La estrategia de ciberseguridad como un actor económico para las empresas en Colombia

Ricardo Andrés Guzman Fajardo

Trabajo de grado para optar al título profesional:

Maestría en Ciberseguridad y Ciberdefensa

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

2020

ESCUELA SUPERIOR DE GUERRA

MAESTRÍA EN CIBERDEFENSA Y CIBERSEGURIDAD NACIONAL

MONOGRAFÍA

LA ESTRATEGIA DE CIBERSEGURIDAD COMO UN ACTOR ECONÓMICO PARA LAS EMPRESAS EN COLOMBIA

BOGOTA, 05 DE AGOSTO DE 2020

ESCUELA SUPERIOR DE GUERRA

MAESTRIA EN CIBERDEFENSA Y CIBERSEGURIDAD NACIONAL

MONOGRAFÍA

LA ESTRATEGIA DE CIBERSEGURIDAD COMO UN ACTOR ECONÓMICO PARA LAS EMPRESAS EN COLOMBIA

RICARDO ANDRES GUZMAN FAJARDO

TUTOR:

LUCAS ADOLFO GIRALDO RIOS MSc, MBA

BOGOTA, COLOMBIA, MAYO 2020

LA ESTRATEGIA DE CIBERSEGURIDAD COMO UN ACTOR ECONÓMICO PARA LAS EMPRESAS EN COLOMBIA

GUZMAN FAJARDO RICARDO ANDRES

FIRMA:
C.C 79.795.926
TEL: 315 3569432
CORREO ELECTRONICO: ricardoguzmanf@hotmail.com

TUTOR: LUCAS ADOLFO GIRALDO RIOS MSc, MBA

FIRMA:

PAGINA DE EVALUACION

LA ESTRATEGIA DE CIBERSEGURIDAD COMO UN ACTOR ECONÓMICO PARA LAS EMPRESAS EN COLOMBIA

AUTOR; RICARDO ANDRES GUZMÁN FAJARDO
C.C 79.795.926

TUTOR: LUCAS ADOLFO GIRALDO RIOS MSc, MBA
C.C 71.790.859

CALIFICACIÓN EN NUMERO:

CALIFICACIÓN EN LETRAS: _____

OBSERVACIONES: _____

_____

_____

EVALUADOR:

FIRMA:

FECHA DE EVALUACION:

Agradezco a Dios por darme el tiempo de vida para llevar a cabo este trabajo,
A mi esposa por su fortaleza, paciencia y guía para concluir el documento,
A mi tutor por su excelente acompañamiento y guía,
A mi familia, a mis amigos personales y laborales por acompañarme en el proceso y a todos los profesionales que me brindaron de manera desinteresada su conocimiento.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LA ESTRATEGIA DE CIBERSEGURIDAD COMO UN ACTOR ECONÓMICO

RESUMEN

La metodología tradicional de suponer que al invertir en alguna solución de tecnología de ciberseguridad, o, de capacitar al usuario en ciberseguridad, permite ahorrar costos frente a un *"posible ataque informático"* que *"posiblemente causaría daños económicos"*; Se basa en el miedo y la incertidumbre, la incertidumbre de por sí, no permite mapear de manera correcta el camino de la estrategia, el miedo, en principio, genera actitudes defensivas generales que permean los cimientos de la estrategia. Tanto la incertidumbre como el miedo influyen también sobre la inversión, desfigurando los puntos de inversión críticos o forzando la inversión sobre ítems que no han demostrado su utilidad. Este caso de estudio, busca proponer un patrón matemático, que permita modelar factores o variables optimas, que puedan ser utilizadas en la generación de una estrategia de ciberseguridad, entregando un resultado de retorno de valor cuantificable, ajustado matemáticamente, que minimice al máximo el factor incertidumbre, optimizando la estrategia de ciberseguridad de la compañía o estado que lo utilice.

Palabras Clave: EVA, retorno de inversión, ciberseguridad, estrategia de ciberseguridad, inversión ciberseguridad, modelo matemático, ciberseguridad economía.

LA ESTRATEGIA DE CIBERSEGURIDAD COMO UN ACTOR ECONÓMICO

ABSTRACT

The traditional methodology of assuming that by investing in some cybersecurity technology solution, or, of training the user in cybersecurity, it allows saving costs against a "possible computer attack" that "could possibly cause economic damage"; It is possible fear and uncertainty, uncertainty in itself does not allow the path of strategy to be mapped correctly, fear, in principle, generates general defensive attitudes that permeate the foundations of the strategy. Both uncertainty and fear also influence investment, disfiguring critical investment points, or forcing investment on possible that have not proven useful. This case study seeks to propose a mathematical pattern that allows modeling optimal possible of variables that can be used in the generation of a cybersecurity strategy, delivering a return possible of quantifiable value, mathematically adjusted, that minimizes the factor as much as possible. Uncertainty, optimizing the cybersecurity strategy of the company or state that uses it.

Keywords: EVA, cybersecurity, cyberdefense, cybersecurity strategy, cyberdefense strategy, cybersecurity model, cybersecurity math model.

LA ESTRATEGIA DE CIBERSEGURIDAD COMO UN ACTOR ECONÓMICO PARA LAS EMPRESAS EN COLOMBIA

Cuando se habla de estrategia y dependiendo del entorno donde se desarrollan las actividades diarias, se pueden evocar diferentes pensamientos, algunos pensamientos dirigidos a grandes batallas donde las victorias han sido contundentes y las conquistas obtenidas han sido representativas para la humanidad, otros pensamientos, dirigidos al surgimiento y crecimiento de grandes empresas o corporaciones que han logrado posicionarse en el planeta y han entregado una marca reconocida mundialmente, otros pensamientos en cambio, dirigidos en personas que por sus actitudes o actividades han logrado ser reconocidas globalmente y se han vuelto iconos para diferentes generaciones.

Sin embargo, más allá de poder pensar en la preparación y la planeación, en la ejecución y el desarrollo de actividades, se avecina un terreno poco explorado, grandes batallas que han terminado en grandes victorias han llevado a grandes imperios en su camino a la destrucción, grandes corporaciones después de haber llagado tras un largo recorrido a la cima empresarial han sufrido caídas estrepitosas, e, ídolos, han encontrado de manera prematura el final de su carrera o de su vida tras un largo recorrido para llegar al éxito.

Esto hace pensar entonces, que más allá de la estrategia para logar un objetivo se encuentra el resultado, ese espacio de tiempo donde el éxito se vuelve palpable, donde lo sembrado se cosecha y donde lo que se quería se consiguió, de esta forma, entender el valor que devuelve el resultado, aún antes de obtenerlo, es un campo que merece una atención especial entre los directores, gobernantes e incluso en los padres de familia, pues el valor obtenido puede llevar en algunas ocasiones al fracaso.

Este documento de investigación relacionará y sustraerá mediante el uso de estructuras financieras y modelos matemáticos, apoyado en definiciones y teorías de diferentes autores, temáticas estratégicas, temáticas financieras, temáticas matemáticas y por supuesto temáticas tecnológicas y de ciberseguridad.

De esta forma y con el fin de generar un lineamiento investigativo, en el primer capítulo se abordarán las convergencias entre estrategias de ciberseguridad de diferentes países y las definiciones de diferentes autores, tomando dos estrategias específicas y realizando un ejercicio de *"análisis estructural"* se identificarán los factores claves que hacen parte de una estrategia de ciberseguridad. En el segundo capítulo, se rondará el ámbito financiero y contable, de forma, que, utilizando la comparación descriptiva, se demostrará la relación existente entre la generación de valor y la implementación de una estrategia de ciberseguridad. En el tercer capítulo, se presentará un modelo matemático simple, que une las variables de generación de valor con la estrategia de ciberseguridad, luego, el modelo se ajustará al ámbito empresarial y mediante el uso de las matemáticas basadas en la *"ecuación logística"*, se ajustará con el fin de maximizar su potencial de uso y minimizar el margen de error del resultado, culminando con un ejerció teórico y un ejercicio práctico que serán fuente importante de las conclusiones del estudio realizado.

1 Problema

Al proceso en el que las tecnologías digitales, crean interrupciones operacionales, que desencadenan respuestas estratégicas de las organizaciones, que buscan modificar o adaptar sus caminos de creación de valor a esta nueva era digital. Y, que además en el camino tienen que gestionar los cambios estructurales y las barreras organizativas que afectan los resultados operacionales, se le conoce como, Transformación Digital (Vial, 2019), este proceso disruptivo afecta profundamente la relación de agregación de valor de la empresa (Brynjolfsson & Hitt, 2000), pero ¿es posible que los problemas o los beneficios propios de las tecnologías digitales y el punto donde estas se desarrollan, el ciberespacio, tales como la ciberseguridad, puedan afectar los modelos de agregación de valor de las organizaciones? Eso es lo que se tratará de explicar a continuación.

José A Calle Guglieri en su libro *Reingeniería y Seguridad en el Ciberespacio* (1997), indica que para abordar un proyecto de reingeniería y de seguridad, se debe tomar en consideración el impacto de internet *"componente más representativo del ciberespacio"* (Guglieri, 1997) entendiendo entonces que Internet es la característica base, que junto con otras características conforman el ciberespacio, Guglieri aborda definiciones de diferentes autores, llegando a un aparte, donde en vez de dar una definición, simplemente le permite al término ciberespacio ser apropiado dependiendo del uso que las organizaciones en el mundo deseen darle, de igual forma, le permite al término ciberespacio obtener las definiciones que diferentes profesionales a nivel mundial le han querido asignar; entendiendo con esto, que una definición universal y estática en el tiempo, no se puede obtener. María José Caro Bejarano en su escrito *Alcance y Ámbito de la Seguridad Nacional en el Ciberespacio* (2011) enmarca ya el término ciberespacio llevándolo más allá del término Internet, uniéndolo al tratamiento de la información y ubicándolo en un entorno de sociedad de la

información, además le entrega al término ciberespacio la característica y la cualidad de ser un elemento, el cual, como elemento se está desarrollando de manera *"veloz y enorme"* (Bejarano, 2011), entendiendo así, que el desarrollo del ciberespacio se da de forma infinita y sin límites.

En el VI Congreso de Relaciones Internacionales, Sergio G. Eissa, Sol Gastaldi, Iván Poczynok y Maria Elina Zacarias di Tullio, en su artículo. *El Ciberespacio y sus Implicancias en la Defensa Nacional. Aproximaciones al Caso Argentino* (2012). Indican que el ciberespacio, aunque es de ámbito global, presenta límites geográficos y/o geopolíticos. Pues es una dimensión, como lo indican los autores, que *"atraviesa a los espacios fisicos"* (Sergio G Eissa, Sol Gastaldi, Ivan Poczynok, Maria Elina Zacarias di Tullio, 2012) que cuentan de por si con características limitantes. Más que ser la información un componente del ciberespacio, los autores apoyan el ciberespacio en la información, he interpretan, de esta forma, que, de manera paralela al tiempo, se ha multiplicado la magnitud de la información que sobre el ciberespacio se ha trasferido, por ende, el ciberespacio, ha crecido.

En 1980 el Information Sciences Institute de University of Southern California generó un documento llamado DOD STANDARD INTERNET PROTOCOL para la Defense Advanced Research Projects Agency, Information Processing Techniques Office. El documento tenía por objeto explicar el protocolo de comunicación usado en internet:

> *"The Internet Protocol is designed for use in interconnected systems of packet-switched computer communication networks. Such a system has been called a "catenet" [1]. The internet protocol provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed length addresses. The internet protocol also provides for fragmentation and reassembly of long datagrams, if necessary, for transmission through "small packet" networks."* (Postel, 1980, p 1)

En la traducción de la definición se puede resaltar que el uso del protocolo de internet está diseñado para sistemas interconectados de redes de comunicación por computadora con conmutación de paquetes. Que, para nuestro entendimiento actual, serían Internet o el ciberespacio. Permitiéndonos retirar con esta definición del término ciberespacio el encanto cultural, comercial y político y aterrizarlo de lleno al ámbito técnico o tecnológico. Como reflexión, se puede decir entonces, que la simplicidad es el reflejo del conocimiento.

Ingresando nuevamente en el entorno social, político, económico e incluso religioso y a medida que el ciberespacio se ha venido desarrollando transversalmente para las diferentes áreas que componen la sociedad, se puede decir entonces que nuestra sociedad se ha convertido en una sociedad de la información. Pensamiento que se ratifica en el Resumen Ejecutivo del Informe del 2015 sobre *Medición de la Sociedad de la Información* realizado por la ONU. Documento que tomo el atrevimiento para recomendarle al lector de este trabajo sea leído detenidamente.

Dominique Nora en su libro *La Conquista del Ciberespacio* (1997), nos indica que al interpretar este desarrollo, más allá, del ámbito tecnológico y del ámbito contable, que son ámbitos fácilmente reconocibles, e, ingresado en el ámbito financiero, que es algo más especulativo, y, entendiendo estos ámbitos, de manera pura como los define el diccionario de la real lengua española.

"Contabilidad: sistema adoptado para llevar la cuenta y razón de las oficinas públicas y particulares", "aptitud de las cosas para poder reducirlas a cuenta o cálculo", finanza es: *"obligación que alguien asume para responder de la obligación de otra persona"*, contable es: *"que puede ser contado"* (RAE actualización, 2019)

"Financiero: perteneciente o relativo a la hacienda pública, a las cuestiones bancarias y bursátiles o a los grandes negocios mercantiles" (RAE actualización, 2019)

Se evidencia que la medición de valor que da la humanidad, sobre la información, ha cambiado y cambia de manera uniforme, y, ha cambiado, y, cambia también de manera drástica, Dominique

nos lleva a un campo donde nos indica que para la sociedad actual ya no es importante el medio de transmisión por donde viaja la información, pues es común para todas las verticales de la industria y los servicios, los ceros y unos componen la base de esta información, en cambio, es como estos ceros y unos se vuelven atractivos para la humanidad, clasificada en el entorno de "clientes". *"los grandes capitanes de la industria se hacen las mismas preguntas que los empresarios jóvenes"* (Dominique, 1997, 24) *"un bit de la novela Madame Bobary no es diferente de un bit de la película Jurassic Park o de un bit del programa Microsoft Word"*. (Dominique, 1997, p 23)

Leónidas Torres Citraro en su ensayo *La importancia de los Activos Intangibles en la Sociedad del Conocimiento* (2014). Hace una revisión exhaustiva sobre el desarrollo de las empresas, iniciando estas en una era industrial y culminando en una era del conocimiento. Como cita en su ensayo.

> *"Ocean Tomo es una empresa pionera en el campo del capital intelectual, con sede en Chicago, Estados Unidos, que ha llevado a cabo una investigación sobre la creciente importancia de los activos intangibles en el valor de las 500 empresas que conforman el índice S&P500 a lo largo de un período de 35 años"*. (Citraro, 2014, p 7)

Y como se puede observar la Imagen 1 de (Citraro, 2014). El cambio de valor entre los activos intangibles y los activos tangibles ha sido notorio y significativo, la evolución entre lo mismos ha sido representativa ante el valor y valoración de las empresas.

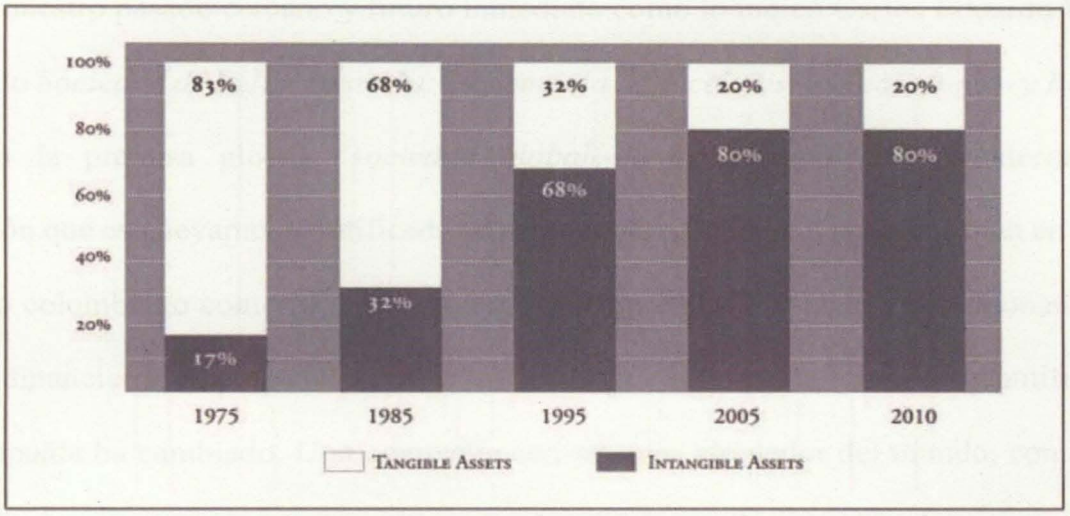


Imagen 1. Evolución del valor de los activos intangibles. Fuente: Citraro, 2014

> *"En el año 1975 el 17% del valor que el mercado asignaba a las 500 empresas que constituyen el índice S&P500 estaba representado por activos intangibles, que para ese momento solo se expresaba bajo la forma de patentes y marcas. El restante 83% eran activos tangibles, como es el caso de terrenos, edificios, maquinarias, equipos y mobiliario. Ya para el año 2005 la proporción era de un 20% para los activos tangibles y un 80% para los activos intangibles, los cuales habían cuadruplicado su proporción"* (Citraro, 2014, p 8).

Esto refuerza la idea que la definición de la sociedad del conocimiento le lleva por lejos a la definición de la sociedad industrial o a la definición de la sociedad agraria la identificación de nuestro momento actual de habitantes de la tierra.

Entendiendo entonces que somos una sociedad de la información, podemos afirmar que las infraestructuras físicas que conocemos, Infraestructuras de explotación de recursos renovables y no renovables, infraestructuras de producción de medios de movilidad, infraestructuras de transformación de materias primas, infraestructuras de producción alimentaria entre otras ya no son más la razón de ser que mide la grandeza, son ahora simplemente las estructuras obligatorias sobre las que se transportan los bits de la sociedad de la información actual (Autoría Propia) de

forma, que nuestro pasado cercano y futuro inmediato como lo indicó Carlos Eduardo Valderrama en su artículo *Sociedad de la Información: Hegemonía Reduccionismo Tecnológico y Resistencias*, se basa en la premisa global *"sociedad global de la información"* (Valderrama, 2012) identificación que es nuevamente ratificada ya no en modo conceptual sino más bien en modo legal para el caso colombiano como lo indica la Ley 1341 de 2009. Por ende y reflexionando bajo los parámetros financieros empresariales, podemos decir entonces que la forma de cuantificar el valor de una compañía ha cambiado. Una compañía con oficinas alrededor del mundo, con empleados, con infraestructura computacional y utilizando tecnología puede valer lo mismo para el mercado que una compañía de un aventurero en un garaje con un servidor conectado a internet y con una aplicación desarrollada y puesta en las tiendas "Play Store" o "App Store" o "Huawei Store" mientras va en el camino a convertirse en "una aplicación masiva", como ejemplo de esto tenemos el reciente cambio de la estructura de valor del sector automotriz, donde TESLA, es la compañía más valiosa del mercado, teniendo una cuota de participación en el mercado automotriz inferior grandes empresas de trayectoria como como Volkswagen Group, Toyota Motor o incluso la otrora siempre poderosa Ford Motor.

Forbes en su nota del 13 de octubre de 2013 relaciona las quince automotrices más importantes del mundo referentes a su valor de mercado, tal como se puede observar en la Tabla 1.

Tabla 1. Capitalización bursátil Mercado Automotriz.

Capitalización Bursátil Mercado Automotriz 2013	
Automotriz	**Millones de Dólares**
Volkswagen Group/Alemania	$ 94.400
Toyota Motor/Japón	$ 167.200
Daimler/Alemania	$ 64.100

Capitalización Bursátil Mercado Automotriz 2013	
Automotriz	**Millones de Dólares**
Ford Motor/EU	$ 51.800
BMW Group/Alemania	$ 56.700
General Motors/EU	$ 38.500
Nissan Motor/Japón	$ 43.400
Honda Motor/Japón	$ 72.400
Hyundai Motor/Corea del Sur	$ 41.500
SAIC Motor/China	$ 26.700
Renault/Francia	$ 20.300
Volvo/Suecia	$ 31.900
Kia Motors/Corea del Sur	$ 19.800
Tata Motors/India	$ 15.900
Suzuki Motor/Japón	$ 13.300

Fuente: https://www.forbes.com.mx/las-15-automotrices-mas-importantes-del-mundo/, 2013

Este mismo análisis realizado al día 2 de marzo de 2020 nos presenta el siguiente resultado en la Tabla 2:

Tabla 2. Capitalización Bursátil Sector Automotriz

Capitalización Bursátil Sector Automotriz 2020	
Compañía	**Capitalización Bursátil**
Tesla	**$ 137.115B**
Volkswagen	**$ 76.001B**

Capitalización Bursátil Sector Automotriz 2020	
Compañía	**Capitalización Bursátil**
GM	**$ 44.899B**
Ford Motor Company	**$ 28.547B**

Fuente: Elaboración Propia, TELSA (https://es-us.finanzas.yahoo.com/quote/TSLA?p=TSLA), Volkswagen (https://es-us.finanzas.yahoo.com/quote/VOW3.DE?p=VOW3.DE&.tsrc=fin-srch), GM (https://es-us.finanzas.yahoo.com/quote/GM?p=GM&.tsrc=fin-srch), FORD (https://es-us.finanzas.yahoo.com/quote/F?p=F&.tsrc=fin-srch), Tomado el 2 de marzo de 2020.

