenciales adversarios puedan tener un acceso sin precedentes a la economía nacional de otros estados, así como a sus ciudadanos y líderes nacionales, extendiendo las amenazas más allá de los límites de las redes –como los ataques a las redes sociales–, y los com-

ponentes computacionales –como el software malicioso–, y haciendo que la información pueda constituir una amenaza en sí misma.

Por ello la misión de un Comando Cibernético debe ser el uso de la tecnología para reunir inteligencia en el campo de batalla, coordinar las operaciones conjuntas de diferentes recursos militares y ayudar en la selección de sus objetivos, sino también, su uso para influir en la opinión pública de ciertos países, llevar a cabo actividades de espionaje y acceder a las ciberinfraestructuras militares y civiles de los que considera sus adversarios.

4. ¿Qué actividades reguladoras deben estar al servicio de las actividades tecnológicas de las que dependerá la viabilidad de un Comando Cibernético Nacional?

En la Era de la Información, es precisamente la información el recurso vital que potencia a todas aquellas esferas de poder.

Al mismo tiempo, sin embargo, el libre flujo de información constituye una amenaza directa y muy seria. Por ejemplo, en el caso de China ha emplazado la 'Gran Muralla Cortafuegos de China' y desplegado un número de censores en el orden de los centenares de miles, a los efectos de limitar la amenaza informativa contra el régimen.

Pero todo ello resulta insuficiente para hacer a un lado las preocupaciones de Pekín. Idealmente, un Gobierno debe controlar e influenciar la totalidad del flujo de información hacia sus adentros, lo cual implica moldear las estructuras internacionales que administran ese flujo de información.

5. Entonces ¿de quién dependerá la Resolución de Conflictos y el logro de la estabilidad ante las Ciber amenazas que enfrenta China como un estado Nación?

Después de la tierra, el mar, el aire y el espacio exterior, muchas personas han denominado al ciberespacio como el quinto dominio para actividades humanas, con múltiples implicaciones para un estado. En pocas palabras, los intereses políticos, económicos y de seguridad de un estado están ahora cada vez más conectados con la ciberseguridad. Sin embargo, Internet es un arma de doble filo, es decir, no solo ofrece enormes beneficios, sino también numerosos riesgos, desafíos y amenazas. Por lo tanto, dada la naturaleza sin fronteras, transnacional y única del ciberespacio, se ha convertido en una nueva frontera para la gobernanza global. China concede gran importancia al desarrollo de Internet y ha hecho enormes progresos en este sentido. Sin embargo, como recién llegado a este campo, China enfrenta varios desafíos y ha sido una de las principales víctimas de los ataques cibernéticos. Al mirar hacia el futuro, China está dispuesta a luchar por un ciberespacio pacífico, seguro, abierto y cooperativo junto con la comunidad internacional. A nivel internacional, existen muchas dudas sobre las políticas y prácticas de China en su desarrollo de Internet debido a malentendidos, prejuicios, falta de conocimiento e incluso la ignorancia de un lado. Por otro lado, existe una demanda creciente para comprender las políticas y prácticas de China en este dominio.

6. ¿De qué manera un Comando Cibernético Nacional buscará y detectará amenazas/oportunidades provenientes del exterior?

La ciberdefensa se ha convertido, en los últimos cinco años, en un tema importante en la escena internacional. Un Comando Cibernético, por el lugar que ocupa, es objeto de atención: es observado, criticado y designado por muchos estados como un actor importante en la ciberseguridad nacional, construyendo su estrategia de defensa cibernética contra lo que se llama la "ciber amenaza". Por lo tanto, es importante comprender mejor los desafíos actuales relacionados con la dimensión cibernética en relación con el ascenso de los conflictos. Las contribuciones de los investigadores internacionales brindan perspectivas cruzadas sobre estos, sus estrategias y políticas para la ciberseguridad y la ciberdefensa. Estos temas ahora han ganado una gran dimensión estratégica.