Lo que refuerza claramente, que la vinculación de la tecnología al sector automotriz, tiene una base operativa más extensa que la base operativa de su surgimiento, unidades que desplacen personas del punto A al punto B.

Esto conlleva que nuevos elementos constitutivos de valoración de empresas, se deben hacer presentes en los cálculos de valoración, toda vez, que los procesos clásicos basado en activos, participación del mercado o ventas podrían estar siendo replanteados, como lo indica Pablo Fernández es su documento de investigación, *Métodos de Valoración de Empresas* (2008). Existen diferentes formas de valorar las empresas clasificando en los grupos que se presentan en la Tabla 3:

Tabla 3. Métodos de valoración empresarial

PRINCIPALES METODOS DE VALORACION					
BALANCE	**CUENTA DE RESULTADOS**	**MIXTOS *(GOODWILL)***	**DESCUENTO DE FLUJOS**	**CREACION DE VALOR**	**OPCIONES**
Valor contable	**Múltiplos** de:	Clásico	*Free cash flow*	EVA	Black y Scholes
Valor contable ajustado	Beneficio: PER	Unión de expertos	Cash flow acciones	Beneficio económico	Opción de invertir
Valor de liquidación	Ventas	Contables europeos	*Dividendos*	*Cash value added*	Ampliar el proyecto
Valor sustancial	Ebitda	Renta abreviada	*Capital cash flow*	CFROI	Aplazar la inversión
Activo neto real	Otros múltiplos	Otros	APV		Usos alternativos

Fuente: Pablo Fernández, Métodos de valoración de empresas (2008)

Y como bien lo explica es su ejemplo Fernández (2008), una empresa desarrollada que desea ingresar al mercado local con la estrategia de adquirir una empresa posicionada solo valora de esta su *"marca"* mientras que la empresa local valorará sus activos, pues puede seguir utilizándolos para operar. Juan Mascareñas en su artículo *Metodología de la valoración de las empresas de internet* (2001) amplia este escenario enfocándolo en las tecnológicas, que basan su operación en el ciberespacio, con métodos como la valoración a través de flujos de cajas estimados o la valoración a través de las opciones reales. Estos métodos tanto clásicos, por llamarlos así, como *sui generis,* permiten crear paralelos de valor entre las empresas que operan en los diferentes dominios.

Esto nos puede llevar a pensar entonces, que el valor de las empresas y la forma de medir este valor ha cambiado. Como lo indica Federico Li Bonilla en su artículo *El valor Económico agregado (EVA) en el valor del negocio.*

> *"El valor económico agregado (EVA) es el importe que queda en una empresa una vez cubiertas la totalidad de los gastos y la rentabilidad mínima proyectada o estimada"* (Bonilla, 2008) *"Adicionalmente, el concepto incorpora activos que casi nunca se toman en cuenta y no aparecen en los estados financieros de las empresas como activos intangibles; por ejemplo, el valor del conocimiento, el cual se encuentra depositado en los colaboradores de la organización"*. (Bonilla, 2008, p 55).

Raúl L Katz, en su libro *El Papel de las Tecnologías de la Información y las Comunicaciones - TIC- en el Desarrollo, Propuesta de América Latina a los Retos Económicos Actuales*. Identifica la relación existente entre la competitividad de un país frente a los demás de la región, la inversión en redes de comunicaciones de un país frente a los demás todos desarrollándose y siendo evaluados en el entorno de la llamada *"sociedad de la información"* (Katz, 2009*)*. Llegando a concluir que

las TIC, si potencian, el crecimiento de un país. Sin embargo, Alice Shiu y Pun-Lee en el documento *Causal Relationship between Telecommunications and Economic Growth: A Study of 105 Countries*. Lograron en su estudio demostrar que la inversión en factores no solo TIC, sino físicos alrededor de las TIC, aumentan el potencial de crecimiento, como lo revelaron en el estudio realizado a China, ratificando que existe una relación entre crecimiento económico y el crecimiento TIC, igual, que entre crecimiento TIC, y, el crecimiento económico (Shiu y Pun-Lee, 2008).

Por lo anterior, podríamos inferir, que el desarrollo de las TIC, ha impulsado el desarrollo del ciberespacio, y, haciendo una relación lógica, el ciberespacio, por tanto, impulsará el desarrollo económico de las *"sociedades de la información"* , arriesgándonos a realizar una retrospectiva, podemos decir, que, el desarrollo en todo su espectro, ha permitido crear la historia de la humanidad, una historia que siempre ha estado ligada de una u otra forma a la seguridad, seguridad sobre lo creado físicamente, estructuras, ciudades, utensilios, herramientas etc. como también a lo creado intelectualmente, literatura, filosofía, nuevas tecnologías. De esta forma, la historia de la humanidad nos ha mostrado siempre la importancia de la protección de las estructuras físicas o lógicas que el desarrollo ha llevado a crear y que componen la sociedad actual; Infraestructuras de explotación de recursos renovables y no renovables, infraestructuras de producción de medios de movilidad, infraestructuras de transformación de materias primas y añadiendo estructuras con fines plenamente sociales, escuelas, hospitales, reservas naturales de nacimiento de especies o de nacimiento de fuentes hídricas, edificaciones de atención al ciudadano de gobierno central o estatal o vías que interconectan regiones y unen territorios divididos de manera natural por la geografía del terreno. Podemos crear el paralelo que, así como la historia nos enseñó a proteger las estructuras físicas, entonces frente al ciberespacio, aparecen hora, infraestructuras físicas y lógicas que deben ser protegidas, que permiten llevarnos en la ruta del desarrollo de la sociedad de la información, y por ende, a la creación de una *"historia de la ciberinformación"* (Autoría Propia).

Para la protección de estructuras físicas hemos visto el despliegue tecnológico de aeronaves, embarcaciones y armas convencionales que de alguna manera garantizan la seguridad del entorno físico, dispositivos y tecnologías generalmente usadas por los gobiernos en sus fuerzas militares y de policía. Y en el entorno tecnológico, hemos visto aparecer tecnologías para la protección de las comunicaciones como lo son las tecnologías de Firewall, tecnologías para la protección de las aplicaciones como lo son los Firewall de Aplicación, tecnologías para la protección de la información estructurada como los son los Firewall de Bases de Datos, tecnologías para la protección de información no estructurada como los son los software de gobierno de datos, tecnologías para la gestión de identidades, tecnológicas para la protección frente al acceso a la nube (CASB) y muchas otras que buscan la protección de la información de los software que la generan o la almacenan y de los usuarios en el ciberespacio.

En el camino del desarrollo tecnológico, la protección física de las estructuras le ha implicado a la sociedad, la inversión o el gasto de recursos monetarios. De igual forma, el desarrollo del ciberespacio, le implicará a la sociedad actual, la inversión de recursos monetarios para su expansión y sostenimiento, y, paralelamente, así como en la dimensión física apareció la protección del entorno físico, en el ciberespacio apareció la protección del entorno *"ciberespacial". Los recursos monetarios siempre serán finitos y el desarrollo contará siempre con la cualidad de ser infinito."* (Autoría Propia).

Por tanto, al haber invertido recursos monetarios en ítems específicos, evolucionamos en la forma de identificarnos como sociedad, de sociedad industrial a sociedad del conocimiento, entonces, debemos pensar que, así como la sociedad evolucionó, las empresas también evolucionan, y lo hacen, al momento de invertir recursos para su operación en el ciberespacio, por tanto, se debe evolucionar también en la forma de valorar las empresas que componen esta nueva sociedad del conocimiento.

En este caso, utilizando y abordando específicamente el valor económico agregado de las compañías u organizaciones, surge entonces un problema, los modelos tradicionales de medición y agregación de valor en las empresas no responden de manera efectiva a las realidades de la cuarta revolución industrial, permeado con el hecho que esta nueva dinámica organizacional conlleva nuevos retos y la vinculación de nuevos agregados al valor empresarial, para nuestro caso, la capacidad de monetizar la ciberseguridad en las organizaciones.

2 Pregunta de investigación:

¿Qué relación existe entre las mejoras en ciberseguridad en las compañías de esta sociedad de la información, el retorno de valor y el valor económico agregado (EVA)?

3 Objetivo

Proponer un patrón matemático que permita modelar factores financieros que puedan ser utilizados en la generación de valor económico agregado, mediante la implementación de una estrategia de ciberseguridad.

3.1 Objetivos Específicos

1. Identificar y conceptualizar dos estrategias en ciberdefensa Internacionales cuyo contenido haya sido pensado con el fin de impactar la economía del país.
2. Identificar, determinar y estimar el nivel de impacto económico obtenido con la implementación de una estrategia de ciberseguridad en un país.
3. Determinar un modelo matemático financiero genérico que permita apoyar la presentación de estrategias de ciberseguridad.
4. Elevar un modelo matemático a un posible uso empresarial o local.

De la misma manera podríamos suponer que en los mercados digitales, aquellas compañías que han mostrado fortaleza tecnológica y han entregado al público seguridad cibernética en sus servicios soportados en TIC´s podrían estar siendo privilegiadas por los usuarios al adquirir sus bienes o servicios utilizando sus medios electrónicos, situación que una formulación matemática podría llegar a relacionar.

Así, la investigación sobre patrones matemáticos relevantes a modelos estratégicos cibernéticos destaca su importancia, por cuanto toda estrategia busca en el tiempo poder cumplir el objetivo para la cual fue creada y entregar de manera recíproca su eficacia. Por tanto, al poder formular una estrategia o al implementar mejoras en seguridad cibernética basada ya en posibles resultados. permitirá deducir el impacto y la aplicabilidad. Objetivos básicos de la planeación.

4 Metodología

El proyecto utilizará un método mixto de investigación pragmático, y, un diseño explicativo secuencial, la utilización de esta metodología permite obtener tanto datos referenciales para la generación de modelos como datos cuantitativos para los ejercicios de comparación. (Hamui-Sutton, 2015)

De manera global, se recopilará la información referente a estrategias de ciberdefensa internacionales, enfocando el ejercicio en dos estrategias que presenten como factor común, la afectación de la economía. Esta información, será conceptualizada y parametrizada, para obtener y filtrar datos e indicadores económicos referenciales de diferentes países, las fuentes de los datos y su correlación, se probará mediante un ejercicio de análisis estructural. Con los indicadores ya tabulados, se normalizarán y se usarán como base para la generación de un modelamiento matemático inicial que servirá de apoyo para demostrar la racionalidad del ejercicio. Se realizará luego, un ejercicio sobre el entorno corporativo, clasificando mediante un ejercicio de análisis estructural las variables que harán parte del modelo matemático. El cual se representará también en una ecuación, El modelo matemático, resultado de este ejercicio, se ajustará mediante el uso de la ecuación logística, permitiendo terminar el caso de estudio con la aplicabilidad sobre a un ejemplo teórico y un ejemplo práctico.

5 Marco Teórico

En el marco actual que nos encontramos de habitar, como se mencionó anteriormente, en un planeta regido por una visión de sociedad de la información, encontramos entonces que la valoración de las empresas que hacen parte de la sociedad, cambia, pues como se abordó, no es igual una empresa ubicada en una sociedad industrial a una empresa ubicada en una sociedad de la información, medir los intangibles en una sociedad industrial no tenía un sentido práctico, pues no se debían entregar productos o soluciones a la medida, en una sociedad de la información, ahora tiene un sentido práctico y casi obligatorio, los productos o soluciones deben ser personalizados, buscando la generación de un bien tangible o intangible que solucione las necesidades de las personas (Clavijo, 2003), en una sociedad de la información los productos o soluciones deben responder con mayor detalle a las especificaciones del consumidor, no solo a sus necesidades, sino también, a sus expectativas, consumidores informados con una mayor capacidad de decisión. El poder ya no está en manos de los productores, sino de los compradores, toda vez que estos definen características emocionales de los productos y servicios (Solow, 1957).

Gracias al desarrollo de las TIC, en los temas referentes al Aprendizaje de Maquina o a la Inteligencia Artificial, en esta sociedad de la información, ahora se pueden recolectar gran cantidad de datos de los clientes y los proveedores, los mismos, ahora se puede analizar de manera rápida, para nuestro caso, la información obtenida y procesada sumará valor a los bienes o servicios entregados (Autoría Propia). Sin embargo, como se mencionó, esto nos lleva al camino paralelo de la seguridad, la cual en la sociedad industrial estaba planamente enmarcada en los activos físicos, cuidado de los espacios físicos, protección del dinero físico, protección de los equipos, protección de la producción, pero, llevándonos ahora a un entorno lógico donde reposa la información, el

ciberespacio nos enmarca plenamente en el campo lógico (datos convertidos en ceros y unos) y en alguna medida en el campo físico (construcciones e infraestructuras de comunicaciones) que lo sustenta, relacionados entre sí de una manera directa, la razón de ser del campo físico es el campo lógico y sin el campo físico el campo lógico no dejaría de ser simplemente una teoría.

En el artículo, *Capital Intelectual y Generación de Valor*. Altuve (2002) nos demuestra la importancia de adicionar, por ejemplo, el capital intelectual a la formulación del valor económico agregado, buscando refutar la idea contable donde el capital intelectual es un pasivo, pues no está inmerso en la empresa, y si en cambio, está en las personas o recursos que en algún momento pueden abandonar la organización. Teniendo presente como lo redacta Gonzalez A. (2005), en su artículo, *Relación entre EVA (Valor Económico Agregado) y los Retornos Accionarios de Empresas Chilenas Emisoras de ADRs*, el termino EVA fue acuñado por la firma Stern Stewart & Company con el fin de convertirlo en la guía para determinar los precios del capital, sin embargo, el autor abre el abanico del cálculo del EVA y lo lleva a dos metodologías, una calculando el EVA desde los Activos y la otra calculando el EVA desde el Patrimonio.

Entendiendo los activos como los expresa Macedo (2007) en su libro *Introducción a la Contabilidad.*

> *"Activo: En contabilidad se le denomina así al total de recursos de que dispone la empresa para llevar a cabo sus operaciones, representa todos los bienes y derechos que son propiedad del negocio".* (Macedo, 2007, p 17)

Y patrimonio como lo indica Irarrazabal (2010) en su libro *Contabilidad, Fundamentos y Usos.*

> *"Patrimonio: diferencia entre los activos y los pasivos de una empresa en un momento dado. El patrimonio está conformado por el capital (aportes de capital efectuados menos retiros de capital) más el resultado acumulado desde que la empresa inició sus actividades".* (Irarrazabal, 2010, p 32)

Podemos observar que se ha abordado la generación de valor con componentes intrínsecos de nuestras industrias y empresas actuales, dejando en evidencia que, aunque todas ellas utilizan el ciberespacio como un medio de acercamiento al público o un medio para el desarrollo de operación, incluso como un medio de producción. No se enumera ni cuantifica el valor del ciberespacio, o mejor, no se cuantifica el valor de uso del ciberespacio por parte de las empresas de la sociedad de la información, no se discriminan los componentes que componen los negocios en el ciberespacio, ni mucho menos, el valor que los mismos agregan al Valor Económico Agregado (EVA, por sus siglas en ingles). Como lo concluyó Marquina Sánchez (2014) en su artículo *Las organizaciones empresariales trasnacionales como autoridad en la gobernanza del ciberespacio* escrito para el XIX Congreso Internacional de Contaduría Administración e Informática.

> *"Las problemáticas en torno a la construcción social del ciberespacio, se han convertido en asuntos públicos de carácter técnico, económico, jurídico, político y social y forman parte de la agenda internacional relacionada con el entorno virtual de los negocios electrónicos"* (Lourdes, 2014, p 13).

Existe ahora según Lourdes (2014) un entorno nuevo de comercio, llamado el entorno virtual de los negocios electrónicos, el cual difiere tanto en su base como en su forma a los modelos de negocios tradicionales sobre los cuales nuestras sociedades han evolucionado.

En su artículo Gonzalez Campo (2010) *E-Stakeholders: Una aplicación de la Teoría de los Stakeholders*, identifica en el internet de los negocios electrónicos, los agentes que lo componen, relacionando entre otros, a las comunidades de desarrolladores, a las comunidades de usuarios de software libre, a los usuarios que están en contra de las multinacionales, a los piratas o hackers de la red. Esta identificación retrata el antes, donde todo eran herramientas de uso y un después donde se identifica un nuevo espacio, esto permite cruzar la línea de pensar en internet, como una

herramienta para los negocios, y, donde al agregarle los agentes que la componen, le brindan una característica diferente, que la acerca más a su evolución como ciberespacio.

En el trabajo de Ballesteros (2002), *El Espacio Social del Cibercomercio. El Caso Español*, liga de manera puntual al comercio electrónico con la sociedad, pues identifica el comercio electrónico limitándolo a la sociedad que lo consume , puede ser una sociedad grande de una capital ruidosa o una sociedad pequeña de un pueblo silencioso en la montaña, de esta forma, puede concluir que el comercio electrónico ya no es, en nuestra sociedad actual, la definición que nos representa, pues al depender este comercio del espacio social, hace que el comercio electrónico evolucione y se convierte entonces en cibercomercio.

> *"Estamos en una época de constante construcción de nuevas relaciones espacio-temporales, de nuevas formas de interacción, control y organización de las sociedades humanas, una época de intensa variedad de ciberespacios, de redes múltiples y heterogéneas que se vinculan a espacios diferenciados".* (Ballesteros 2002, p 671)

Internet Society en su informe 2019, I*nforme Global de Internet Society, Consolidación en la Economía de Internet*, nos brinda una idea clara para muestra sociedad de la información actual

> *"Internet está creciendo y disminuyendo al mismo tiempo, los usuarios y el tráfico aumentan, pero las interacciones son con un número menor de actores multiservicio"* (Internet Society, 2019, p 24).

6 Identificación y Conceptualización de Estrategias y Ciberseguridad

Para identificar un modelo matemático basado en una estrategia, lo primero sería entender el contexto de la palabra estrategia, partiendo del entendimiento que de la misma ofrecen diferentes autores que la tratan desde el campo, contextual, político, administrativo y militar

La estrategia, como palabra, tiene su origen y se define según la real academia de la lengua como:

> *Del lat. strategĭa 'provincia bajo el mando de un general', y este del gr. στρατηγία stratēgía 'oficio del general', der. de στρατηγός stratēgós 'general'*
> *1. f. Arte de dirigir las operaciones militares.*
> *2. f. Arte, traza para dirigir un asunto.*
> *3. f. Mat. En un proceso regulable, conjunto de las reglas que aseguran una decisión óptima en cada momento*

Es, por tanto, el arte o proceso de dirigir o trazar operaciones, procesos o asuntos particulares. La estrategia, al ser abordada por economistas o empresarios, puede diferir o contextualizarse de diferentes maneras, la estrategia al ser abordada por los políticos o los militares, igual que, por los economistas o empresarios, puede tomar nuevos rumbos y ensanchar sus capacidades. La misma, connota diferentes factores que bien vale la pena enumerar con el fin de convertirlos en términos manejables, denominados variables, podemos decir entonces, que para el ámbito político la estrategia podría ser como lo indica Acevedo Zapata, S, (2018).

> *"Los lineamientos estratégicos como la directriz o las líneas de acción (políticas sociales, económicas etc.) que permitan sustentar la creación y el uso de la estrategia. Teniendo estos una introducción, un objetivo, un alcance y una justificación".* (Zapata, 2018, p 25)

Una definición que, al relacionar las políticas sociales, económicas etc. le suman a la estrategia condiciones globales, como lo son las políticas de gobierno, y, donde el entendimiento de la estrategia debe ser redactado para los actores que influyen en la misma, políticos, líderes sociales,

líderes comunitarios etc. Ubicando así, las líneas de acción de la estrategia en una modalidad de redacción basada en la tipificación simple de la introducción, el objetivo, el alcance y la justificación.

Una definición empresarial de la estrategia según otro autor es:

> *"La estrategia es la creación de una posición única y valiosa que involucra un conjunto diferente de actividades"* (Porter & Porter, 2008, p 10)

En este caso, la definición al citar, "una posición única", le agrega a la estrategia un espacio de acción y le da de manera indirecta una personalización, convirtiéndola en única para cada individuo, empresa, organización o estado.

Una definición militar de la estrategia se enmarca como:

> *"trazar el plan de guerra ... dirigir las campañas individuales y, a partir de ello, decidir acerca de los compromisos individuales"* (Von Clausewitz, 1976, p 177)

Así entonces, el autor le agrega a la estrategia el compromiso frente a la actividad y la divide en cuerpos pequeños llamados "campañas".

La estrategia, es una palabra común y genérica que cae bien en los diferentes escenarios donde se use, de esta forma y partiendo de las definiciones anteriores, podemos extraer y decir que la estrategia se ve reflejada en los pasos mentales diseñados para ser ejecutados de manera coordinada en el tiempo, con el fin de lograr un objetivo deseado.