ENTREVISTA ESPECIALISTA 2

(Idioma original español)

1. ¿Qué opinión le merece el tema de la Ciberseguridad hoy día?

Al igual que con la nube y big data, la ciberseguridad en los últimos tiempos, sospecho que va a ser la siguiente gran palabra de moda que vamos a estar escuchando por un tiempo. En cuanto a si se convierte o no en algo muy positivo para el Estado, tendremos que esperar y ver. Hablar es fácil, pero soy optimista sobre la innovación en esta área.

2. ¿Cuáles son las mayores amenazas de seguridad cibernética de hoy, y qué deberían estar haciendo las organizaciones vinculadas con el Estado para reaccionar ante ellas?

Mis puntos focales recomendados para ciberseguridad, al menos por ahora, serían aquellos que están causando mayor dolor al en el para el Estado. Estos están probablemente en las áreas de IPS, control de acceso y registro y monitoreo de eventos, pero sus implementaciones sin duda estarán limitadas a lo que sus proveedores soportan.

3. ¿Existen estrategias universales que hayan demostrado ser particularmente eficaces para la seguridad cibernética, o es más importante ser flexibles y adaptarse conforme las amenazas evolucionan?

Claro que sí. Por ejemplo, organizar grupos y sistemas de seguridad específicos (con políticas para hosts, aplicaciones y entidades de red similares) que cruzan las fronteras físicas y lógicas y han demostrado ser difíciles de manejar con cualquier apariencia de eficiencia.

De igual forma el facilitar dominios de seguridad dinámicos para móviles, nube y en todos los sistemas de redes tradicionales, permitiendo a las organizaciones montar y desmontar sistemas a voluntad y, al mismo tiempo, ser capaces de hacer cumplir consistentemente las políticas de seguridad en todos los ámbitos, independientemente del momento y la ubicación de estos sistemas.

Ofrece una mejor integración con otras tecnologías definidas por software, por ejemplo, SDN, para moverse hacia una automatización más holística para tecnologías de seguridad tales como prevención de intrusiones, gestión de identidad y acceso, prevención de pérdida de datos y geolocalización.

Y finalmente enfocarse en una inteligencia a un nivel superior –en el software– en lugar de en el hardware, lo que puede permitir que los gerentes y a los administradores de seguridad enfocarse en las políticas y no en mantener los sistemas corriendo en un nivel inferior.

4. ¿Qué papel desempeñan los profesionales de nivel gerencial en la ciberseguridad?

Estos deben motorizar la necesaria una curva de aprendizaje inicial para la provisión, implementación y aplicación de las políticas de seguridad a través de sistemas y plataformas únicos que pueden o no pueden soportar.

Para ello deben introducir un nuevo tipo de complejidad que implica la creación y gestión de políticas de seguridad. El quién, qué, cuándo, dónde y por qué de las políticas tendrá que ser bien definido por estos antes de que su organización se embarque en un proyecto de este tipo.

5. ¿Cómo las regulaciones en materia de Seguridad se acercan a la ciberseguridad?

Pienso que el Consejo de Defensa Suramericano tendrá que hacer algunas consideraciones cuidadosas con el fin de decidir qué controles de seguridad se desplegarán a través de sus plataformas tecnológicas. Algunas paises que integran el Consejo de Defensa Suramericano pueden beneficiarse de esto más que otras, como aquellas en industrias altamente reguladas (por ejemplo, financiera) o grandes empresas que tienen una presencia más nacional o global. La Ciberseguridad no es una tecnología donde una talla aplica para todos; el caso de uso de cada organización será diferente. Al final, no debería importar si sus controles de seguridad son basados en hardware o en software, siempre y cuando se esté utilizando lo que realmente se necesita para minimizar sus riesgos.

6. ¿Cuál ha de ser la misión de un Comando Cibernético Nacional? Vale decir, sus propósitos y las actividades que la hacen viable.