A partir de estos elementos, en un ámbito económico, serían los pasos mentales diseñados para ser ejecutados de manera coordinada en el tiempo que nos lleven a un objetivo financiero deseado, utilizando la definición en un ámbito empresarial, serían los pasos mentales diseñados para ser ejecutados de manera coordinada en el tiempo que nos lleven a un objetivo comercial o de posicionamiento deseado, utilizado la definición en el ámbito político, podrían ser los pasos

mentales diseñados para ser ejecutados de manera coordinada en el tiempo que nos lleven a un objetivo social deseado y en el ámbito militar, podrían ser los pasos mentales diseñados para ser ejecutados de manera coordinada en el tiempo que nos lleven a un objetivo misional deseado.

Extendiendo la definición, al ámbito competente de este trabajo de investigación sobre el cual estamos construyendo, podríamos decir entonces que son los pasos mentales diseñados para ser ejecutados de manera coordinada en el tiempo que nos lleven a un objetivo cibernético deseado, y, si lo enmarcamos en la defensa cibernética, serian entonces, los pasos mentales diseñados para ser ejecutados en el tiempo de manera coordinada que nos lleven a un objetivo de ciberdefensa o ciberseguridad deseado.

Desde un punto ortodoxo que ya ha sido estudiado, aplicado, analizado y contextualizado, por diferentes autores frente al tema como lo son OC Ferell en su libro *Estrategia de Marketing* 2012, R Andreu en su libro *Estrategia y Sistemas de Información* 1996, Me Porter en su libro *Estrategia y Ventaja Competitiva* 2005, JA Amaya en su libro *Gerencia: Planeación y Estrategia* 2005, JC Maroto en su libro *Estrategia. De la Visión a la Acción* 2007, KR Andrews en su libro *El Concepto de Estrategia de la Empresa* 1984, Car Cleri en su *libro Estrategia Bonsái: y otras Estrategias para el Desarrollo de las PyMEs*, M Guizot en su libro *Historia de la Civilización Europea* 1846, JF de Couto en su libro *Historia del Combate Naval de Trafalgar, Precedida de la del Renacimiento de la Marina Española Durante el Siglo XVIII* 1851, Antoine Henri Jomini en su libro *De la Teoría Actual de la Guerra y de su Utilidad* 1840, podemos tomar entonces para este trabajo una definición administrativa de la estrategia, la definición dada por Porter, la cual enmarca dentro de sí características de las definiciones anteriormente citadas.

> *"la estrategia puede ser percibida como la práctica de construir defensas contra las fuerzas competitivas, o, como encontrar una posición en un sector, donde las fuerzas son más débiles. Modificaciones en la fortaleza de las fuerzas, indican cambios en el escenario*

competitivo que son clave para la elaboración continua de la estrategia" (Porter, 1979, p 58)

Esta definición tiene ya más de treinta años de ser validada y usada en el mundo corporativo global, por tanto, tiene todo el sentido utilizarla y proyectarla a un entorno cibernético que es nuevo. De esta forma, al desglosarla en cada una de sus partes podríamos decir:

a. Práctica de construir defensas: En un entorno cibernético se construyen defensas que permiten contener al o los atacantes con el fin de detener la rapidez del ataque, buscando con esto poder identificar el vector y el origen antes que puedan llegar al objetivo.
b. Contra las fuerzas competitivas: el entorno cibernético representa claramente estas fuerzas competitivas, países buscando secretos, empresas buscando secretos, delincuentes buscando recompensas, delincuentes compartiendo conocimiento, gobiernos y delincuentes compartiendo conocimiento, empresas inventando soluciones tecnológicas, fuerzas con muchos intereses que de alguna manera impactan el entorno.
c. Posición en un sector donde las fuerzas son más débiles: se pasó ya por el camino donde las empresas y gobiernos tenían toda su infraestructura e información en sus propios datacenter, para luego alojarlos en los datacenter de terceros y ahora la información y la infraestructura están en tecnologías como servicio (nubes públicas) logrando con ello ubicarse dentro de un entorno donde las fuerzas antes mencionadas son más débiles en su capacidad de acceso, pero no de uso.
d. Modificaciones en la fortaleza de las fuerzas indican cambios en el escenario competitivo: Por ahora se denotan los primeros pinos donde las fuerzas han empezado a romper estas nubes públicas, robando credenciales se han permitido el acceso a bases de datos con información de clientes o empleados inconformes han cambiado o eliminado el acceso a

servicios contratados, situación que está llevando al entorno cibernético a enfocarse en métodos de autenticación muy fuertes forzando las empresas tecnológicas a recorrer entonces los caminos cuánticos para el cifrado o a aplicar tecnologías no comerciales sobre las redes se súper alta velocidad.

e. Que son clave para la elaboración continua de la estrategia: Al identificar los cambios tecnológicos, las estrategias de ciberseguridad deben modificarse a la misma velocidad que los cambios tecnológicos, antes, las comunicaciones eran persona a persona, luego, persona a cientos o miles o millones de personas, ahora, son máquina persona y en el futuro podrían ser maquina a millones de máquinas y millones de personas, junto con todas las iteraciones posibles, de esta forma, los métodos defensivos y ofensivos se deben adaptar, utilizando, por ejemplo, tecnologías como, la inteligencia artificial o tecnologías como, el aprendizaje de máquina.

Con los conceptos previamente relacionados, podemos evidenciar que muchos países han iniciado el camino de crear y aplicar estrategias de ciberdefensa, Canadá 2010, España 2011, Francia 2011, EEUU 2003, Estonia 2008, Japón 2009, Colombia 2011, Australia 2009 etc. En algunas ocasiones, enmarcadas en modelos estratégicos que ya han sido usados por otros países, y, que ya en el presente han empezado a entregar resultados, reflejados por ejemplo en la creación de agencias o de legislación enfocada en ciberdelitos o delitos informáticos. Esto como nos lo deja ver el artículo, *Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local*, LEIVA (2015)

Nos encontramos entonces con estrategias que, aunque son nuevas, teniendo en cuenta la cronología de nuestra humanidad, son estrategias de ciberseguridad o ciberdefensa ya declaradas, como, la del Reino Unido, la de Estados Unidos, la de China, la de Portugal, la de Argentina, la de

Canadá, la de Australia, la de Malasia, la de Omán, la de Nueva Zelanda, la de Estonia, la de Alemania. En total, más de 150 estrategias, una cifra representativa frente a los 193 países que las naciones unidas reconocen como estados miembros y 2 más como estados no miembros. *Naciones Unidas, (2020), Estados Miembros. Recuperado de https://www.un.org/es/member-states/index.html*

Según el informe realizado por la firma ABI Research y su índice GCI (Indice Global de Ciberseguridad) el cual mide el desarrollo de ciberseguridad de un país, informe que fue expuesto en el foro económico mundial del 2015 y que condensa el camino por el que han transitado y están transitando los países en este frente, podemos identificar que la gran mayoría de los países comenzaron o ya dieron sus primeros pasos en este sentido, pasos legales, pasos tecnológicos y pasos sociales, entre otros.

Haciendo un comparativo basado en algunos de sus datos, se puede crear una línea base de actividades que bien podrían ser, con el objetivo de convertirlos nuevamente en términos manejables para este documento, variables mayores, variables que permiten identificar diferencias y similitudes entre las estrategias de ciberseguridad de los diferentes países, de esta forma, relacionando algunos pocos países y tomando al menos un país por cada uno de los cinco continentes según el compendio utilizado por Naciones Unidas (América, Europa, África, Asia y Oceanía) se puede crear una matriz representativa válida para este estudio.

El contenido marco de la matriz comparativa estará compuesto entonces por las actividades realizadas por un país frente a legislación, las actividades realizadas por un país frente a regulación, la creación de estándares tecnológicos y de agencias diferentes a ministerios para abordar la ciberdefensa.

Estas variables, son elegidas, debido a que las mismas logran captar de manera macro el compromiso de un estado frente a la estrategia de ciberseguridad. El hecho que un estado logre

enmarcar una legislación frente a ciberseguridad, evidencia que el ejecutivo y el legislativo tienen un norte definido frente al tema, lo cual le brinda a la nación su primera línea de defensa frente a incidentes cibernéticos. De igual manera, el que existan actividades de regulación y cumplimiento, denotan la madurez del estado frente a la ciberseguridad y los actores del mercado, al existir regulaciones se reconoce que existen actores importantes que deben ser protegidos de manera directa o indirecta por el estado y que los mismos son de carácter vinculante en la estrategia. El que el estado regule la utilización de estándares locales o internacionales, da un paso fuerte frente a la ciberseguridad, pues permea todas las actividades y a todos los actores del país, pasando por el gobierno, aterrizando en las empresas y culminando en los ciudadanos, estándares seguros, obligan a la creación y uso de soluciones seguras. La creación de agencias responsables, diferentes al ministerio de comunicaciones, connota la relevancia frente a la ciberseguridad, desprendiéndola de los cambios políticos y de su relación primaria con las comunicaciones, entregándole a la ciberseguridad los demás aspectos que la componen, como lo son, los medios físicos, los medios lógicos y la humanidad. *Unión Internacional de Comunicaciones, (2020), Development. Recuperado de https://www.itu.int/pub/D-STR-SECU-2015/es.*

La Tabla 4 condensa la información frente a las actividades previamente descritas y realizadas con corte en el año 2013 por los estados de Brasil, de Austria, de Canadá, de Egipto, de Camerún, de Papua New Guinea y de Filipinas. Seleccionar estos países nos permite dar un recorrido por el globo terráqueo, partiendo de la idea de no seleccionar únicamente los países con mayor desarrollo frente a la ciberseguridad, evitando caer en la parcialidad de las fuentes, permitiendo contextualizar de mejor manera las actividades fundamentales a aplicar por parte de los gobiernos, bien sea que estén desarrollados y/o en proceso de desarrollo frente al ciberespacio.

Tabla 4. Matriz actividades fundamentales en la estrategia de ciberseguridad

Actividades Fundamentales Estrategia Ciberseguridad	
Regulación y Cumplimiento	Agencia Responsable de la Ciberseguridad Diferente al Ministerio de Comunicaciones
Legislación Dentro del Código Penal	Estándares

Fuente: Elaboración propia a partir de ITU (2019)

La implementación de estrategias de ciberdefensa por parte de un gran número de países como lo evidencia el informe, muestra el compromiso global frente al tema, sin embargo, debemos tener presente que las estrategias de los países a diferencia de las estrategias corporativas incluyen dentro de su desarrollo variables permeadas por situaciones enmarcadas en factores sociales y en el ámbito económico global, las cuales efectivamente tienen un peso importante al momento de la planeación, situaciones que frente a las estrategias corporativas presentan un peso menor, indicándonos que, aunque son variables utilizadas en común, incluyen un factor de ponderación diferente.

Con el fin de desarrollar el documento, tomaremos las estrategias de Reino Unido y de Turquía como base de estudio, estas estrategias tienen como objetivo el desarrollo económico de la sociedad, reflejando, la preocupación de los países autores, en entender, que la ciberseguridad no puede convertirse en un gasto o una carga económica, sino, que al contrario, la ciberseguridad puede y busca ser un trampolín para que los diferentes sectores productivos del país, en mayor o menor medida, puedan generar dinamismo económico.

Abordando entonces estrategias de ciberseguridad maduras y enfocando el análisis al descubrimiento de variables de composición de la estrategia, detallemos la estrategia del Reino Unido conocida como *NATIONAL CYBER SECURITY STRATEGY 2016-2021* y la estrategia de la

Republica de Turquía conocida como *NATIONAL CYBER SECURITY STRATEGY AND 2013-2014 ACTION PLAN.*

6.1 Estrategia Reino Unido

En su introducción se plantea de manera explícita que el futuro y la prosperidad del reino Unido descansa en los fundamentos tecnológicos, y, que lo demás, es, por tanto, construir una sociedad digital resistente a las ciber amenazas, equipada con el conocimiento y las habilidades para explotar las oportunidades del mundo digital, con conocimiento suficiente para manejar el riesgo. Esta introducción en la estrategia, nos pone en el contexto claro que el futuro para el Reino Unido es tecnológico y que la tecnología es la base de la prosperidad, y a su vez, la base de la sociedad, en este caso la tecnología es un bien supremo y toda gira en torno a ella.

Su estrategia se plantea un camino hasta el año 2021 donde quiere llegar a ser un país seguro, resistente a las ciber amenazas próspero y confiado en el mundo digital y toma como conceptos fundamentales para llegar a ello, la defensa, el desalentar y el desarrollar. De esta forma el Reino unido quiere transitar por el mundo digital sin problemas, pensando que para ello se debe poder defender de manera pasiva o activa frente a las amenazas, debe desalentar el actuar de las amenazas contra el Reino Unido y debe desarrollar sus propias tecnologías seguras.

Con este fin, la estrategia hace una definición de ciberseguridad que se adapta a su visión. "Ciberseguridad se refiere a la protección de la información, sistemas (hardware, software e infraestructura asociada), los datos sobre ellos y los servicios que brindan, por acceso no autorizado, daño o mal uso, incluyendo el daño causado intencionalmente por el operador del sistema o accidentalmente como resultado de no seguir los procedimientos de seguridad". Esta

definición permite entonces encajar de manera activa los conceptos de desalentar y de desarrollar, todos ellos enfocados a servir a la ciberseguridad, ciber defensa, ciber desaliento y ciber desarrollo.

Luego, la estrategia de ciberseguridad, clasifica los vectores de ataque de una manera simple: Delitos ciber dependientes y delitos tradiciones fortalecidos con tecnologías cibernéticas. Situación que claramente le permite al ámbito legal poder juzgar los delitos tecnológicos bajo las leyes tradiciones de delitos comunes adicionándoles el agravante ciber.

Con los vectores ya clasificados, la estrategia ahora relata los orígenes de los vectores que para ella tienen una relevancia clave, clasificándolos en cuatro grupos: Grupos Rusos, grupos dentro del Reino unido, grupos de Asia y grupos de África Occidental. Así pues, la estrategia ahora tiene un norte defensivo claro, lo que permite priorizar los recursos financieros y operacionales del estado frente a las múltiples amenazas.

Apalancando los vectores y ahora los orígenes de los vectores, la estrategia le entrega los roles y las responsabilidades a cada uno de los actores de la sociedad, individuos, empresas y gobierno. Al clasificar a los responsables, el Reino Unido aterriza la estrategia como un fin nacional, donde todos deben participar y retira del gobierno la gran responsabilidad de cumplimiento de la misma, distribuyéndola en la nación como un todo.

Luego, la estrategia define los pasos que va a tomar para que todos los actores se puedan involucrar: Apalancamientos e incentivos, coordinación basada en la inteligencia entre las diferentes agencias del estado, desarrollo e implementación de nuevas tecnologías de ciberseguridad, creación de un único centro de ciberseguridad (NCSC). Este despliegue de medidas de manera contundente le entrega a la estrategia los recursos operacionales y tácticos para poder llevar a cabo su visión y la aterriza sobre un gran interesado (NCSC) que de manifiesto toma la responsabilidad de ejecución de la estrategia.

Para apoyar la estrategia y evitar inconvenientes con sus actores relevantes, se plantea la clasificación y el trabajo directo entre el CNI las Empresas y los ciudadanos que sean considerados críticos para el país. De igual forma y con el fin de poder tener información frente a los resultados de la estrategia, se crean parámetros de medición frente a eventos y amenazas cibernéticas. Con estas actividades finales se garantiza de manera detallada el alcance de las labores de las partes y se toman las métricas que a la final son las únicas que realmente permiten medir la efectividad del trabajo de manera cuantitativa.

6.2 Estrategia Turquía

En su introducción se plantea la formación de un ecosistema de seguridad cibernética que sea competitivo internacionalmente, que contribuya con la riqueza y la seguridad de sociedad, con un eficiente crecimiento económico nacional. De esta forma, Turquía ubica la estrategia no como el todo para su sociedad, sino, como una parte que ayuda al crecimiento de la sociedad, que se describe, como una sociedad, tradicional.

Su estrategia se basa en las actividades desarrolladas desde el 2013 enfocadas a ser culminadas en el 2019. Esto evidencia que muchos pasos, aunque fueron dados de manera organizada, estaban descentralizados y al vincularlos en una estrategia, los mismos alimentaron la planeación de la misma.

Turquía, previamente había definido términos como Sectores de infraestructura crítica, ciberespacio nacional, servicios críticos, productos críticos, ciber incidente, ciber ataque, perímetro de seguridad, ciber seguridad nacional. Estas definiciones le permiten entonces a Turquía crear planes basados en su visión entorno a la ciber seguridad, situación que le facilita personalizar su

actuar frente a los incidentes, reconociendo los mismos ya en un espacio reducido y clasificado. De esta forma, Turquía obtuvo una conciencia situacional temprana, que le permitió, desarrollar sus planes a futuro de manera coordinada con el sector privado.

Con las definiciones ya estructuradas, la estrategia entonces define en tres, las actividades que debe desarrollar: Garantizar la seguridad, confidencialidad y privacidad de los servicios y transacciones realizadas a través de medios de tecnologías de la información, Determinar las acciones a tomar para minimizar los efectos de los incidentes de seguridad y desarrollar tecnologías y productos que garanticen la ciberseguridad y en caso contrario si se deben adquirir productos de terceros que los mismos sean usados de manera segura. Así entonces, la estrategia delimito sus alcances y limitó sus debilidades frente al entorno cibernético global.

La estrategia relaciona los riesgos a los que se enfrenta, referenciando y clasificando diez riegos, lo que le permite entonces a la estrategia, enfocar sus recursos operacionales y financieros, y, a su vez, le permite obtener, mediciones de efectividad.

La estrategia culmina determinando los actores responsables, definiendo así tres grandes actores; miembros del comité de ciber seguridad, las instituciones encargadas de la regulación y supervisión y los sectores cubiertos por el CIRT. De esta forma, se vincula a la nación y a sus diferentes actores frente a la responsabilidad de ejecución de la estrategia y se descarga del gobierno la total responsabilidad frente a los resultados.

Así entonces, finalizando este aparte y extrayendo los factores comunes entre las estrategias, se crea una matriz de relación de variables mayores, estas variables son acciones de carácter macro que son usadas en las estrategias y que tiene cabida en el ámbito militar, en el ámbitos político y en el ámbito empresarial, y variables menores, que relacionan actividades específicas, que sumadas, soportan a las actividades macro, y que de manera cuantitativa, ayudan a la medición sobre la efectividad de la implementación y el desarrollo de la estrategia.

Se puede decir entonces, que a partir de la revisión de la información entregada por el GCI, ya expuesta previamente, sumándole a esta, la identificación y descripción detallada de dos países, Reino Unido y Turquía, que vinculan de manera medular su estrategia de ciberseguridad en el desarrollo económico de sus territorios, se puede extraer que los factores (entendidos como un elemento, circunstancia, influencia, que contribuye a producir un resultado) de mayor nivel de relevancia que permiten entender cómo la ciberseguridad impacta o afecta el andamiaje económico de los territorios se presentan en la Tabla 5:

Tabla 5. Factores Relevantes

FACTORES RELEVANTES		
Construcción de Defensas	Determinación de los Lineamientos Estratégicos	Creación de Campañas Menores Dentro de la Estrategia
Identificación de las Fuerzas Competitivas	Determinación de las Líneas de Acción	Creación y Aplicación de Legislación
Identificación de la Posición en un Sector	Determinación de la Posición Única	Creación y Aplicación de Regulaciones
Identificación de las Modificaciones en las Fuerzas	Medición del Compromiso Individual	Creación y Aplicación de Estándares
Resistencia a Ciber Amenazas	Obtener Conocimiento Digital	Creación de Agencias Especializadas
Confianza en el Mundo Digital	Obtener Habilidad Digital	Desalentar al enemigo
Ecosistema de Seguridad	Obtener Manejo del Riesgo	Confidencialidad de los Servicios
Desarrollar Tecnologías	Incidentes de Seguridad	Privacidad de los servicios
	Minimizar los Efectos de los Incidentes	Confidencialidad de las Transacciones
		Privacidad de las Transacciones

Elaboración Propia basada en GCI y Estrategias de Ciberseguridad de Turquía y Reino Unido

Estos factores, son la base para la construcción de variables, entendiendo que un Factor se define según la real academia de la lengua como:

Del lat. factor, -ōris 'el que hace'.

1. *Elemento o causa que actúan junto con otros*
2. *Cada una de las cantidades o expresiones que se multiplican para obtener un pro ducto*

Y una variable se define según la real academia de la lengua como:

Del lat. variabĭlis.

1. *adj. Que varía o puede variar.*
2. *adj. Inestable, inconstante y mudable.*
3. *adj. Gram. Dicho de una palabra: Que admite flexión.*
4. *f. factor (elemento o causa). Un proceso en el que intervienen diversas variables*
5. *f. Mat. Magnitud que puede tener un valor cualquiera de los comprendidos en un conjunto*

Por tanto, haciendo una relación interpretativa entre factor y variable podemos determinar que ambos términos cuentan con una similitud referencial, un Factor. definido como un elemento o causa que actúa junto a otros y una variable, definida como un elemento o causa en un proceso en el que intervienen diversas variables. De esta forma, los elementos *factores relevantes* relacionados en la tabla 5. Podrán por tanto ser elementos "*variable*". Que se transformarán, un insumo matemático, que será usado de manera determinante posteriormente en este trabajo de investigación.