La razón de ser hoy día de un Comando Cibernético Nacional ante las emergentes amenazas en materia de ciberseguridad, es la lograr la adecuada transición de un modelo de ciberseguridad de carácter preventivo y defensivo, hacia un esquema que incorpore elementos de mayor fuerza disuasoria en un contexto global de mayor competencia geopolítica.

Por ello en mi opinión, ante la rápida evolución de las ciberamenazas, aconsejo una aproximación y desarrollo más proactivo de la ciberinteligencia.

7. ¿Qué actividades reguladoras deben estar al servicio de las actividades tecnológicas de las que dependerá la viabilidad de un Comando Cibernético Nacional?

El adecuado desarrollo de un Comando Cibernético Nacional, exige trabajar con un enfoque multidisciplinar en todos los sentidos, que englobe aspectos más allá de los básicamente técnicos, vale decir de consolidación dela infraestructura tecnológica necesaria; del monitoreo, registro y control de ciberataques; o de la ubicación y empleo adecuado del factor humano, que en estos momentos es paradójicamente escaso pero altamente demandado.

En este sentido, el sector público y privado juega un papel relevante como ges-

tores y propietarios mayoritarios de los activos digitales de una Nación, por lo que las capacidades de ciberseguridad para soportar un Comando Cibernético Nacional residen en gran medida en las de sus empresas y entidades públicas.

8. ¿de quién dependerá la Resolución de Conflictos y el logro de la estabilidad organizacional de un Comando Cibernético Nacional?

La gestión de las situaciones de crisis en cualquier ámbito, que, por su transversalidad o dimensión, desborden las capacidades de respuesta de los mecanismos recursos habituales es responsabilidad ineludible de un CEO-C.

9. ¿Cómo se lograría la sinergia entre los organismos y empresas del sector público y privado con competencias en materia de ciberseguridad en una Nación?

Ante las amenazas y desafíos en el ciberespacio, que se derivan de su condición global y nacional, la existencia de una doctrina, la elevada tecnificación y una máxima conectividad son los factores calves que posibilitaran la sinergia entre las partes para atenuar el impacto ante cualquier ataque.

10. A su entender, en un Comando Cibernético Nacional ¿Quién será el responsable de la Regulación Interna y de la Optimización de los procesos y recursos?

Como en toda organización compleja, en un Comando Cibernético Nacional debe existir un CEO-C responsable de la cohesión de las partes, para garantizar la seguridad y resiliencia de los activos estratégicos de la Nación, entendiendo por estas, a todos los entes públicos y privados con responsabilidad en materia de Ciberseguridad.

11. ¿De qué manera un Comando Cibernético Nacional buscará y detectará amenazas/oportunidades provenientes del exterior?

Con el monitoreo y actualización permanente del mapa de ciberamenazas locales, regionales y globales.

12. ¿Cómo se producirá la planificación que asegurar la viabilidad de largo plazo? ¿Quién estará a cargo de la Adaptación y la anticipación?

El ciberespacio, más allá de un espacio común global, proporciona una visión de conjunto del ámbito de la ciberseguridad, de allí las razones que afianzan la necesidad de contar con una Estrategia Nacional de Ciberseguridad, que debe ser formulada e implementada bajo la rectoría de un Comando Cibernético Nacional.

13. ¿Quién proporcionará las directrices de la organización y cuál será el medio para hacerlas cumplir? ¿Quién asumirá la Autoridad Última, diseñará la política y garantizará identidad organizacional?

Un Comando Cibernético Nacional, tiene sentido para apoyar al Consejo de Seguridad Nacional y asiste al presidente del Gobierno en la dirección y coordinación de la política de Seguridad Nacional en el ámbito de la ciberseguridad. De esta manera fomenta las relaciones de coordinación, colaboración y cooperación entre Administraciones Públicas y entre estas y el sector privado, ante situaciones que por

su transversalidad o dimensión, desborden las capacidades de respuesta de los mecanismos recursos habituales con que cuenta el ecosistema de ciberseguridad nacional.

De allí la importancia de que su diseño este basado en un modelo de gobernanza con una considerable madurez, que delinee mecanismos de adaptación, regulación y control que permitan la interacción activa de los sectores público, sector privado y el resto de la sociedad civil.

APÉNDICE 6

Auto-entrevista a los autores

AUTO-ENTREVISTA AUTOR 1
(Idioma original español)

1. ¿Qué opinión le merece el tema de la Ciberseguridad hoy día?

El tema de la ciberseguridad es ya una cuestión de cultura y en consecuencia existe la necesidad de que la sociedad tome conciencia porque aún queda mucho trabajo de divulgación y concienciación por hacer.

Lo que ha pasado con en Venezuela con el Sistema Eléctrico Nacional y en anteriores casos con los Sistemas de Pago Electrónico o el sabotaje a la Industria Petrolera Nacional, nos demuestra que la Ciberseguridad no sólo es cuestión de legislación y de la transformación digital del Estado, las cuales además van a menor ritmo que la revolución digital que vivimos día a día.

Una vez más se pone sobre la mesa el tema de la creación de una Institucionalidad responsable de la protección de datos e infraestructuras críticas del Estado, y esto no es algo que deba pasar desapercibido, porque de no tomarse las medidas necesarias rápidamente, estos casos seguirán ocurriendo, con mayor frecuencia y con mayores consecuencias.

Pienso que debemos salir de la zona de confort y crear más cultura de la ciberseguridad para el conjunto de la sociedad.

2. ¿Cuáles son las mayores amenazas de seguridad cibernética de hoy, y qué deberían estar haciendo las organizaciones vinculadas con el Estado para reaccionar ante ellas?

A mi manera de ver las amenazas a la ciberseguridad hoy día son tres: el cibercrimen, que incluye actores individuales o grupos que dirigen ataques a sistemas para obtener ganancias financieras; la ciberguerra, que a menudo involucra recopilación de información con motivaciones políticas; y el ciberterrorismo, cuyo propósito es comprometer los sistemas electrónicos y causar pánico o temor.

Las organizaciones del Estado deberían prepararse para contrarrestar los métodos comunes que usan los ciberatacantes para controlar las infraestructuras críticas que emplean en sus operaciones computadoras o redes, toda vez que estas hoy son vulnerables mediante mediante diferentes tipos de ataque.

Entre los más destacados en lo que va del 2019, la literatura reseña los ataques de ransomware, que es un tipo de software malicioso de criptovirología que ame-

naza con publicar los datos de la víctima o bloquear perpetuamente el acceso a ellos a menos que se pague un precio. Los Cryptomining o programas de software y componentes de malware desarrollados para apropiarse de los recursos de un ordenador y utilizarlos para la extracción de criptocurrency sin el permiso explícito de un usuario.

El phishing, conocido como una de las formas más exitosas para que un hacker te robe información confidencial fingiendo que es alguien que no es, constituyéndose en el intento fraudulento de obtener información confidencial como nombres de usuario, contraseñas y datos de tarjetas de crédito disfrazándose de entidad de confianza en una comunicación electrónica.

Los Botnets, utilizados por los hackers para usar computadoras como herramienta y explotar su potencia para realizar ataques y estafas a gran escala.

Finalmente, los virus y los gusanos que cada día se vuelven más peligrosos y resistentes que nunca.

3. ¿Existen estrategias universales que hayan demostrado ser particularmente eficaces para la seguridad cibernética, o es más importante ser flexibles y adaptarse conforme las amenazas evolucionan?