Entendiendo que no todas las variables afectan de la misma manera un modelo matemático o lógico donde son utilizadas, Se llevará a cabo un ejercicio de metodología de análisis estructural, que permitirá determinar las variables claves. En la tabla 5 se relacionaron 27 *factores relevantes* que ahora son 27 *variables,* las cuales se relacionan a continuación etiquetándolas para fines prácticos con la sigla V#

1. *Confianza en el Mundo Digital (V1)*
2. *Confidencialidad de las Transacciones (V2)*
3. *Confidencialidad de los Servicios (V3)*
4. *Construcción de Defensas (V4)*
5. *Creación de Agencias Especializadas (V5)*
6. *Creación de Campañas Menores Dentro de la Estrategia (V6)*

7. *Creación y Aplicación de Estándares (V7)*
8. *Creación y Aplicación de Legislación (V8)*
9. *Creación y Aplicación de Regulaciones (V9)*
10. *Desalentar al enemigo (V10)*
11. *Desarrollar Tecnologías (V11)*
12. *Determinación de la Posición Única (V12)*
13. *Determinación de las Líneas de Acción (V13)*
14. *Determinación de los Lineamientos Estratégicos (V14)*
15. *Ecosistema de Seguridad (V15)*
16. *Identificación de la Posición en un Sector (V16)*
17. *Identificación de las Fuerzas Competitivas (V17)*
18. *Identificación de las Modificaciones en las Fuerzas (V18)*
19. *Incidentes de Seguridad (V19)*
20. *Medición del Compromiso Individual (V20)*
21. *Minimizar los Efectos de los Incidentes (V21)*
22. *Obtener Conocimiento Digital (V22)*
23. *Obtener Habilidad Digital (V23)*
24. *Obtener Manejo del Riesgo (V24)*
25. *Privacidad de las Transacciones (V25)*
26. *Privacidad de los servicios (V26)*
27. *Resistencia a Ciber Amenazas (V27)*

Estas variables mediante un proceso de juicio, y, como primer paso para llevar a cabo la metodología planteada, fueron relacionadas con el fin de obtener una matriz de interacción, donde el número 3 nos da una relación Fuerte, el número 2 una relación Media y el número 1 una relación Débil, tal como se presenta en la Imagen 2. y como se apoya con el Anexo 1.

		V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	V14	V15	V16	V17	V18	V19	V20	V21	V22	V23	V24	V25	V26	V27
V1	Confianza en el Mundo Digital		3	1	3	3	3	3	3	1	2	3	3	2	3	2	2	2	3	3	3	3	3	3	2	2	3
V2	Confidencialidad de las Transacciones	3		1	3	1	1	3	1	2	2	2	2	1	3	3	2	3	2	3	3	2	2	2	2	2	2	2
V3	Confidencialidad de los Servicios	3	1		3	1	1	3	1	2	2	2	1	1	3	3	2	3	2	3	3	2	2	2	2	2	2	2
V4	Construcción de Defensas	2	1	2		3	2	2	2	1	2	3	3	2	2	2	3	3	2	2	2	3	3	3	3	2	1	3
V5	Creación de Agencias Especializadas	3	1	2	1		1	3	3	3	3	3	3	2	3	3	3	3	2	1	2	3	3	3	3	2	1	3
V6	Creación de Campañas Menores Dentro de la Estrategia	3	2	1	1	3		1	1	3	3	1	1	1	3	1	1	2	3	1	3	3	3	2	2	1	1	2
V7	Creación y Aplicación de Estándares	3	3	3	3	3	3		3	3	3	3	3	3	3	3	3	3	3	1	2	3	3	3	3	2	1	3
V8	Creación y Aplicación de Legislación	3	3	3	3	3	3	3		3	3	3	3	3	3	3	3	3	3	1	2	3	3	3	3	2	1	3
V9	Creación y Aplicación de Regulaciones	3	3	3	3	3	3	3	3		3	3	3	3	3	3	3	3	3	1	2	3	3	3	3	2	1	3
V10	Desalentar al enemigo	1	3	2	3	3	3	2	3	2		3	3	2	1	2	2	2	2	1	2	2	2	2	2	1	1	2
V11	Desarrollar Tecnologías	1	3	1	3	3	1	3	2	1	2		3	3	1	2	2	2	2	2	1	2	2	3	2	1	1	3
V12	Determinación de la Posición Única	1	1	1	2	2	1	3	2	2	1	3		3	2	2	1	1	2	3	1	1	3	3	3	1	2	3
V13	Determinación de las Líneas de Acción	1	1	2	3	3	1	3	2	2	1	2	2		2	2	2	2	2	3	1	1	3	3	3	1	2	3
V14	Determinación de los Lineamientos Estratégicos	1	1	2	3	3	2	3	2	2	2	2	2	3		2	2	2	2	3	1	1	3	3	3	1	2	3
V15	Ecosistema de Seguridad	2	1	3	3	2	1	2	2	1	1	3	3	2	2		2	2	2	2	2	3	3	3	3	2	2	3
V16	Identificación de la Posición en un Sec	1	1	3	2	1	2	2	3	2	2	2	3	1	3	2		2	2	2	1	2	3	3	2	1	1	2
V17	Identificación de las Fuerzas Competiti	1	2	2	3	2	1	1	3	1	3	2	3	2	2	2	2		2	2	1	2	3	3	3	1	1	3
V18	Identificación de las Modificaciones en las Fuerzas	1	1	2	3	2	1	1	3	2	3	2	3	2	2	2	2	3		2	2	2	3	3	3	1	1	3
V19	Incidentes de Seguridad	1	1	2	2	2	3	2	3	2	3	3	2	1	1	3	1	2	1		2	3	2	2	2	2	2	2
V20	Medición del Compromiso Individual	2	1	1	2	2	3	1	1	1	3	1	1	1	1	3	1	1	1	2		3	1	2	1	1	3	1
V21	Minimizar los Efectos de los Incidente	1	2	1	3	2	1	2	3	2	3	3	1	1	2	3	1	1	2	3	3		2	2	3	2	2	1
V22	Obtener Conocimiento Digital	2	1	3	1	2	3	3	1	2	2	3	2	2	2	2	2	1	1	2	3	3		2	3	1	2	2
V23	Obtener Habilidad Digital	2	2	3	1	3	3	3	2	2	3	3	2	2	2	3	2	2	3	2	3	3	3		3	1	2	2
V24	Obtener Manejo del Riesgo	1	3	3	1	3	3	3	1	2	3	1	2	2	2	2	2	2	3	3	3	2	3	3		1	2	2
V25	Privacidad de las Transacciones	3	3	2	3	2	1	3	3	1	2	3	2	1	2	2	2	1	3	2	2	3	2	2	2		3	1
V26	Privacidad de los servicios	3	2	2	3	2	2	3	3	1	2	3	2	1	2	2	2	1	2	2	2	2	2	2	2	3		1
V27	Resistencia a Ciber Amenazas	2	2	1	3	3	3	2	3	3	3	3	3	2	2	3	2	2	3	3	3	2	3	3	3	2	2	

Imagen 2. Matriz de iteración variables de impacto de países. Fuente: Elaboración propia, (2020)

Como segundo paso, para llevar a cabo la metodología planteada, se alimenta el *Software MIC MAC,* como se presenta en la Imagen 3, con la matriz de interacción, como resultado, el software nos arroga entre otros datos, el gráfico de influencias indirectas potenciales, el cual relaciona mediante el uso de líneas de conexión y la identificación de colores la influencia existente entre las variables y sus influencias, clasificadas como: más débiles, débiles, medias, relativamente importantes, más importantes.

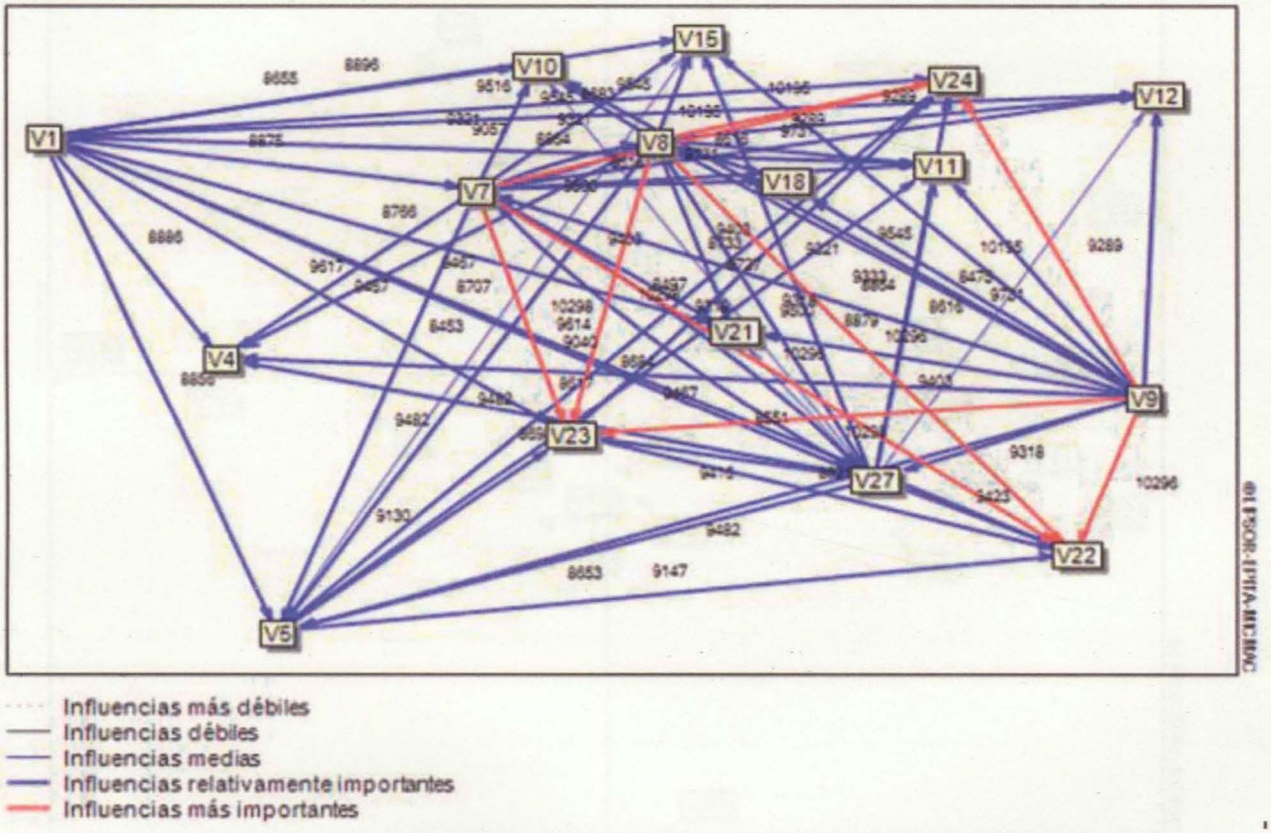


Imagen 3. Gráfico de Influencias Indirectas Potenciales Fuente: Elaboración propia a partir del Reporte Software MIC MAC LIPSOR EPITIA, (2020)

Así, el gráfico de influencias indirectas potenciales que arroja el software da una luz referente a la influencia que tiene las variables V22, V9 V24, V8, V7, V23. Que identifican los siguientes factores:

Obtener Conocimiento Digital (V22)
Creación y Aplicación de Regulaciones (V9)
Obtener Manejo del Riesgo (V24)

Creación y Aplicación de Legislación (V8)
Creación y Aplicación de Estándares (V7)
Confidencialidad de los Servicios (V3)

Sin embargo, la herramienta de software proporciona un plano cartesiano, ver Imagen 4, que permite identificar de mejor manera la influencia de la variable vs la dependencia de la misma.

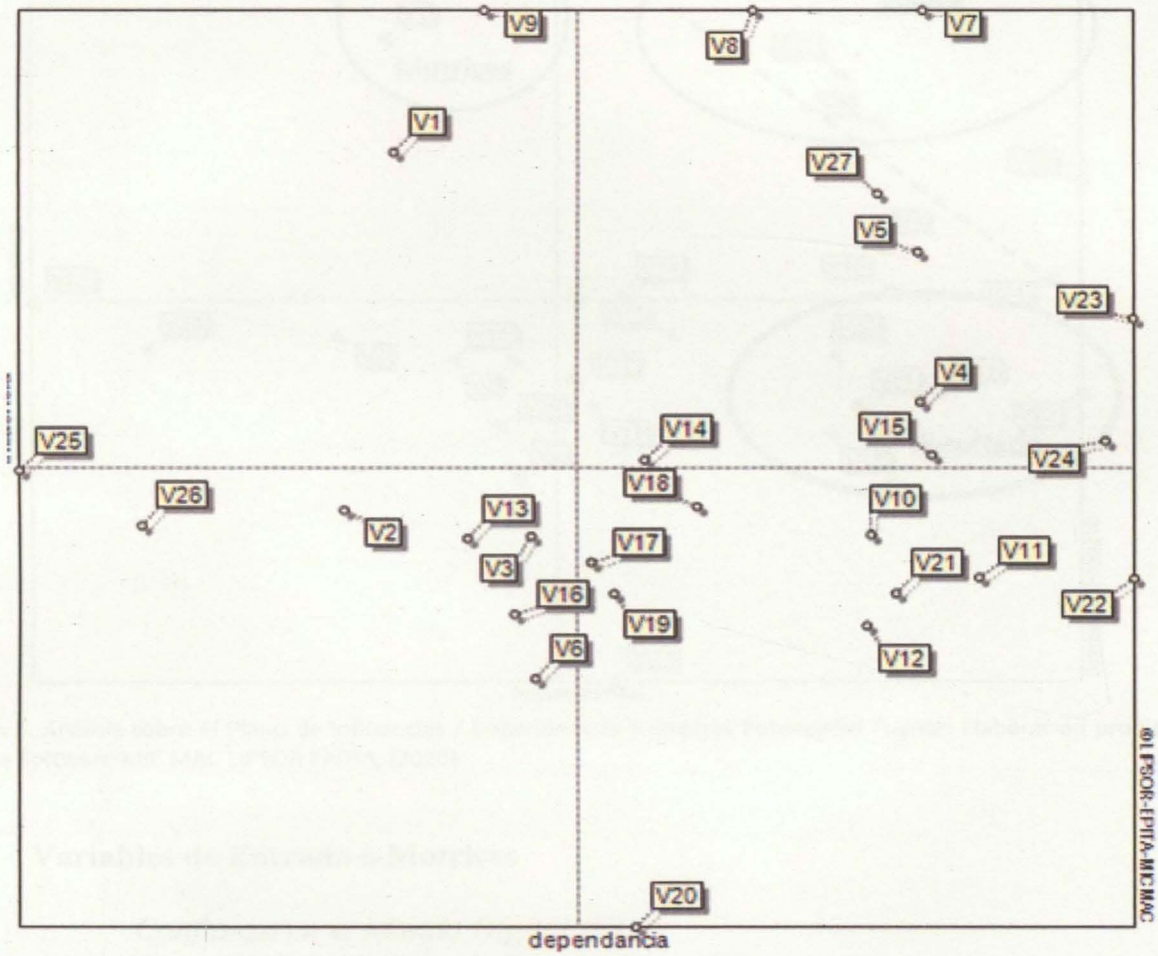


Imagen 4. Plano de Influencias / Dependencias Indirectas Potenciales Fuente: Elaboración Propia a partir del Reporte Software MIC MAC LIPSOR EPITIA, (2020)

Y utilizando la metodología de análisis "*Relación de expertos de Godet",* identificamos y clasificamos en el plano las siguientes variables como *variables motrices, variables de enlace y variables de resultado,* las cuales son críticas para el ejercicio que se está llevando a cabo, pues

permitirán ajustar de mejor manera el resultado del modelo matemático que se está construyendo, tal como se muestra en la Imagen 5.

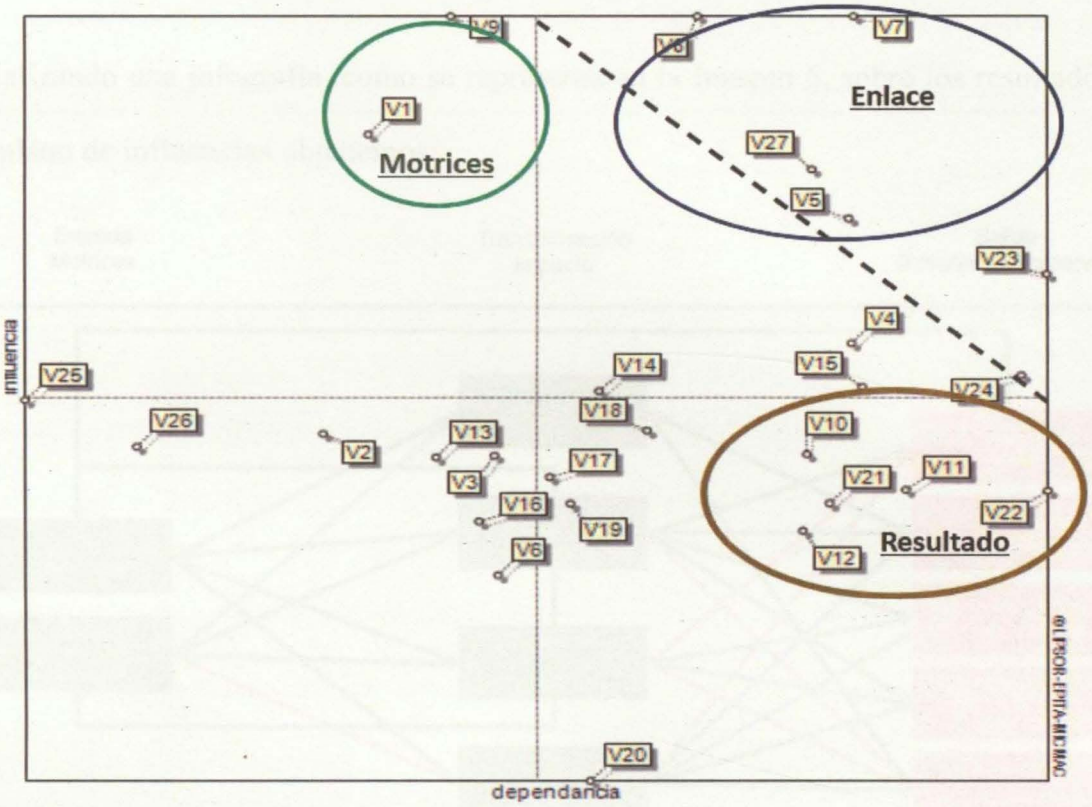


Imagen 5. Análisis sobre el Plano de Influencias / Dependencias Indirectas Potenciales Fuente: Elaboración propia a partir del Reporte Software MIC MAC LIPSOR EPITIA, (2020)

Variables de Entrada o Motrices

Confianza en el Mundo Digital (V1)
Creación y Aplicación de Regulaciones (V9)

Variables de Enlace, Transformación o Impacto

Creación de Agencias Especializadas (V5)
Creación y Aplicación de Estándares (V7)
Creación y Aplicación de Legislación (V8)
Resistencia a Ciber Amenazas (V27)

Variables de Salida, Resultado o Evidencia

Desalentar al enemigo (V10)
Desarrollar Tecnologías (V11)
Determinación de la Posición Única (V12)
Minimizar los Efectos de los Incidentes (V21)
Obtener Conocimiento Digital (V22)

Realizando una infografía, como se representa en la Imagen 6, sobre los resultados obtenidos en el plano de influencias obtenemos:

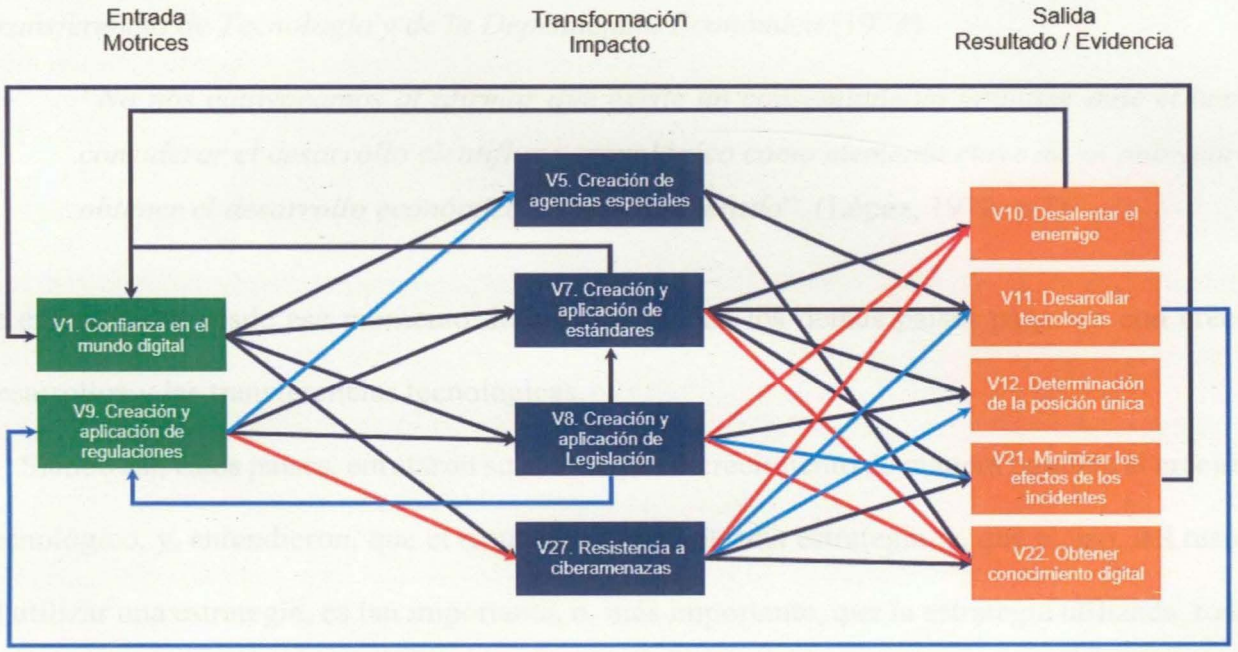


Imagen 6. Infografía sobre el Plano de Influencias Fuente: Elaboración Propia, (2020)

Como conclusión, entones se relacionará, para el modelo que estamos construyendo, que la variable V1 tendrá un peso de 4 y la variable V9 tendrá un peso de 4.5. La variable V5, tendrá un peso de 3 y las variables V7, V8, V27 tendrán un peso de 3.5. Y las Variables V10, V22 tendrán un peso de 2.5 y las variables V11, V12, V21 tendrán un peso de 2. Dejando claro que las demás variables del ejercicio son importantes, pero no proporcionarán para el modelo un peso diferente a 1.