Hoy día los Estados deben hacer frente a ataques contra la seguridad de sus infraestructuras críticas que son soportadas por Tecnologías de la Información y las Comunicaciones, de allí que gobiernos, administraciones públicas y empresas con alto valor estratégico han entendido que la prevención sigue siendo mejor estrategia que la cura. De allí que, contar con organizaciones especializadas en el tema de la ciberseguridad sin duda podría ayudar a evitar posibles ataques, mediante la detección temprana, neutralización, exploración de ciberamezas, para defensa o ataque ante actores que atenten contra las infraestructuras de tecnologías de información, sobre todo aquellas que soportan procesos críticos para el buen desenvolvimiento de la sociedad.

Esta situación ha conformado un nuevo escenario, que precisa atención de los diferentes actores políticos para conformar en el ámbito del planeamiento de la seguridad nacional una institucionalidad en la materia que permita adaptarse.

4. ¿Qué papel desempeñan los profesionales de nivel gerencial en la ciberseguridad?

Tienen la responsabilidad de estudiar en profundidad cuáles son las amenazas y los riesgos derivados den la materia para organizar el proceso de planeamiento nacional en el campo de la ciberseguridad, que de lugar al Plan Nacional de Ciberseguridad.

5. ¿Cómo las regulaciones en materia de Seguridad se acercan a la ciberseguridad?

La ciberseguridad no es un elemento aislado de la seguridad, sino un dominio que se encuentra incardinado en las estructuras de seguridad de nivel superior. Las regulaciones en materia de seguridad deben contemplar que el ciberespacio ha de ser protegido de incidentes, actividades malintencionadas y utilizaciones abusivas.

6. ¿Cuál ha de ser la misión de un Comando Cibernético Nacional? Vale decir, sus propósitos y las actividades que la hacen viable.

Asegurar la continuidad, funcionalidad e integridad de las infraestructuras críticas; con el fin de prevenir, gestionar, mitigar y/o restaurar sus funciones ante un eventual ataque cibernético.

7. ¿Qué actividades reguladoras deben estar al servicio de las actividades tecnológicas de las que dependerá la viabilidad de un Comando Cibernético Nacional?

Es crucial que las entidades reguladoras de los sectores clasificados como de infraestructura crítica asuman un papel más protagónico y comiencen a definir y dictar lineamientos claros sobre el tema de seguridad cibernética y a los fines de que las entidades reguladas cumplan con la normativa, estándares y buenas prácticas vigentes tanto de su sector en particular, como aquellas de acatamiento nacional.

8. ¿De quién dependerá la Resolución de Conflictos y el logro de la estabilidad organizacional de un Comando Cibernético Nacional?

De un Comité Consultivo que deberá integrarse con los responsables de las áreas que brindan soporte a aquellas donde se materializa la misión del Comando Cibernético Nacional.

9. ¿Cómo se lograría la sinergia entre los organismos y empresas del sector público y privado con competencias en materia de ciberseguridad en una Nación?

Facilitando y promoviendo el intercambio de información entre los responsables de seguridad de la información del gobierno a través de una red de confianza, donde se apliquen altos niveles de confidencialidad y profesionalismo. Los ataques y eventos a menudo afectan múltiples organizaciones. Una comunicación y coordinación adecuadas podrían reducir los riesgos y minimizar el posible impacto.

10. A su entender, en un Comando Cibernético Nacional ¿Quién será el responsable de la Regulación Interna y de la Optimización de los procesos y recursos?

El Comité Consultivo, que tendrá la responsabilidad de analizar la implementación de la estrategia y emitir informes que contengan recomendaciones debidamente justificadas para efectuar las modificaciones que sean necesarias.

11. ¿De qué manera un Comando Cibernético Nacional buscará y detectará amenazas/oportunidades provenientes del exterior?

La Internet es un ecosistema altamente cambiante, por lo que deben aplicarse mecanismos de análisis de entorno e inteligencia corporativa para mantenerse al

tanto de los cambios y cerrar tan pronto como sea posible las brechas que puedan surgir como consecuencia de los cambios y nuevos riesgos.

12. ¿Cómo se producirá la planificación que asegurar la viabilidad de largo plazo? ¿Quién estará a cargo de la Adaptación y la anticipación?