7 Identificación y Estimación del Nivel de Impacto Económico Luego de la Implementación de una Estrategia de Ciberseguridad

Los países que entendieron que sobre la estrategia del desarrollo tecnológico se encontraba el desarrollo de la economía, lograron de manera vertical expresar su forma de relacionamiento con el resto de países del mundo, como lo indicó Arcesio López en su artículo, *Acerca de la Transferencia de Tecnología y de la Dependencia Económica* (1972)

> *"No nos equivocamos al afirmar que existe un consentimiento unánime ante el hecho de considerar el desarrollo científico y tecnológico como elemento clave de un país que desee obtener el desarrollo económico y social acelerado*". (López, 1972, p 7)

se entendía ya, desde ese momento de la historia, que los demás países pagarían con creces los desarrollos y las transferencias tecnológicas.

Siendo así, estos países, enrutaron su estrategia de crecimiento de manera paralela al crecimiento tecnológico, y, entendieron, que el resultado de utilizar una estrategia, y, que el uso, del resultado, al utilizar una estrategia, es tan importante, o, más importante, que la estrategia utilizada, toda vez, que el resultado, define el futuro y enmarca el nuevo escenario, convirtiéndolo, en el principal recurso de la estrategia futura. Poder proyectar el resultado con anterioridad e imaginar en cómo usarlo, permite cimentar de manera clara un entorno que llevará a crear caminos duraderos en el tiempo. Como lo indica Teresa Gamboa, Medelein Arellano y Yuneska Nava en su artículo *Actores y Fines de las Estrategias Empresariales una reflexión desde las Pequeñas y Medianas Empresas* (2003) toda estrategia tiene un fin que si se cumple se convertirá en la nueva posición inicial de donde parte la nueva estrategia.

Con el fin de verificar esta idea, se revisarán los resultados de crecimiento anual de las exportaciones de bienes y servicios que presentaron algunos países en el mundo, previamente se había tratado la información de Brasil, de Austria, de Canadá, de Egipto, de Camerún, de Papua New Guinea, de Filipinas, Reino Unido y de Turquía. De esta forma es conveniente realizar sobre estos mismos países un ejercicio comparativo, utilizando la información suministrada por *The Global Economy.* Como marco referencial inicial, se tomará lo expresado por Arcesio López en 1972, avanzando así, hasta tiempos recientes sobre los cuales exista información condensada de cada uno de los países como se relaciona en la Tabla 6.

La definición que da Global Economy a la **Tasa de crecimiento anual de las exportaciones de bienes y servicios** es: Las exportaciones de bienes y servicios representan el valor de todos los bienes y otros servicios de mercado prestados al resto del mundo. Incluyen el valor de mercancías, fletes, seguros, transporte, viajes, regalías, derechos de licencia y otros servicios, como servicios de comunicación, construcción, financieros, de información, comerciales, personales y gubernamentales. Excluyen la remuneración de los empleados y los ingresos por inversiones (anteriormente llamados servicios de factores) y los pagos de transferencia.

Tabla 6. Indicadores de Resultado por Países Año 1972 - 1977

Crecimiento Exportaciones de Bienes y Servicios	Brasil	Austria	Canadá	Egipto	Camerón	Papua New Guinea	Pilipinas	Reino Unido	Turquía
1972	24.16	10.15	8.64	-1.75	5	54.61	12.49	1.08	
1973	14.25	5.44	10.09	4.41	2.61	39.82	16.05	12.31	
1974	2.33	10.71	-4.85	4.70	13.67	13.63	-11.41	7.31	
1975	11.57	-2.40	-8.30	23.30	-10.29	-3.50	3.53	-2.96	
1976	-0.32	11.06	7.77	12.38	16.09	-8.72	12.83	9.11	
1977	-0.35	2.39	6.42	40.65	-11.92	3.99	16.41	6.88	

Elaboración Propia Basada en Global Economy, (2020), recuperado de https://www.theglobaleconomy.com/texts_new.php?page=aboutus

Tomando como referencia el año 1980, relacionada en la Tabla 7 , donde el mundo ingreso a una nueva era tecnológica, al dar inicio a las conexiones entre dispositivos como lo indicó el *Information Sciences Institute de University of Southern California*:

Tabla 7. Indicadores de Resultado por Países Año 1981 - 1986

Crecimiento Exportaciones de Bienes y Servicios	Brasil	Austria	Canadá	Egipto	Camerón	Papua New Guinea	Pilipinas	Reino Unido	Turquía
1981	21.32	4.88	1.71	29.70	27.40	5.4	9.48	-0.49	
1982	-9.19	-0-08	-1.38	-10.41	-15.80	-1.63	-10.69	1.11	
1983	14.33	1.58	5.78	7.47	19.58	1.74	3.45	2.01	
1984	21.95	8.32	18.62	5.81	44.27	3.15	4.54	6.74	
1985	7.03	8.95	4.48	1.1	8.91	12.25	-16.07	5.85	
1986	-10.5	-4.05	4.5	1.85	-13.85	12.01	16.91	4.16	

Elaboración Propia Basada en Global Economy, (2020), recuperado de https://www.theglobaleconomy.com/texts_new.php?page=aboutus

Ahora, ya en tiempos modernos como se relaciona en la Tabla 8, donde el desarrollo de las tecnologías basadas en las comunicaciones de dispositivos podemos decir ha madurado a nivel global, encontramos entonces:

Tabla 8. Indicadores de Resultado por Países Año 2012 - 2017

Crecimiento Exportaciones de Bienes y Servicios	Brasil	Austria	Canadá	Egipto	Camerón	Papua New Guinea	Pilipinas	Reino Unido	Turquía
2013	1.83	0.64	2.46	4.52	4.15	-7.58	-0.97	1.18	1.07
2014	-1.57	2.89	6.32	-10.94	5.27	6.61	12.63	1.04	8.15
2015	6.82	3.05	3.42	-0.04	6.37	-6.44	8.48	3.77	4.30
2016	0.86	3.07	1.41	-15.03	-0.63	-8.97	11.62	2.47	-1.87
2017	4.91	5.02	1.41	86.04	-1.59	-3.76	19.66	6.10	11.96
2018	4	5.88	3.08	32.16	2.34	-10.32	13.44	-0.86	7.83

Elaboración Propia Basada en Global Economy, (2020), recuperado de https://www.theglobaleconomy.com/texts_new.php?page=aboutus

A simple vista, la información referenciada entrega resultados dispares,

Tabla *9* , al realizar un promedio de crecimiento, obtenemos una imagen del comportamiento antes de la llegada de Internet, durante el proceso de conocimiento del potencial de Internet y un después que Internet ha madurado en el planeta.

Tabla 9. Promedios Indicadores de Resultado por Países Año 1972 - 2018

Promedio de Crecimiento Exportaciones de Bienes y Servicios	Brasil	Austria	Canadá	Egipto	Camerón	Papua New Guinea	Pilipinas	Reino Unido	Turquía
1972 - 1977	8.61	6.23	3.30	13.95	2.53	16.64	8.32	5.62	
1981 – 1986	7.49	1.95	5.62	5.92	11.75	5.49	1.27	3.23	
2013 - 2018	2.81	3.43	3.02	16.12	2.65	-5.08	10.81	2.28	5.24

Elaboración Propia Basada en Global Economy, (2020), recuperado de https://www.theglobaleconomy.com/texts_new.php?page=aboutus

La información obtenida arroja resultados donde todavía es difícil relacionar el crecimiento económico que brinda la tecnología como lo mencionaba Arcesio López, algunos países muestran un crecimiento significativo y luego muestran un estancamiento o un retroceso igual, llevándonos a determinar que existen factores que efectivamente pueden estar condicionados por vectores diferentes al desarrollo tecnológico que causan un impacto mayor o menor en el rendimiento macroeconómico de un país.

Para determinar entonces una relación directa más efectiva entre crecimiento económico y desarrollo tecnológico, se utilizará el índice de Exportaciones de Bienes y Servicios como porcentaje del PIB, de esta forma se evidenciará de mejor manera la relación existente entre desarrollo tecnológico exportado y crecimiento económico, estos se relacionan en la Tabla 10, Tabla 11, Tabla 12.

Tabla 10. Indicadores de Resultado por Países Año 1972 - 1977

% Exportaciones de Bienes y Servicios Frente al PIB	Brasil	Austria	Canadá	Egipto	Camerón	Papua New Guinea	Pilipinas	Reino Unido	Turquía
1972	7.26	26.93	21.29	12.71	20.39	31.21	19.68	20.62	6.02
1973	8.27	26.92	22.77	13.54	20.69	44.88	24.77	22.43	7.03
1974	8.01	29.11	24.07	20.37	25.44	46.88	25.02	26.8	5.73
1975	7.54	28.09	22.03	18.17	22.68	39.98	21.02	25.38	4.42
1976	7.04	28.75	21.76	17.17	22.64	41.77	19.33	27.99	4.86
1977	7.25	27.95	22.78	21.59	25.06	44.97	21.06	29.65	3.82

Elaboración Propia Basada en Global Economy, (2020), recuperado de https://www.theglobaleconomy.com/texts_new.php?page=aboutus

Tabla 11. Indicadores de Resultado por Países Año 1981 - 1986

% Exportaciones de Bienes y Servicios Frente al PIB	Brasil	Austria	Canadá	Egipto	Camerón	Papua New Guinea	Pilipinas	Reino Unido	Turquía
1981	9.42	33	26.47	30.96	21.87	38.24	23.83	25.96	8.24
1982	7.61	31.74	25.28	26.33	33.21	36.83	20.22	25.62	11.86
1983	11.42	30.48	25.02	22.93	30.40	36.20	21.34	25.75	12.47
1984	13.53	32.75	28.04	20.57	33.48	39.44	24.02	27.52	15.61
1985	12.25	34.92	27.65	18.23	33.45	42.11	24.02	27.88	15.86
1986	8.82	32	27.10	13.83	23.28	43.58	26.33	24.83	13.31

Elaboración Propia Basada en Global Economy, (2020), recuperado de https://www.theglobaleconomy.com/texts_new.php?page=aboutus

Tabla 12. Indicadores de Resultado Por Países Año 2013 - 2018

% Exportaciones de Bienes y Servicios Frente al PIB	Brasil	Austria	Canadá	Egipto	Camerón	Papua New Guinea	Pilipinas	Reino Unido	Turquía
2013	11.74	53.44	30.41	17.02	25.57	26.47	28.02	29.95	22.27
2014	11.01	53.39	31.81	14.24	24.94	65.96	28.91	28.50	23.76
2015	12.9	53.09	31.92	13.18	22.26	21.50	28.40	27.65	23.35
2016	12.47	52.45	31.53	10.35	19.24	51.41	28.10	28.44	21.97
2017	12.52	54.04	31.46	15.82	18.58	58.86	31.02	30.37	24.77
2018	14.89	55.76	32.13	18.91	19.31	58.81	31.68	30.01	29.53

Elaboración Propia Basada en Global Economy, (2020), recuperado de https://www.theglobaleconomy.com/texts_new.php?page=aboutus

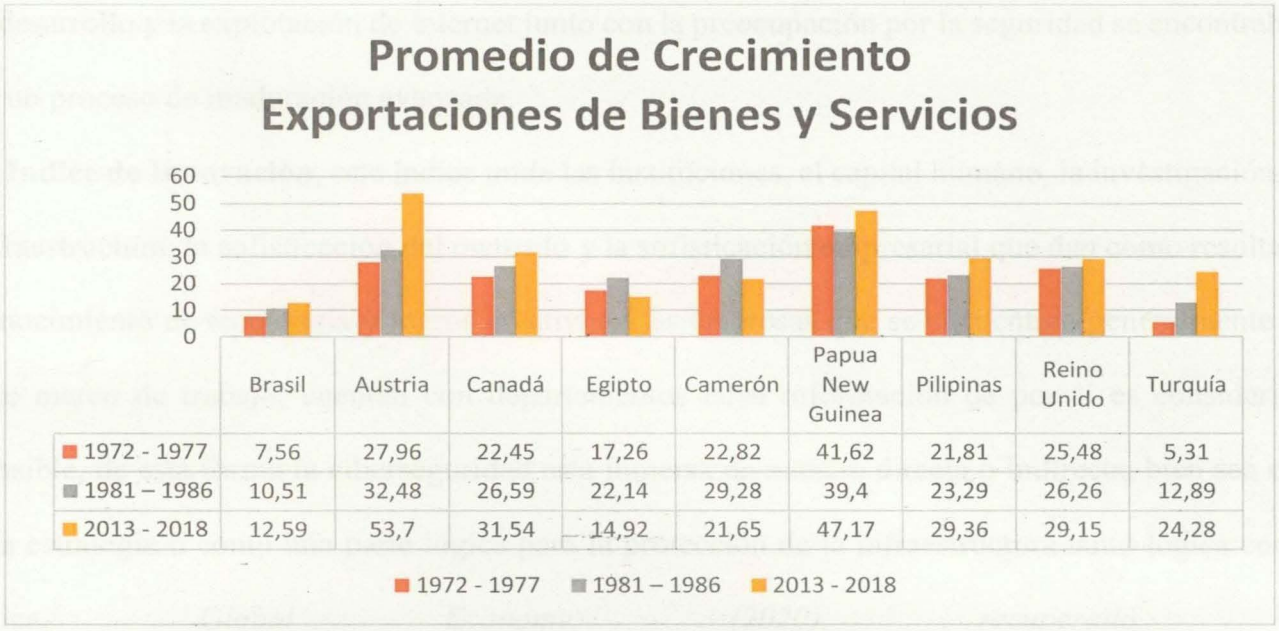
Para determinar la tendencia de cada país y así saber si esta existió, se realizará un promedio por cada ciclo, Tabla 13, el cual fijará las bases determinísticas del aporte de las exportaciones de bienes y servicios al desarrollo económico.

Tabla 13. Promedios Indicadores de Resultado Por Países Año 1972 - 2018

Promedio de Crecimiento Exportaciones de Bienes y Servicios	Brasil	Austria	Canadá	Egipto	Camerón	Papua New Guinea	Pilipinas	Reino Unido	Turquía
1972 - 1977	7,56	27,96	22,45	17,26	22,82	41,62	21,81	25,48	5,31
1981 – 1986	10,51	32,48	26,59	22,14	29,28	39,40	23,29	26,26	12,89
2013 - 2018	12,59	53,70	31,54	14,92	21,65	47,17	29,36	29,15	24,28

Elaboración Propia Basada en Global Economy, (2020), recuperado de https://www.theglobaleconomy.com/texts_new.php?page=aboutus

Con el fin de identificar mejor la información, se relaciona la Imagen 7.



	Brasil	Austria	Canadá	Egipto	Camerón	Papua New Guinea	Pilipinas	Reino Unido	Turquía
1972 - 1977	7,56	27,96	22,45	17,26	22,82	41,62	21,81	25,48	5,31
1981 – 1986	10,51	32,48	26,59	22,14	29,28	39,4	23,29	26,26	12,89
2013 - 2018	12,59	53,7	31,54	14,92	21,65	47,17	29,36	29,15	24,28

Imagen 7. Promedio de Crecimiento Exportaciones de Bienes y Servicios. Elaboración Propia, basada en los datos de https://www.theglobaleconomy.com/texts_new.php?page=aboutus

De esta forma ahora se puede identificar la relación existente entre el crecimiento económico y el desarrollo tecnológico, pues los países en alguna manera han intentado enrutar su economía a bienes y servicios exportables a fin de hacer crecer sus indicadores financieros, de esta forma y para determinar una relación más directa entre el desarrollo tecnológico en el campo de la ciberseguridad y el desarrollo económico, se utilizarán índices más precisos, que con en el ejercicio anterior, permitan determinar la relación existente.

Al no existir un ítem específico sobre exportaciones en tecnologías de ciberseguridad se realizará un acercamiento desde los índices que son afines a la ciberseguridad, adicionando un índice político el cual afecta directamente el desarrollo del país. Se utilizarán entonces como variables de comparación, el índice de innovación, el índice de exportaciones de alta tecnología, el índice de exportaciones de tecnologías de la información y el índice de percepción de la corrupción. Estas variables se relacionarán desde el año 2014 hasta el año 2017 pues en este rango de tiempo

el desarrollo y la explotación de Internet junto con la preocupación por la seguridad se encontraban en un proceso de maduración avanzada.

El Indice de Innovación, este índice mide las instituciones, el capital humano, la investigación, la infraestructura, la sofisticación del mercado y la sofisticación empresarial que dan como resultado conocimiento de tecnología y logros creativos. Las empresas que se encuentran generalmente en este marco de trabajo, cuentan con departamentos cuya información de por si es considerada sensible, de esta forma la ciberseguridad está inmersa de manera directa o indirecta, bien sea con una estrategia o como una parte lógica para la protección de la infraestructura tanto lógica como física. *Global Economy, (2020), recuperado de https://www.theglobaleconomy.com/texts_new.php?page=aboutus*

El Indice de Exportación de Alta Tecnología, en el cual se identifican productos que llevan un componente de I+D alto, tomando como ejemplo la industria aeroespacial, la industria computacional, los productos farmacéuticos, los instrumentos científicos, la maquinaria eléctrica. Esta área de mercado debido a las cualidades de los productos que genera y a los métodos científicos o industriales utilizados para conseguirlos, aplica igual que el marco anterior, seguridad sobre sus activos lógicos y físicos, Se entiende que la información relacionada con el saber cómo es crítica y que la misma es continuamente buscada y deseada por actores negativos del entorno. *Global Economy, (2020), recuperado de https://www.theglobaleconomy.com/texts_new.php?page=aboutus*

El Indice de Exportación de Tecnologías de la Información, se relaciona como un porcentaje frente a las exportaciones totales y se identifican bienes como computadoras, equipos periféricos, equipos de comunicación, equipos electrónicos de consumo, componentes electrónicos. Su relación con la tecnología es directa y las empresas que desarrollan sus actividades sobre esta vertical procesan información sensible y desarrollan procesos que de alguna manera se buscan proteger

frente a la competencia con el fin de mantener una delantera comercial, apoyados en la generación de nuevas necesidades o con productos modernos y diferenciales. *Global Economy, (2020), recuperado de https://www.theglobaleconomy.com/texts_new.php?page=aboutus*

El Indice de Percepción de la Corrupción, mide la percepción de la corrupción del sector público, es decir la corrupción administrativa y la corrupción política. Su relación con la tecnología no se entiende de manera directa, sin embargo, el uso de la tecnología por parte del estado en sus procesos elimina el factor humano, lo cual es sentido por la sociedad como algo que permite limitar la corrupción, de igual forma, al funcionar el estado en entornos digitales permite que el mercado local cree, desarrolle y aplique tecnologías para la protección de estos entornos digitales. *Global Economy, (2020), recuperado de https://www.theglobaleconomy.com/texts_new.php?page=aboutus*

Estos índices, representados en la Tabla 14,

Tabla *15*, Tabla 16, Tabla 17, en general, se pueden ver afectados por diferentes factores, estados, instituciones, empresas o individuos, como fueron determinados previamente dentro de las fuerzas competitivas (Porter, 1979) que para este caso de estudio podrían llegar a identificar de manera simple o de manera más profunda la ciberseguridad como un elemento fundamental del actuar cotidiano y de igual forma podrían entender la ciberseguridad como una parte natural del ecosistema tecnológico, bien sea utilizando y llevando la ciberseguridad de manera ordenada como estrategia en su entorno o de manera natural como un medio de defensa.