La adopción de un proceso formal de planificación y gestión del riesgo es esencial, para prever acciones ante los riesgos importantes relacionados con tecnologías de información, que podrían ocurrir de manera regular, y que proporcionaría un enfoque coherente en materia de ciberseguridad.

Un régimen de seguridad cibernética eficaz adopta o desarrolla un ciclo continuo de evaluación del riesgo, desarrollo de políticas de ciberseguridad que den garantía de continuidad del negocio, asignando de responsabilidades, promoviendo concienciación y seguimiento de la eficacia de los controles implementados. La planificación en ciberseguridad es una medida proactiva que asegura que, en caso de emergencias, fallos de sistema o desastres es posible recuperar y mantener las funciones normales en caso de ocurrir algún riesgo grave. La incertidumbre es un tema central en Riesgos de Tecnologías de la Información y por ello se requiere la implementación de las mejores prácticas para su gestión.

13. ¿Quién proporcionará las directrices de la organización y cuál será el medio para hacerlas cumplir? ¿Quién asumirá la Autoridad Última, diseñará la política y garantizará identidad organizacional?

Se debe designar un coordinador nacional que tendrá la responsabilidad de articular las acciones en materia de seguridad cibernética y darle direccionalidad y seguimiento al cumplimiento de una estrategia nacional en esta materia. La figura de un coordinador nacional, que recaerá en el Comando Cibernético Nacional, será el punto focal a nivel nacional e internacional para cualquier tema relacionado con seguridad cibernética.

AUTO-ENTREVISTA AUTOR 2

(Idioma original español)

1. ¿Qué opinión le merece el tema de la Ciberseguridad hoy día?

La ciberseguridad se ha vuelto muy complicada para las organizaciones de todo tipo conforme nuevas amenazas aparecen constantemente y las antiguas evolucionan. Estas han tenido que adaptar sus procesos de negocio y sus funciones para proteger los datos contra las amenazas que emergen del complejo entramado de relaciones y flujos dinámicos de información que habilitan las redes tele comunicacionales de hoy.

2. ¿Cuáles son las mayores amenazas de seguridad cibernética de hoy, y qué deberían estar haciendo las organizaciones vinculadas con el Estado para reaccionar ante ellas?

Las mayores amenazas son de acceso no autorizado, ataques de malware a partir de inyecciones de código, phishing. Por otra Parte se observan ataques muy sofisticados contra los estados-nación que los están haciendo no solo los llamados hacktivistas, sino ciberterroristas que tienen muchas habilidades, y están siendo empleados para la desestabilización de algunos gobiernos.

3. ¿Existen estrategias universales que hayan demostrado ser particularmente eficaces para la seguridad cibernética, o es más importante ser flexibles y adaptarse conforme las amenazas evolucionan?

Hay estándares de proveedores y de gobiernos para la utilización de los diferentes sistemas operativos en software libre o Linux. Sin embargo, se observa que existe una preferencia en usar y comprar productos propietarios como Windows.

4. ¿Qué papel desempeñan los profesionales de nivel gerencial en la ciberseguridad?

He estado compartiendo este tema con profesionales que trabajan en diferente organizaciones, y me comentan que les toca jugar roles diferentes. Lo que me preocupa son dos cosas que veo constantemente en el caso del Estado: Lo primero es que no tienen suficiente visibilidad y acceso para ser efectivos. Por lo general, están enterrados en algún lugar de las organizaciones públicas, y es el Estado quien es el representante de seguridad nacional.

La segunda cosa que veo es que los profesionales con roles gerenciales del Estado en esta materia simplemente no cuentan con recursos.

5. ¿Cómo las regulaciones en materia de Seguridad se acercan a la ciberseguridad?

La respuesta simple es que no están ayudando. Los responsables de la función de Seguridad Física no entienden la complejidad de la seguridad de la información. Lo que aún hacen hoy en día, es crear una lista de verificación de aspectos físico

susceptibles de ser vulnerados. El problema es que esto requiere conocimiento especializado y ello toma tiempo.