Tabla 14. Indicadores de Resultado por Países Año 2017

MD: Millones de Dólares	Brasil	Austria	Canadá	Egipto	Camerón	Papua New Guinea	Pilipinas
Índice de Innovación	33.8	50.9	53.9	27.5	23.9	-	36.2
Exportación Alta tecnología MD	9.924	12.943	24.220	72	28,6	-	32.114
Exportación Tecnologías de la Información	0.36	3.48	1.95	2.88	0.05	-	35.87
Percepción de Corrupción	37	75	82	32	25	29	34

Elaboración Propia Basada en Global Economy, (2020), recuperado de https://www.theglobaleconomy.com/texts_new.php?page=aboutus

Tabla 15. Indicadores de Resultado por Países Año 2016

MD: Millones de Dólares	Brasil	Austria	Canadá	Egipto	Camerón	Papua New Guinea	Pilipinas
Índice de Innovación	33.2	53.1	54.7	26	22.8		31.8
Exportación Alta tecnología MD	9,775	15,499	23.974	52	11.4		26.139
Exportación Tecnologías de la Información	0.39	3.79	2.12	2.7	0.03		43.21
Percepción de Corrupción	40	75	82	34	26	28	35

Elaboración Propia Basada en Global Economy, (2020), recuperado de https://www.theglobaleconomy.com/texts_new.php?page=aboutus

Tabla 16. Indicadores de Resultado por Países Año 2015

MD: Millones de Dólares	Brasil	Austria	Canadá	Egipto	Camerón	Papua New Guinea	Pilipinas
Índice de Innovación	34.9	54.10	55.7	28.9	27.8		31.10
Exportación Alta tecnología MD	8.848	15.947	26.318	88.3	13.3		26.192
Exportación Tecnologías de la Información	0.45	4.12	2.14	3.7	0.03		42.91
Percepción de Corrupción	38	76	83	36	27	25	35

Elaboración Propia Basada en Global Economy, (2020), recuperado de https://www.theglobaleconomy.com/texts_new.php?page=aboutus

Tabla 17. Indicadores de Resultado por Países Año 2014

MD: Millones de Dólares	Brasil	Austria	Canadá	Egipto	Camerón	Papua New Guinea	Pilipinas
Índice de Innovación	36.3	53.4	56.1	30	27.5		29.9
Exportación Alta tecnología MD	8.228	19.269	26.552	176.3	26.7		23.838
Exportación Tecnologías de la Información	0.39	4.28	1,93	2.84	0.03		34.62
Percepción de Corrupción	43	72	81	37	27	25	38

Elaboración Propia Basada en Global Economy, (2020), recuperado de https://www.theglobaleconomy.com/texts_new.php?page=aboutus

Igual que anteriormente se abrió un espacio para analizar al Reino Unido frente a Turquía, se abre un espacio para realizar un análisis entre los indicadores de las dos estrategias la estrategia del

Reino unido y la estrategia de Turquía adicionando a este ejercicio un ítem nuevo, usuarios de Internet, que podría ser relevante para apoyar la extracción de conclusiones como se referencian en la Tabla 18 y la

Tabla *19* respectivamente.

Tabla 18. Indicadores de Resultado Reino Unido 2013 - 2019

Reino Unido							
	2019	**2018**	**2017**	**2016**	**2015**	**2014**	**2013**
Índice de Innovación	61.3	60.10	60.9	61.9	62.4	62.4	61.3
Exportación Alta tecnología MD		70.158	68.625	68.279	69.417	70.652	69.223
Exportación Tecnologías de la Información			4.25	4.5	4.1	4.16	3.82
Percepción de Corrupción		80	82	81	81	78	76
Usuarios de Internet %			94.62	94.62	92	91.61	89.84

Elaboración Propia Basada en Global Economy, (2020), recuperado de https://www.theglobaleconomy.com/texts_new.php?page=aboutus

Tabla 19. Indicadores de Resultado Turquía 2013 - 2019

Turquía							
	2019	**2018**	**2017**	**2016**	**2015**	**2014**	**2013**
Índice de Innovación	36.9	37.4	38.0	39	37.8	38.2	36
Exportación Alta tecnología MD			3.052	2.182	2.323	2.346	2.176
Exportación Tecnologías de la Información			1.25	1.35	1.47	1.52	1.45
Percepción de Corrupción		41	40	41	42	45	50
Usuarios de Internet %			64.68	58.35	53.74	51	46.25

Elaboración Propia Basada en Global Economy, (2020), recuperado de https://www.theglobaleconomy.com/texts_new.php?page=aboutus

De igual forma se tendrá presente un ítem adicional que proviene del estudio de *ABI Research* donde para el año 2013 posicionan al Reino Unido en el puesto número cinco y Turquía en el puesto número siete frente a la implementación de un modelo de ciberseguridad, resaltando que cada uno de los países ha culminado las siguientes actividades referenciadas en la

Tabla *20.*

Tabla 20. Actividades Realizadas Frente a la Ciberseguridad Hasta el Año 2013

	Reino Unido	**Turquía**
Fecha de la información	2013	2013
Legislación dentro del código Penal	SI	SI
Regulación y Cumplimiento	SI	SI
Estándares	SI	NO
Agencia Responsable de la Ciberseguridad Diferente al Ministerio de Comunicaciones	SI	NO

Elaboración Propia Basada en El Estudio Realizado por ABI Research.

Se puede extraer de la información relacionada entonces, que Turquía y el Reino Unido han desarrollado estrategias de ciberseguridad enfocadas en el desarrollo económico, que estas estrategias iniciadas en el año 2013 han venido madurando de diferente manera en cada país y han desembocado en actividades frente a la ciberseguridad que son medibles, su desarrollo económico se ha ligado cada vez más con los bienes y servicios. En el caso de Reino Unido escalando poco a poco en esta relación, fortaleciéndola y obteniendo resultados positivos, por ejemplo, con una gran cobertura de usuarios de internet y una gran confianza en el gobierno, en el caso de Turquía dando impulsos temporales frente a la misma, obteniendo una cobertura de usuarios de internet que la limita frente a la explotación del recurso y de igual forma en alguna medida la inseguridad de los usuarios, se refleja en el índice de corrupción que se mantiene de manera general en un nivel de confianza bajo frente al gobierno.

8 Modelo Matemático que Materializa la Estrategia y el Retorno de Valor

En el mundo, existen diferentes modelos matemáticos que soportan a los indicadores de uso cotidiano y que han ayudado a la humanidad a entender el comportamiento de la economía, el comportamiento de las sociedades, el comportamiento de los ecosistemas, el comportamiento de las estrellas, en general, el modelamiento a partir de la observación, del análisis de datos, de la simulación práctica ha permitido llevarnos a entornos de predicción los cuales en mayor o menor medida han contribuido con el proceso de la generación de historia en nuestra humanidad.

Como ejemplo del uso de modelos matemáticos en la economía tenemos el documento *Global Cibersecurity Index & Ciberwellness Profiles* utilizó como método de evaluación el siguiente modelo matemático:

$$CIc = Iqc \,/\, 34$$
$$Iqc = Rank\,(xqc)$$

Incluyendo de esta forma variables

xqc; Value of the individual indicator q for country c, with q=1,..., Q and c=1,..., M.

Iqc; Normalized value of individual indicator q for country c

CIc; Value of the composite indicator for country c

Elena Escrig Olmedo, Mª Ángeles Fernández Izquierdo, Mª Jesús Muñoz Torres, hacen de manera ordenada y descriptiva una extracción de las variables que componen diferentes índices internacionales, los cuales relacionan en su publicación *Inversión Socialmente Responsable: Criterios de Valoración y Análisis de ISR Seguidos por los Índices y Agencias de Análisis de Sostenibilidad* (2014).

Como ejemplo del uso de modelos matemáticos para medir criterios como la sostenibilidad tenemos el *índice Dow Jones*:

$$TS = SUMATORIA\ (ANS * CRW * QUW)$$

TS: *Puntuación total*
ANS: *Puntuación de la respuesta*
CRW: *Peso o Ponderación del Criterio*
QUW: *Peso o Ponderación de la Pregunta*

La OIT de igual manera aplica y enseña cómo aplicar modelos matemáticos que le permitan a las organizaciones determinar de manera correcta indicadores de gestión, indicadores de resultado, indicadores de efecto, indicadores de impacto etc. cuando en la estrategia se involucran individuos, como ejemplo del uso de modelos matemáticos para medir criterios como el nivel de aprendizaje o de educación podemos tomar:

- ***Costo hora de formación*** *= Valor presupuesto ejecutado / Horas de formación aplicadas*
- ***Variación de Ingresos*** *= ((Ingresos después – Ingresos antes) / ingresos antes) * 100*

Como ejemplo del uso de modelos matemáticos en campos como la biología, se puede tomar la publicación realizada por Maria Gloria Basáñez y Diego J Rodriguez donde se refieren a la dinámica de transmisión y modelos matemáticos de enfermedades trasmitidas por vectores, los autores toman el *modelo de Ross-Macdonald* donde se determinan las variables que componen un vector de infección para luego basados en esta línea base extender el modelo a poblaciones humanas.

$$(dt / dx) = qapy\ (1\text{-}x) - gx$$

"donde los humanos susceptibles (1-x) se infectan con una probabilidad p por picada cuando están expuestos a una tasa de picadas infectantes por persona igual a qay, y los infectados (x) se recuperan con una tasa g por persona"

Teniendo presente entonces, que los modelos matemáticos, o, fórmulas matemáticas, permiten ser modificables para ser adaptados a diferentes entornos, en general y de manera más precisa, para entornos similares o de correspondencia, y, teniendo como referente en este trabajo los factores que pueden convertirse en variables, y, según lo tratado previamente donde se identificó que el uso de modelos matemáticos cuantificables se basan en variables, y, al repasar que los modelos matemáticos propuestos por entidades de carácter global o por estudios con sustento experimental son utilizados de manera general por la sociedad, podríamos determinar entonces que los modelos matemáticos o fórmulas matemáticas son usados con el fin de modelar un caso de uso particular sobre el que se buscan resultados futuristas o de posible reacción ante actividades realizadas, la real academia de la lengua define fórmula como:

1. *f. Medio práctico propuesto para resolver un asunto controvertido o ejecutar algo difícil.*
2. *f. Manera fija de redactar algo.*
3. *f. Composición de una mezcla e instrucciones para su elaboración.*
4. *f. Expresión concreta de una avenencia o transacción entre diversos pareceres, partidos o grupos.*
5. *f. Dep. Categoría de automóviles de competición, cuyos niveles se designan por numerale s. Gran premio deFórmula 1.*
6. *f. Mat. Ecuación o regla que relaciona objetos matemáticos o cantidades.*
7. *f. Quím. Combinación de símbolos químicos que expresa la composición de una molécula.*

Al realizar una abstracción sobre el contenido tratado y refiriéndonos a un entorno tradicional de mercado como lo indica Jorge Eliecer Prieto Herrera en su libro Investigación de Mercados *"la producción, distribución venta y consumidor"* (Herrera, 2013, Pag 3), vemos que los productos o servicios ofertados por las empresas o por los gobiernos, parten de la insuficiencia presente por cubrir una necesidad existente o creada sobre la ciudadanía.

De esta forma, entendemos que entre la idea para satisfacer una necesidad y la entrega del servicio o del producto que satisfagan la necesidad, existen pasos o actividades que al ser sumadas darán un resultado que siempre se busca y espera sea el deseado. Como interpretan C. Burgos, J.-

C. Cortés, D. Martínez-Rodríguez, A. Navarro-Quiles, R.-J. Villanueva en su libro Un Modelo de Oferta y Demanda con Incertidumbre (2019)

> *"En economía, la oferta y la demanda se definen como la cantidad de bienes (o servicios) que los productores están dispuestos a vender a los consumidores o que los consumidores están dispuestos adquirir, en una unidad de tiempo específica."* (Burgos, Corés, Martinez, Navarro, Villanueva, 2019, p 112)

Si bien, las actividades de por si son claves para la ejecución del plan, el esfuerzo y el peso que le demos a las variables es importantes, por ejemplo, entender el mercado global de las materias primas para la producción de cueros es importante, sin embargo, su influencia frente al consumo interno del cuero puede no ser significativa, si en cambio, una tendencia ecologista por el remplazo del cuero por materiales sintéticos puede ser de un impacto alto para las actividades de publicidad, donde se deben entonces demostrar los beneficios ecológicos del uso del cuero frente a los materiales sintéticos.

Como lo indican los autores Tracy y Wierseman (1999) en su libro *"La disciplina de los líderes del mercado*".

> *"Una astuta combinación de Know-How incomparable, aplicación tecnológica y gestión impecable. El secreto para triunfar con esta disciplina de valor se resume con una sola palabra: fórmula"* (Tracy y Wierseman, 1999, p 16).

Entendiendo esto, podemos crear una relación entre una estrategia y un modelo, un modelo con las variables correctas y con el peso de las variables definido de manera correcta es clave para poder llevar una estrategia del mundo calificable al mundo cuantificable.

Para este estudio y con el fin de conseguir la iteración entre las variables de la estrategia y las variables del modelo, se utilizarán las *Actividades Fundamentales Estrategia Ciberseguridad* descritas anteriormente, vs, los *Indicadores de Resultado* asimismo tratados anteriormente y

referenciados en la Tabla 21. El resultado de esta relación se denominará, *Valor Estimado por la Aplicación de una Estrategia de Ciberseguridad,* y, con el fin de ajustar la información al caso de uso de este proyecto de investigación, se reducirán las variables de once a cuatro, teniendo como base de selección que las variables seleccionadas cubran por lo menos un factor Político, un factor legal y un factor técnico

Buscando generar iteraciones, se realizará un ejercicio de interacción de variables, donde se pretende representar la fuerza de lazos que determinen relaciones entre las variables de origen y los indicadores de resultado, expresados en

Tabla *22* , entendiendo que entre todas las variables que componen la estrategia de ciberseguridad existe en alguna medida una relación de dependencia y una relación de causa y efecto frente a la tecnología.

Tabla 21. Indicadores de Resultado

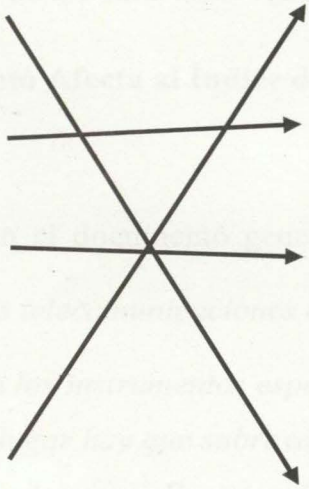
Indice de Innovación	Indice de Exportación de alta tecnología

Indice de exportación de tecnologías de la información	Indice de percepción de la corrupción

Elaboración Propia basada en The Global Economy Fuente; https://es.theglobaleconomy.com/

Tabla 22. Actividades Fundamentales Estrategia Ciberseguridad VS Indicadores de Resultado

Legislación dentro del código Penal	***A***
Regulación y Cumplimiento	***B***
Creación y/o Aplicación de Estándares	***C***
Agencia Responsable de la Ciberseguridad Diferente al Ministerio de Comunicaciones	***D***



m	***Índice de Innovación Puntos***
n	***Índice Exportación Alta Tecnología MD***
o	***Índice Exportación Tecnologías de la Información %***
p	***Índice Percepción de Corrupción Puntos***

Elaboración Propia Basada en GSI y Global Economy

8.1 La Legislación Afecta Directamente al Indice de Percepción de la Corrupción

Esta relación aparece de manera intrínseca en nuestra sociedad, como lo indica Teresa Medina Arnaiz en su artículo *La necesidad de reformar la legislación sobre contratación pública para luchar contra la corrupción: las obligaciones que nos llegan desde Europa.*

> *"Es necesario también corregir las lagunas del marco normativo respecto de las prohibiciones de contratar vinculadas a una condena penal por actos de corrupción, para que éstas puedan explotar su potencial de instrumento de lucha contra estos fenómenos delictivos"* (Arnaiz, 2016, p 108)

O como lo indica Boris Begovic en su artículo Corrupción: conceptos, tipos, causas y consecuencias.

> *"La corrupción viola el estado de derecho, y el estado de derecho es un prerrequisito de la economía de mercado. Si no existe estado de derecho, no hay protección de los derechos de propiedad privada ni cumplimiento de los contratos*". (Begovic, 2005, Pag 7)

8.2 La Regulación y el Cumplimiento Afecta al Indice de Exportación de Alta Tecnología

Como lo indica Marcio Wohlers en el documento generado para la CEPAL *Convergencia tecnológica y agenda regulatoria de las telecomunicaciones en América Latina*

> *"el impacto de convergencia en los instrumentos específicos de la regulación sectorial de telecomunicaciones, en primer lugar hay que subrayar la existencia de una gran cantidad y variedad de instrumentos regulatorios. Enmarcado por un modelo de regulación por incentivos (a ejemplo de los price-caps), estos instrumentos están directamente ligados a la estructura y a la arquitectura de las redes de telecomunicaciones y también a los modelos de formación de precios y tarifas en un entorno de redes"* (Wohlers, 2008, p 22)

Nos muestra que las regulaciones permiten la expansión de las empresas en nuevos mercados donde existen regulaciones similares y en el caso de las TIC´s la expansión basada en nuevas tecnologías que cubren viejas y nuevas regulaciones.

8.3 La Creación y/o la Aplicación de Estándares Afecta al Indice de Exportación de Tecnologías de la Información

Como lo indica José Valentín Álvarez Álvarez en su artículo *Uso de Estándares E-Learning en Espacios Educativos*

> *"Varias iniciativas se adelantan para definir estándares en el campo de e-Learning; IMS, AICC, SCORM, entre otras organizaciones apuestan por imponer sus especificaciones para la cabal administración y gestión de la enseñanza y el conocimiento en la red. El adagio que reza "en e-Learning si el contenido es el Rey, la plataforma es Dios", no ilustra otra cosa que la imperiosa necesidad de poder integrar y lograr la Interoperatividad entre contenidos de cursos y plataformas, ya que día a día, la experimentación decae y da paso a la consolidación de una tecnología que está en franca ebullición y que sin lugar a duda dará mucho de qué hablar en los próximos años"* (Álvarez, 2004, p 2)

Evidencia de forma clara como una tecnología como el e-learning que apoya las labores educativas que son típicas de cada país, cada región e incluso de cada institución ingresan en el marco de la estandarización a fin de convertirlas en tecnologías de uso global que sobrepasen las barreras de País, región e institución.

8.4 La Creación de Agencias Responsables de la Ciberseguridad Diferentes al Ministerio de Comunicaciones Afecta Directamente al Indice de Innovación

En el documento, Políticas deficiencia, tecnología e innovación Juan José Díaz y Juana Kuramoto citan en sus conclusiones:

> *"Crear un arreglo institucional para el sector de CTI, que se base en tres pilares: (a) el Concytec, que se encargue del diseño, análisis y evaluación de políticas de ciencia y tecnología; (b) el CNC, que se encargue del diseño, análisis y evaluación de las políticas de innovación; y (c) organismos de ejecución."* (Díaz, J. J., & Kuramoto, J, 2011, p 34)

De esta forma identifican la creación organismos de ejecución especializados que logren enfocar el desarrollo de la innovación en el campo de interés del país.

Al considerar entonces que la formulación permite cuantificar podemos entonces realizar un modelo matemático donde la relación resultante RT puede representarse entonces de manera lineal, de esta forma, sin alterar las calificaciones obtenidas, las mismas se pueden representar matemáticamente como:

$$RT = Ap + Bn + Co + Dm$$

RT: *Valor Estimado por la Aplicación de una Estrategia de Ciberseguridad*
Ap: *Variable de Factor Político*
Bn: *Variable de Factor Legal - Económico*
Co: *Variable de Factor Técnico – Económico*
Dm: *Variable de Factor Político – Técnico*

Apoyándonos en el trabajo realizado anteriormente y sabiendo que el peso sobre la variable es un factor relevante para la cuantificación, utilizaremos la información resultante del estudio *Ranking de Ciberseguridad* como el peso de la variable. Este peso le aportara a la variable el sustento matemático para darle relevancia.

Teniendo en cuenta entonces el ranking presentado por la firma *ABI Research y su índice GCI (Índice Global de Ciberseguridad)* la ubicación en el ranking en el año 2015 de los países utilizados en el ejercicio aparece en Tabla 23:

Tabla 23. Rankin de Ciberseguridad

Rankin de Ciberseguridad						
Brasil	**Austria**	**Canadá**	**Egipto**	**Camerón**	**Papua New Guinea**	**Pilipinas**
5	6	2	9	15		17

Elaboración Propia Basada en GCI 2015

De esta forma, al agregar el peso sobre la variable y aterrizando el mismo a un campo cuantificable se podría interpolar entonces a la formulación una variable de ponderación quedando entonces una nueva fórmula cualitativa lineal.

$$RT = RC\ (Ap) + RC\ (Bn) + RC\ (Co) + RC\ (Dm)$$

RT: *Valor Estimado por la Aplicación de una Estrategia de Ciberseguridad*
RC: *Ranking de Ciberseguridad*
Ap: *Variable de Factor Político*
Bn: *Variable de Factor Legal - Económico*
Co: *Variable de Factor Técnico – Económico*
Dm: *Variable de Factor Político – Técnico*

El agregar esta ponderación no afecta la relación cualitativa obtenida en el proceso de relacionamiento inicial (*Actividades Fundamentales Estrategia Ciberseguridad vs Indicadores de Resultado)* sobre las variables, pero acerca el modelo a un campo de uso general, es decir, a la interpretación del mismo sobre el objetivo país.

Utilizando a Turquía y al Reino Unido como ejemplo y basándonos en los indicadores previamente identificados y con el fin de probar el uso y como medio de validación a fin de determinar que la misma entregue un resultado insumo para la toma de decisiones, con el fin de

regularizar los datos, no se tendrán en cuenta las unidades y las mismas se convertirán en una unidad genérica denominada *"puntos"*.

Para realizar el tratamiento de los datos que permita construir el modelo se estandarizarán con el fin que sus unidades sean equivalentes y comparables y que además permitan ser trabajadas en un modelo matemático.

Para el ejercicio a realizar se usará la definición de estandarizar que la real academia de la lengua define como:

> *Tr tipificar.*
> *1. ajustar a un tipo o norma.*
>
> Y tipificar se define como:
>
> *1. tr. Ajustar varias cosas semejantes a un tipo o norma común.*
> *2. tr. Dicho de una persona o de una cosa: Representar el tipo de la especie o clas e a que pertenece.*
> *3. tr. Der. En la legislación penal o sancionatoria, definir una acción u omisión co ncretas, a las que seasigna una pena o sanción.*

De esta forma y con el fin de llevar los datos a una norma común los mismos se tratarán de la siguiente manera:

1. *Utilizando la relación con un promedio de 7 años y base por los años con información.*
2. *Percepción de la corrupción teniendo presente que 100 es sin corrupción.*
3. *Rankin de ciberseguridad sobre 29 puntos.*
4. *A B C D toman el valor de 1 o 2 con el fin de convertirlas en ponderadores.*
5. *se normalizará dividiendo por 10.000 eliminando el factor tipo de moneda.*

Con el fin de mantener una lectura fluida sobre los modelos matemáticos se resumirá el significado de cada una de las variables utilizadas.

Tabla 24. Resumen Variables del Ejercicio

Resumen Variables del Ejercicio		
Ap	Legislación dentro del código Penal	Índice Percepción de Corrupción

Bn	Regulación y Cumplimiento	Índice Exportación Alta Tecnología
Co	Creación y/o Aplicación de Estándares	Índice Exportación Tecnologías de la Información
Dm	Agencia Responsable de la Ciberseguridad Diferente al Ministerio de Comunicaciones	Índice de Innovación

Elaboración Propia

RT Reino Unido

RT = RC ((Ap) + (Bn) + (Co) + (Dm))

RT = (29-5) ((2 * 79.6) + (2 * 69.392) + (2 * 4.16) + (2* 61.4))

RT = (24) ((159.2) + (138.784) + (8.32) + (122.8))

RT = (24) (429.104)

RT = 10298.49 Puntos

Como resultado se obtiene que las actividades realizadas por Reino Unido frente a la ciberseguridad durante los últimos siete años le permitieron obtener 10298.49 puntos de relación.

RT Turquía

RT = RC ((Ap) + (Bn) + (Co) + (Dm))

RT = (29-7) ((2 * 43.1) + (2 * 2.415) + (1 * 1.4) + (1 * 37.6))

RT = (22) ((86.2) + (4.830) + (1.4) + (37.6))

RT = (22) (130.03)

RT = 2866,66 Puntos

En el ejercicio con Turquía se obtiene la ciberseguridad durante los últimos siete años le permitieron obtener 2866,6 puntos de relación.

De esta forma, al revisar los datos obtenidos, podemos expresar que Reino Unido aventaja a Turquía en una relación de 3 a 1, determinando así, que las diferentes inversiones realizadas por

Reino Unido en su estrategia de ciberseguridad han dado resultado tres veces mejores que los de Turquía, si expresáramos las inversiones en unidades monetarias, podríamos decir entonces que Reunido Unido obtendría un beneficio tres veces mayor que Turquía al implementar la estrategia de Ciberseguridad o que la estrategia de ciberseguridad en el mismo lapso de tiempo entre Reino Unido y Turquía le ha representado a Reino Unido una ventaja competitiva en el entorno de Ciberseguridad tres veces mayor que a Turquía.

Así pues, si al modelo que permitió obtener estos resultados le adicionáramos la ponderación propuesta en el ejercicio de análisis estructural, obtendríamos resultados de un modelo aún más ajustado a la realidad, abriendo entonces un espacio para que en estudios posteriores se profundice aún más en el afinamiento del modelo matemático que como referencia fue propuesto en este caso de estudio.

Con esta información, nacen entonces nuevas preguntas, que no son parte de este estudio, pero que no dejan de ser importantes, ¿de cuánto ha sido la inversión de cada país para obtener este puntaje?, ¿cuánto tiempo real se invirtió para obtener este puntaje?, ¿cuántas empresas privadas están involucradas en la obtención de este puntaje?, ¿cuántas empresas extranjeras están involucradas en la obtención de este puntaje?, ¿cuántas empresas de gobierno están involucradas en la obtención de este puntaje? y otras.

9 Modelo Matemático para Uso Empresarial

Teniendo presente el escenario para el desarrollo de un modelamiento matemático y centrándonos en el entorno cibernético sobre el cual estamos trabajando, ya enfocándolo no a un modelo país, sino a un entorno empresarial, es pertinente entonces comenzar organizando y clasificando las variables por algunas de las dimensiones que las concentran y que hacen parte del entorno cibernético empresarial, lo que permitirá como se trató en el ejercicio anterior, incluir en cada una de estas dimensiones un valor de ponderación preciso. Para este ejercicio tomaremos:

1. **Dimensión Humana:** Dimensión donde las variables que la componen se relacionan directamente con el individuo y sus capacidades personales.
2. **Dimensión Tecnológica:** Dimensión donde los variables que la componente depende del desarrollo tecnológico y la capacidad de entendimiento y uso que se le dé a la tecnología.
3. **Dimensión de Procesos:** Dimensión donde las variables que la componen hacen parte de los sistemas de uso o modos de uso documentados y que intervienen actores humanos y/o tecnológicos.

La Imagen 8 describe la relación existente entre las dimensiones e identifica el canal que las relaciona entre sí.

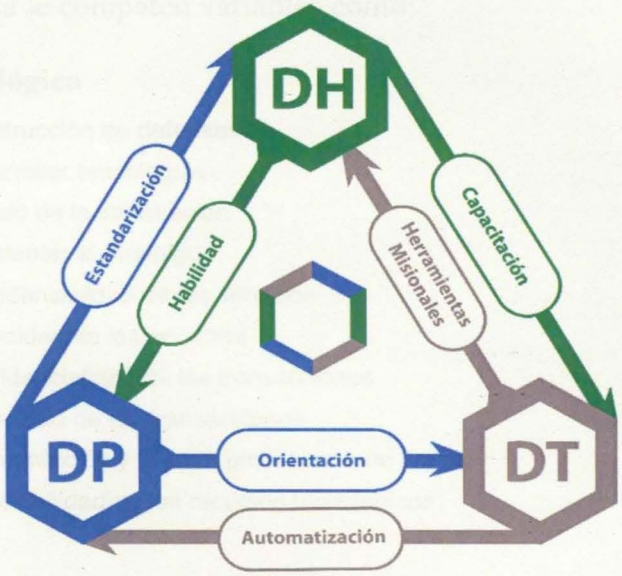


Imagen 8. Triangulo Dimensiones Entorno Cibernético, Fuente: Elaboración Propia, (2020)

Relacionando las variables en las diferentes dimensiones propuestas, según lo visto en capítulos anteriores y como lo expresó entre otros autores Porter 2008 podemos indicar que a la dimensión humana le competen variables como:

Dimensión Humana

V1	Concienciación frente a la ciberseguridad de la operación
V2	Concienciación frente a la ciberseguridad de las directivas
V3	Identificación de las fuerzas competitivas
V4	Identificación de la posición en un sector
V5	Confianza en el mundo digital
V6	Determinación de los lineamientos estratégicos
V7	Determinación de las líneas de acción
V8	Determinación de la posición única
V9	Medición del compromiso individual
V10	Obtener conocimiento digital
V11	Obtener habilidad digital
V12	Creación y aplicación de legislación
V13	Creación y aplicación de regulaciones
V 14	Creación y aplicación de estándares
V 15	Identificación de las modificaciones en las fuerzas

A la dimensión tecnológica le competen variables como:

Dimensión Tecnológica

V16	Construcción de defensas
V17	Desarrollar tecnologías
V18	Cifrado de la información
V19	Desalentar al enemigo
V20	Confidencialidad de los servicios
V21	Privacidad de los servicios
V22	Confidencialidad de las transacciones
V23	Privacidad de las transacciones
V24	Segmentación y microsegmentación de áreas
V25	Disponibilidad de los recursos tecnológicos

A la dimensión de Procesos le competen variables como:

Dimensión de Procesos

V26	Independencia tecnológica
V27	Resiliencia
V28	Posesión del control
V29	Políticas de seguridad
V30	Normas de uso de dispositivos
V31	Ecosistema de seguridad
V32	Resistencia a ciber amenazas
V33	Obtener manejo del riesgo
V34	Minimizar los efectos de los incidentes
V35	Creación de campañas menores dentro de la estrategia
V36	Creación de agencias especializadas
V37	Gestión y retención del talento humano

Con esta clasificación de variables se puede generar entonces un ejercicio de metodología de análisis estructural y obtener la relación entre las variables, la fuerza entre las variables y asignar así una ponderación que hará que el modelo propuesto se ajuste y sea preciso en sus resultados.

El resultado de realizar un ejercicio de análisis estructural con el software MIC MAC similar al ejecutado previamente en este trabajo y como se refleja en la Imagen 9, nos arroga que las variables

15, 11 y 25 son variables de entrada relevantes, que las variables 33, 36, 12 y 26 son variables procesos interesantes y que las variables 5, 27 y 31 son variables de salida importantes.

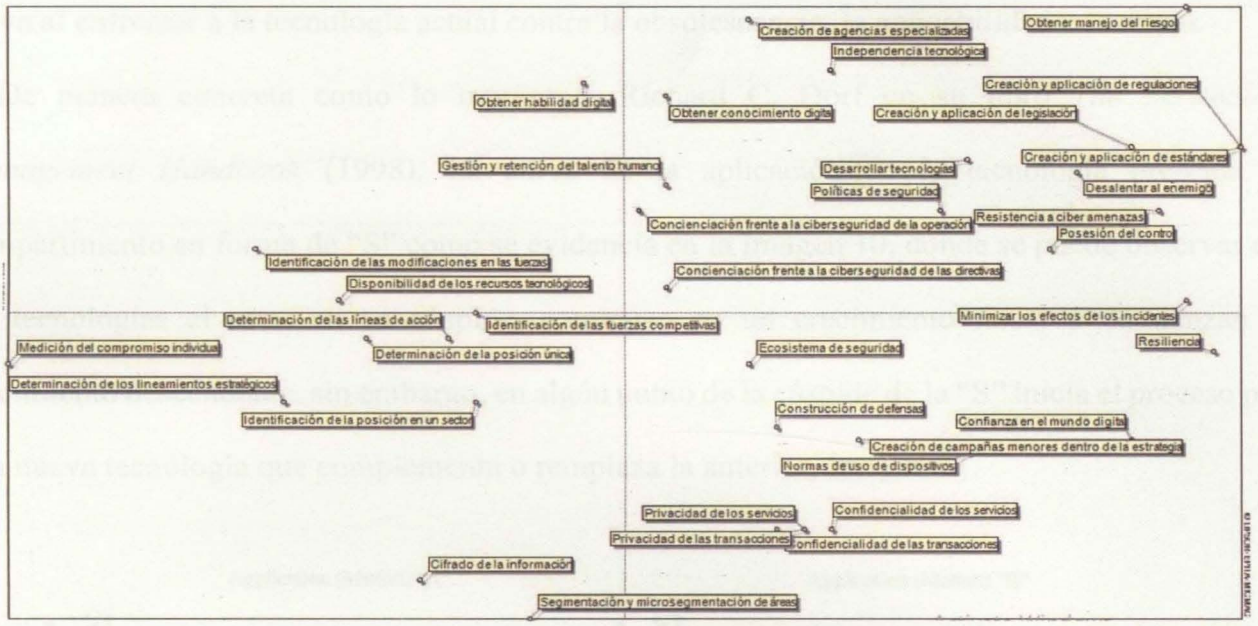


Imagen 9. Plano de Influencias / Dependencias Indirectas Potenciales Fuente: Elaboración propia a partir del Reporte Software MIC MAC LIPSOR EPITIA, (2020)

De esta forma, para el ejercicio en cuestión, se reducen a 10 las variables para el modelo, de igual forma que en ejercicio anterior, se dará un peso adicional (P) al uso de estas variables quedando de la siguiente forma:

$$RT = 3*V15 + 3*V11 + 3*V25 + 2*V33 + 2*V36 + 2*V12 + 2*V26 + V5 + V27 + V31$$

Con el fin de normalizar el ejercicio se pueden tratar las variables en torno a la inversión (X), permitiéndole así al modelo utilizar el factor económico como la unidad de medida y asumiendo que los modelos lineales no representan de manera real el entorno de la ciberseguridad frente al uso o la aplicabilidad de las tecnologías que la componen, podemos determinar y extrapolar el entorno de la ciberseguridad con el entorno tecnológico del cual además hace parte, de igual forma al asumir que la relación predominante en el entorno tecnológico se puede representar en una curva,

donde las tecnologías inician su carrera de asimilación, luego entran en un entorno de uso y finalmente estas decaen ante la presencia de nuevas tecnologías que presionan la pendiente de la curva al enfrentar a la tecnología actual contra la obsolescencia, la aplicabilidad o la moda.

De manera concreta como lo represento Richard C. Dorf en su libro *The Technology Management Handbook* (1998). La curva de la aplicación de la tecnología presenta un compartimento en forma de "S" como se evidencia en la Imagen 10, donde se puede observar que las tecnologías al estar en su cúspide, continúan en un crecimiento lineal o comienzan un crecimiento descendente, sin embargo, en algún punto de la cúspide de la "S" inicia el proceso para una nueva tecnología que complementa o remplaza la anterior, Imagen 11.

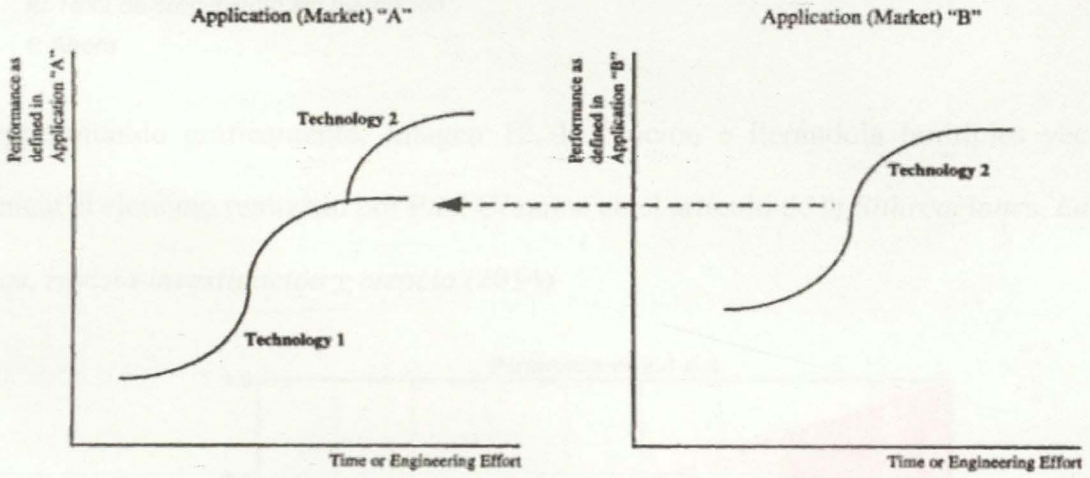


Imagen 10. Curva S de la Tecnología, Fuente: Dorf, 1998

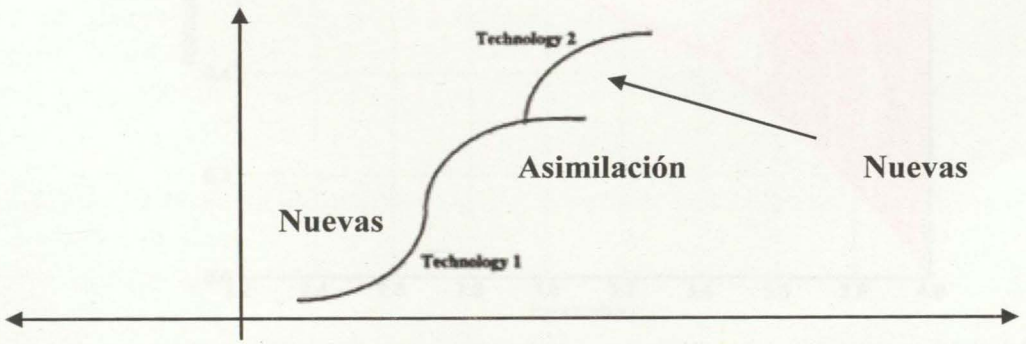


Imagen 11. Curva S de la Tecnología Ciberseguridad, Adaptación Fuente: Dorf, 1998

Así pues, buscando una precisión mayor en el resultado, podemos ajustar el modelo al utilizar la teoría de los caos, basados en su ecuación representativa *"ecuación logística"* como lo explicó Ian Stewart en su libro *17 Ecuaciones que cambiaron el Mundo* (2013) donde se explica el funcionamiento de la ecuación y como el resultado de una iteración está determinado por el resultado de la iteración anterior, así para el caso de estudio desarrollado, le da el sentido completo a la intención de invertir o no invertir en una variable a fin de obtener un mejor resultado futuro.

$$X_{t+1} = \mathrm{k}\, X_t(1\text{-}X_t)$$

X: *Tamaño de la Población.*
t+1: *de la Generación Siguiente*
k: *Tasa de crecimiento sin restricción*
t: *Ahora*

Representando gráficamente, Imagen 12, la función e iterándola múltiples veces como lo referencia el ejercicio realizado por Paul Cézanne en el artículo de la *Bifurcaciones*, *La Ruta Hacia el Caos*, *revista investigación y ciencia* (2014)

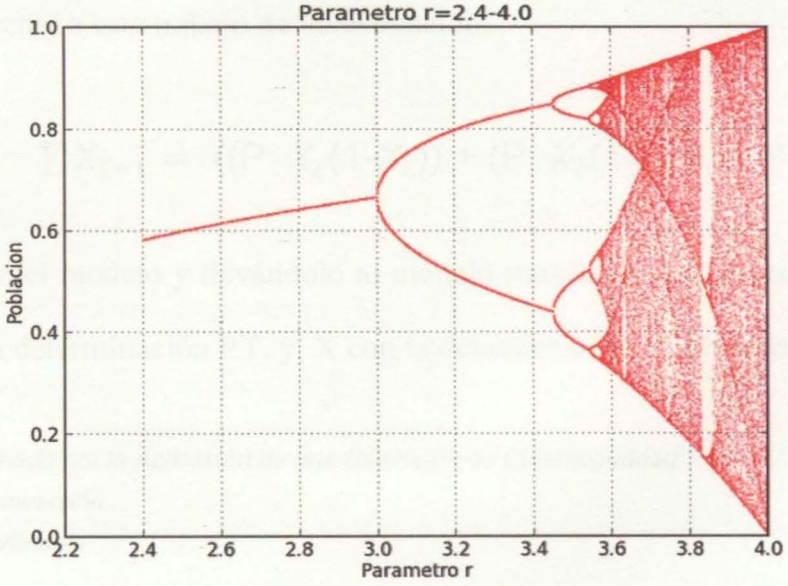


Imagen 12. Bifurcaciones, Fuente: www.investigacionyciencia.es/blogs/matematicas/33/posts/bifurcaciones-12410, 2014

Vemos como la curva en un punto de cúspide inicial, se abre, para generar una nueva curva superior y al tiempo iniciar una nueva curva inferior.

Comparando los modelos gráficos, Imagen 13, podemos determinar que este modelo de curva es el atractor del sistema.