6. ¿Cuál ha de ser la misión de un Comando Cibernético Nacional? Vale decir, sus propósitos y las actividades que la hacen viable.

La misión de una Organización dedicada a la Ciber seguridad desde la perspectiva de la Cibernética, debe ser la de prevenir e identificar las potenciales ciber amenazas, para responder atenuando y/o amplificando la variedad que ellas suponen, y así recuperar exitosamente infraestructuras críticas que hayan sido vulneradas ante incidentes cibernéticos.

7. ¿Qué actividades reguladoras deben estar al servicio de las actividades tecnológicas de las que dependerá la viabilidad de un Comando Cibernético Nacional?

La actividad de regulación y control, son responsabilidad en el Modelo de Sistemas Viables, de la función anti oscilatoria o sistemas dos (S2), y tienen que ver con el Intercambio de información, la cooperación y la coordinación efectiva y oportunas entre las partes interesadas. Vale decir en este caso, de aquellas organizaciones dedicadas a la seguridad cibernética a nivel nacional, regional e internacional.

8. ¿De quién dependerá la Resolución de Conflictos y el logro de la estabilidad organizacional de un Comando Cibernético Nacional?

De un responsable encargado de desarrollar estrategias nacionales de ciberseguridad, que garanticen que el Comando Cibernético como un todo coherente, se comporte como un Sistema Viable, de forma de mantener la homeostasis en la infraestructura critica del país. Para ello habrá de involucrar a todas las partes interesadas relevantes de manera que se ajusten a la situación legislativa, cultural, económica y estructural del país y apoyen las iniciativas en esta materia a nivel nacional.

9. ¿Cómo se lograría la sinergia entre los organismos y empresas del sector público y privado con competencias en materia de ciberseguridad en una Nación?

Estableciendo y dándole cumplimiento a los principios básicos de toda organización cibernética:

1.- Requisito de variedad;

2.- Capacidad de canal;

3.- Capacidad de transducción. De esta manera las instituciones públicas y privadas podrían coadyubar en dar respuesta a incidentes de seguridad informática y brindar asistencia técnica personalizada en los momentos y lugares que sean requeridos.

10. ¿De qué manera un Comando Cibernético Nacional buscará y detectará amenazas/oportunidades provenientes del exterior?

Desarrollando la función de inteligencia, mediante la evaluación permanente de lo que acontece en el entorno, materializando estudios técnicos prospectivos e informes basados en hechos reales actuales donde se identifiquen los problemas y desafíos claves de seguridad cibernética en la región, a los fines de guiar a los res-

ponsables de políticas en esta materia, a los llamados CSIRT, a los operadores de infraestructura críticas tanto de organizaciones privadas y la sociedad civil.

11. ¿Cómo producir la planificación que asegure la viabilidad de largo plazo? ¿Quién estará a cargo de la Adaptación y la anticipación?

Creando una cultura organizacional en esta materia. Aumentando el acceso al conocimiento e información sobre amenazas y riesgos cibernéticos por parte de los interesados públicos, privados y de la sociedad civil, así como los usuarios de Internet.

Esta actividad debería estar a cargo de una Unidad o Centro de Planificación Estratégica Cibernética.

12. ¿Quién proporcionará las directrices de la organización y cuál será el medio para hacerlas cumplir? ¿Quién asumirá la Autoridad Última, diseñará la política y garantizará identidad organizacional?

Un Consejo Nacional de "alerta, vigilancia y prevención", también conocido en el medio como Equipo de Respuesta a Incidentes (CSIRT), en general asumen esta responsabilidad en diferentes países; estos Consejos promueven el desarrollo de Estrategias Nacionales sobre Seguridad Cibernética; y fomentan el desarrollo de una cultura que permita el fortalecimiento de la Seguridad Cibernética en el país.