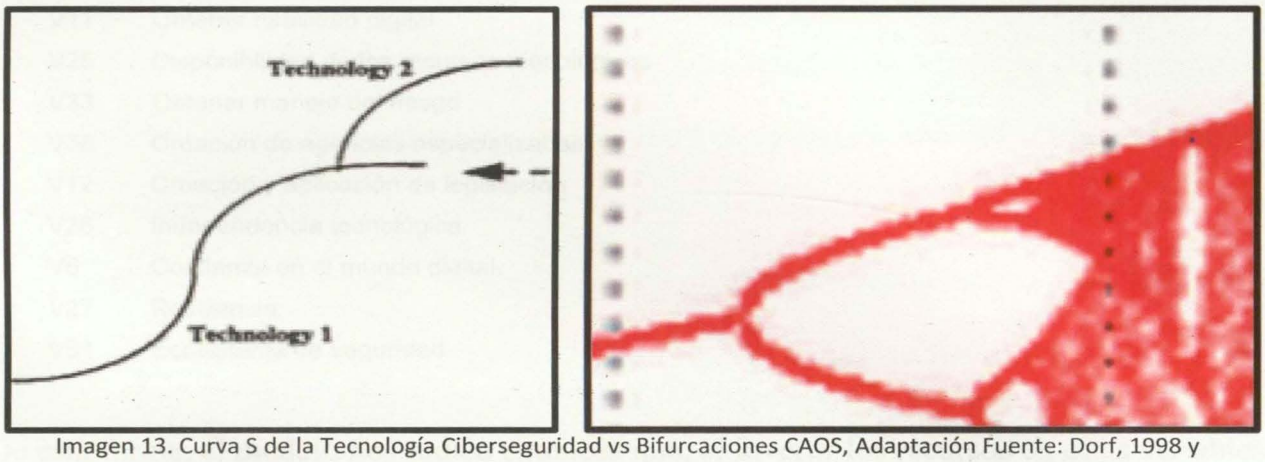


Imagen 13. Curva S de la Tecnología Ciberseguridad vs Bifurcaciones CAOS, Adaptación Fuente: Dorf, 1998 y www.investigacionyciencia.es/blogs/matematicas/33/posts/bifurcaciones-12410, 2014

Por tanto, llevando el modelo lineal inicial y ajustándolo con la *"ecuación logística"* tendíamos para ejercicio pertinente a este trabajo de investigación.

$$\sum X_{t+1} = ((P\ X_t(1\text{-}X_t)) + (P\ X_t(1\text{-}X_t)) + (P\ X_t(1\text{-}X_t))$$

Complementando el modelo y llevándolo al modelo tratado en esta investigación, iteramos la variable X_{t+1} con la determinación RT, y, X con la determinación V, obteniendo:

RT: *Valor Estimado por la Aplicación de una Estrategia de Ciberseguridad.*
V: *Variable de inversión.*
P: *Peso de la Variable*

$$\sum RT_{t+1} = (\mathrm{P}\ V_t(1\text{-}V_t)) + (\mathrm{P}\ V_t(1\text{-}V_t)) + (\mathrm{P}\ V_t(1\text{-}V_t))$$

Aplicando el modelo a los resultados obtenidos en el ejercicio de análisis estructural tendríamos entonces:

RT = ((3*V15 (1-V15)) + 3*V11 (1-V11) + 3*V25 (1-V25) + 2*V33 (1-V33) + 2*V36 (1-V36) + 2*V12 (1-V12) + 2*V26 (1-V26) + V5 (1-V5) + V27 (1-V27) + V31(1-V31))

V15	Identificación de las modificaciones en las fuerzas
V11	Obtener habilidad digital
V25	Disponibilidad de los recursos tecnológicos
V33	Obtener manejo del riesgo
V36	Creación de agencias especializadas
V12	Creación y aplicación de legislación
V26	Independencia tecnológica
V5	Confianza en el mundo digital
V27	Resiliencia
V31	Ecosistema de seguridad

De esta forma, el modelo nos indica entonces que, al invertir los recursos en estas variables, se obtendría el mejor valor estimado de la inversión, siendo este valor estimado mejorado cada vez que se realice una inversión adicional en alguna de las variables, permitiendo entonces predecir la mejor forma de distribuir los recursos en la estrategia de ciberseguridad.

Recapitulando sobre la información procesada y obtenida hasta ahora, se puede identificar, para el caso de estudio, que en el entorno empresarial, la inversión sobre *La Dimensión Humana* es la más relevante, la misma contempla cuatro de los 10 factores más importantes a ser tratados en una estrategia de ciberseguridad, específicamente, los factores *identificación de las modificaciones de las fuerzas* y *obtener habilidad digital* son relevantes para la estrategia y los factores *creación y aplicación de la legislación* y *confianza en el mundo digital* son factores que aceleran la efectividad de la estrategia y le brindan un apoyo importante.

La siguiente dimensión que se aborda es la *Dimensión Tecnológica*, esta solo contempla un factor relevante, las inversiones en el factor *disponibilidad de los recursos tecnológicos,* que son suficientes para apoyar la estrategia de ciberseguridad y operan como un habilitante estructural, según lo identificado en el documento.

Finalmente, contemplando la *Dimensión de Procesos*, la inversión sobre esta, representa un impacto en 5 de los 10 factores más importantes, *obtener manejo del riesgo*, *creación de agencias especializadas*, *independencia tecnológica*, *resiliencia* y *ecosistema de seguridad*, son varios factores que de manera distribuida fortalecen significativamente la estrategia de ciberseguridad, toda vez, que se convierten en el puente que permite hacer que la inversión tenga un retorno de valor continuo para la organización.

Como ejemplo teórico, podemos trabajar con un presupuesto finito de Z unidades de valor, el cual debe ser invertido por dos diferentes directores de seguridad de la información, de dos diferentes compañías, teniendo presente que se tienen múltiples variables para invertir, los directores deberían iniciar invirtiendo en las variables "importantes" relacionadas anteriormente en la investigación y distribuir de esta forma el presupuesto hacia las demás, como resultado, la compañía A y la compañía B obtendrán un *Valor Estimado por la Aplicación de una Estrategia de Ciberseguridad* diferente, pero óptimo, y al reinvertir nuevamente en el periodo siguiente, obtendrán entonces un nuevo *Valor Estimado por la Aplicación de una Estrategia de Ciberseguridad* más preciso, y así, sucesivamente hasta el punto donde se crea conveniente añadir si se desea, cada vez, más variables de distribución, desplazándose entonces en el tiempo sobre inversiones optimas que permiten una visión ajustada al futuro con una visión presente sobre el retorno.

Como ejemplo práctico, tenemos la empresa Black Hat Archetype, una empresa que lleva en el mercado colombiano operando por más de 15 años en el sector de servicios, específicamente en las

verticales de seguridad informática, seguridad de la información, ciberseguridad y seguridad digital. Como parte fundamental de su operación, la seguridad de su infraestructura lógica y la seguridad de la infraestructura física que la soporta es muy importante, de esta forma, las inversiones sobre estos dos campos se convierten en permanentes y fundamentales.

Para el caso de estudio,

$$\sum RT_{t+1} = (P\ \ V_t(1\text{-}V_t) + (P\ \ V_t(1\text{-}V_t) + (P\ \ V_t(1\text{-}V_t)$$

RT: *Valor Estimado por la Aplicación de una Estrategia de Ciberseguridad.*

V: *Variable de inversión.*

P: *Peso de la Variable*

El modelo estratégico de las áreas de la compañía se trabaja por periodos de dos años lo que hace que la estrategia contemplada sea de ejecución inmediata a fin de obtener en periodos cortos los resultados deseados, pensando en un presupuesto de $ 300.000.000 millones de Pesos Colombianos para completar la estrategia de ciberseguridad, el ejercicio se desenvolvería de la siguiente manera.

Normalización de las Unidades

Presupuesto: 300.000.000 Pesos / $ 1.000.000 Pesos

Presupuesto: 300

Año 2020

RT = ((3*50 (1-50)) + 3*30 (1-30) + 3*43 (1-43) + 2*30 (1-30) + 2*33 (1-33) + 2*21 (1-21) + 2*17 (1-17) + 25 (1-25) + 23 (1-23) + 28(1-28))

De esta forma se ejemplifica la distribución de los recursos a fin de conseguir que la estrategia de ciberseguridad sea exitosa, primero, mejorando la postura y segundo, retornando valor a la compañía.

RT = ((3*50/300 (1-50/300)) + 3*30/300 (1-30/300) + 3*43/300 (1-43/300) + 2*30/300 (1-30/300) + 2*33/300 (1-33/300) + 2*21/300 (1-21/300) + 2*17/300 (1-17/300) + 25/300 (1-25/300) + 23/300 (1-23/300) + 28/300(1-28/300))

		50	30	43	30	33	21	17	25	23	28
✚	300	0.17	0.10	0.15	0.10	0.11	0.07	0.06	0.09	0.08	0.10
		3	3	3	2	2	2	2	1	1	1
✖	Ans	0.51	0.30	0.45	0.20	0.22	0.14	0.12	0.09	0.08	0.10
		1	1	1	1	1	1	1	1	1	1
▬	Ans	0.83	0.90	0.85	0.90	0.89	0.93	0.94	0.91	0.92	0.90

RT = 0.43 + 0.27 + 0.39 + 0.18 + 0.20 + 0.13 + 0.12 + 0.09 + 0.08 + 0.09
RT = 1.98

Año 2021

RT = ((3*V15 (1-V15)) + 3*V11 (1-V11) + 3*V25 (1-V25) + 2*V33 (1-V33) + 2*V36 (1-V36) + 2*V12 (1-V12) + 2*V26 (1-V26) + V5 (1-V5) + V27 (1-V27) + V31(1-V31))

AnsVt		0.43	0.27	0.39	0.18	0.20	0.13	0.12	0.09	0.08	0.09
		3	3	3	2	2	2	2	1	1	1
✖	AnsVt	1.29	0.81	1.17	0.36	0.40	0.26	0.24	0.09	0.08	0.09
		1	1	1	1	1	1	1	1	1	1
▬	AnsVt	0.57	0.73	0.61	0.82	0.80	0.87	0.88	0.91	0.92	0.91

RT = 0.74 + 0.60 + 0.72 + 0.30 + 0.32 + 0.23 + 0.22 + 0.09 + 0.08 + 0.09
RT = 3.39

El cambio en RT del año 2020 frente al 2021, representa la forma en que la estrategia está cumpliendo con su efectividad, el incremento presentado refleja que la estrategia al segundo año con las mismas condiciones iniciales, casi dobla el retorno de la inversión, la "*ecuación logística*" nos indica que al iterar el modelo otro año y luego otro año y luego otro año, el modelo tenderá a estabilizarse, indicándonos, que la estrategia ya no genera más valor y por tanto, sobre la misma, se deberá incluir una nueva variable o modificar el valor de la variable, a fin, de tener nuevamente un retorno maximizado.

10 Conclusiones

Con este resultado, podemos expresar entonces, que más allá, de pensar en un retorno de inversión frente a la ciberseguridad, expresado en la simplicidad e indeterminación de haber podido evitar la materialización de un riesgo gracias a una inversión. La implementación de una estrategia de ciberseguridad sobre las variables del caso de estudio, retornan efectivamente valor a la compañía o estado que la implementa.

El usar un modelo matemático para proyectar el retorno de la inversión, permite utilizando el campo teórico y mediante el uso de un proceso de comparación de estrategias, analizar la distribución efectiva del presupuesto que retornará mayor valor a la compañía o estado.

El resultado de la implementación de una estrategia de ciberseguridad, se basa en la inversión consciente de recursos, pero, no en la inversión sobre todos los factores tecnológicos que conocemos o presuponemos son eficaces para mejorar la ciberseguridad, en cambio, la inversión en factores específicos que realmente impactan la estrategia, permite optimizar el resultado de las inversiones.

La ciberseguridad es personalizable, cada empresa puede obtener recursos de la aplicación de una estrategia de ciberseguridad, y, por tanto, cada empresa puede crear su propio camino en ciberseguridad, un camino que puede ser paralelo a lo ofrecido en el mercado tradicional de seguridad, pero, no independiente de la tecnología.

La inversión en ciberseguridad, más allá, de ser una inversión que permite la operación, es ahora, en nuestra sociedad de la información, una inversión que permite el retorno de valor, no solo como el valor de mantener la operación, sino, como un valor monetario cuantificable para la organización o el país que la implementan.

Las inversiones en ciberseguridad, ya no son entonces únicamente de un área de tecnología, y, aunque la ciberseguridad está inmersa en la tecnología, la inversión en la estrategia toca campos humanos y de procesos que por ahora están fuera de la visión de muchas compañías, pero que, con el tiempo, y, forzados por la sociedad de la información, harán parte o alimentaran los recursos del área de tecnología.

11 Recomendaciones y Futuros Trabajos

Como caso de estudio, si se realiza una división entre el *Valor Estimado por la Aplicación de una Estrategia de Ciberseguridad* y el monto total de la inversión, se puede obtener el porcentaje de reciprocidad monetaria recibido al implementar la estrategia, una información que es útil para las áreas financieras y que permite soportar de manera efectiva las solicitudes de recursos frente a la alta gerencia, el manejo de porcentajes durante la presentación de una estrategia permite relacionar de una mejor manera un éxito o un avance, como ejemplo, y, utilizando uno de los resultados del ejercicio anterior, podríamos indicar, RT = 3.39 al dividir este resultado por un total de inversión imaginario y normalizado I = 10, obtendríamos 33,9%. Concluyendo que en ese instante se habría ganado sobre la inversión un 33,9%.

También como caso de estudio, si se pensara en realizar un análisis y se dividiera el *Valor Estimado por la Aplicación de una Estrategia de Ciberseguridad* previamente normalizado, con el f*act*or numérico "1" obtendríamos entonces el punto de pérdida de valor de la estrategia frente al tiempo. Y, de igual forma, si se dividieran cada una de las variables del modelo, entre f*act*or numérico "1", obtendríamos los puntos de pérdida de valor de cada variable frente al tiempo. Permitiendo analizar la parte baja de la bifurcación, situación que permitiría realizar un estudio sobre la actualización del sentido de la variable o la eliminación de la misma debido a los cambios tecnológicos o sociales o de procesos.

Es posible y recomendable realizar nuevos ejercicios de análisis estructural, añadiendo nuevos factores, tanto al ámbito nacional como al ámbito empresarial, de forma que el modelo podría ser extendido en su composición, situación que permitiría al estratega tener un campo de acción algo más diverso al propuesto en el ejercicio realizado.

También, para el ámbito nacional, sería pertinente realizar el ejercicio de ajuste con la ecuación logística, pretendiendo obtener basados en datos existente una relación ajustada entre la tecnología, el avance tecnológico y el mejoramiento económico. Y, si no se usan datos existentes y se complementan los factores del modelo con fuentes detalladas, se podría realizar un ejercicio de proyección, que apoyaría de manera concreta las decisiones nacionales frente a la ciberdefensa y la ciberseguridad.

Referencias

1. Anahiby Becerril, A, 2019, La ciberseguridad en los Tratados de Libre Comercio. Revista chilena de derecho y tecnología, 8(2), Pag 111-137.
2. Aguilar-Antonio, J. M. 2019, Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad, Revista Latinoamericana de Estudios de Seguridad, 25, Pag 24-40. E-ISSN 1390-4299 ISSN 1390-3691
3. Álvarez Valenzuela, D, 2019, La paz y la seguridad internacional en el ciberespacio. Revista chilena de derecho y tecnología, 8(2), Pag 1-3.
4. Orellana-Daube, D. F, 2020, El efecto global de la actual revolución tecnológica 4ª revolución industrial y la industria 4.0 en acción. Revista GEON (Gestión, Organizaciones y Negocios), 7(2), Pag 1-24.
5. Marcela Meneses Guzmán, Juan Hernández, 2020, Industria 4.0. Transformación digital, un cambio en el que participamos todos. Investiga. TEC, Pag 11-13.
6. Mariano Bartolomé, 2020, Las Ciberamenazas y su Impacto en ll Campo de la Seguridad Internacional, Revista de la ESG, 602, Pag 151-163
7. Lamus Villamizar, 2019, Integración y ciberespacio. Geopolítica y Nuevos Actores de la Integración Latinoamericana, Ediciones Universidad Cooperativa de Colombia, Pag 311-333. doi: https://dx.doi.org/10.16925/9789587601992
8. Núñez, M. A., Rivas-Montoya, L. M., Villanueva, E., Mejía, P., Montoya-Londoño, C. A., & Jaraba, I, 2020, Riesgo estratégico. Universidad EAFIT.
9. Alice SHIU y Pun-Lee LAM, 2010, Causal Relationship Between Telecommunications and Economic Growth a Study of 105 Countries, ScienceDirect, Volumen 34 Número 4, Pag 6.

10. Alicia Hamui-Sutton, (Octubre – Diciembre 2013), Un acercamiento a los métodos mixtos de investigación en educación médica, Investigación en Educación Médica, Volumen 2, Issue 8, Pag 211-216.
11. Aníbal Irarrázabal C, 1997, Contabilidad, Fundamentos y Usos, editorial C.I.P Pontificia Universidad Católica de Chile, ISBN: 978-956-14-0995-8, Pag 32
12. Arnáiz, T. M, 2016, La necesidad de reformar la legislación sobre contratación pública para luchar contra la corrupción: las obligaciones que nos llegan desde Europa. Revista Vasca de Administración Pública. Herri-Arduralaritzako Euskal Aldizkaria, Pag 77-113.
13. Aurora Ballesteros, 2002, El Espacio Social del Cibercomercio, El Caso Español. Estudios Geográficos, 63. 10.3989/egeogr, i248-249.242.
14. Basáñez M-G, Rodríguez Dj, 2004, Dinámica de Transmisión y Modelos Matemáticos en Enfermedades Transmitidas por Vectores. Entomotrópica, Pag 113-134. ISSN 1317-5262
15. Begovic, B, 2005, Corrupción: conceptos, tipos, causas y consecuencias. Centro para la apertura y el desarrollo de América Latina, Pag 26.
16. Keith Crane, James Dobbins, Laurel E. Miller, Charles P. Ries, Christopher S. Chivvis, Marla C. Haims, Marco Overhaus, 2010, Building a More Resilient Haitian State Book Author(s), RAND Corporation. http://www.jstor.org/stable/10.7249/mg1039srf-cc.12, ISSN 0924-0608
17. Burgos Simón, C., Cortés López, J., Martínez Rodríguez, D., Navarro Quiles, A., & Villanueva Micó, R, 2019. Un modelo de oferta y demanda con incertidumbre. Modelling in Science Education and Learning, 12(1), Pag 111-122. https://doi.org/10.4995/msel.2019.10897

18. Carlos Eduardo Valderrama H, 2012, Sociedad de la Información: Hegemonía, Reduccionismo Tecnológico y Resistencias Nómadas, Universidad Central, Pag 13-25, ISSN: 0121-7550, Ni 36.

19. Cesare Guariniello, Daniel DeLaurentis, 2014, Communications, Information, and Cyber Security in Systems-of-Systems: Assessing the Impact of Attacks through Interdependency Analysis,
In Procedia Computer Science, Volume 28, Pag 720-727, ISSN 1877-0509
https://doi.org/10.1016/j.procs.2014.03.086.
http://www.sciencedirect.com/science/article/pii/S1877050914001495

20. Definición de la palabra Estrategia, Real Academia Española, 2020
https://dle.rae.es/?id=GxPofZ8

21. Definición de la palabra Fórmula, Real Academia Española, 2020
https://dle.rae.es/?w=f%C3%B3rmula&m=form

22. Definición de la palabra Estandarizar, Real Academia Española, 2020
https://dle.rae.es/?w=f%C3%B3rmula&m=form

23. Definición de la palabra Tipificar, Real Academia Española, 2020
https://dle.rae.es/?w=f%C3%B3rmula&m=form

24. Dominique Nora, La Conquista del Ciberespacio, Andrés Bello, 1997, ISBN 84-89691-06-1, Pag 23-24.

25. Dorf, R. C, 1998. The Technology Management Handbook. CRC Press.

26. Estados Miembros de las Naciones Unidas, 2020
https://www.un.org/es/member-states/index.html

27. Forbes México, Las 15 automotrices más importantes del mundo, 2013
https://www.forbes.com.mx/las-15-automotrices-mas-importantes-del-mundo

28. Gamboa Cáceres, T., Arellano Rodríguez, M., & Nava Vasquez, Y, 2010, Actores y Fines de las Estrategias Empresariales. Una reflexión desde las pequeñas y medianas empresas. Visión Gerencial, 0(1), Pag 28-39. http://erevistas.saber.ula.ve/index.php/visiongerencial/article/view/820
29. González Araya, M. y Sáez Leal, Relación entre EVA y los Retornos Accionarios de Empresas Chilenas Emisoras de ADRs, 2005, http://repositorio.uchile.cl/handle/2250/127412
30. https://www.investing.com, 2020
31. https://www.theglobaleconomy.com/texts_new.php?page=aboutus, 2020
32. Hans Rott, Economics and Economy in the Theory of Belief Revision (Preliminary Report), 2003, In Electronic Notes in Theoretical Computer Science, Volume 84, Pag 30-44, ISSN 1571-0661, https://doi.org/10.1016/S1571-0661(04)80842-9. http://www.sciencedirect.com/science/article/pii/S1571066104808429
33. José A Guglien, 1997, Reingeniería y Seguridad en el Ciberespacio, Diaz de Santos, Pag 5.
34. Juan Mascareñas, 2001, Metodología de la Valoración de las Empresas de Internet, Universidad Complutense de Madrid, Pag 2-7
35. Jorge Eliecer Prieto Herrera, 2013, Investigación de Mercados, Pag 3, ISBN 958648985X, 9789586489850
36. José German Altuve G, 2002, Capital Intelectual y Generación de Valor, Actualidad Contable Universidad de los Andes Mérida, Venezuela Faces, vol. 5, núm. 5, Pag 7-22
37. Juan José Ávila Macedo, 2013, Introducción a la Contabilidad, Umbral Editorial S.A de C.V, ISBN: 968-5430-04-07, Pag 17

38. Leiva E, 2015, Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local Revista Latinoamericana de Ingeniería de Software, 3(4): 161-176, ISSN 2314-2642

39. Li Bonilla F, 2010, El Valor Económico Agregado (Eva) en el Valor del Negocio. Revista Nacional de Administración, 1(1), Pag 55-70. https://doi.org/10.22458/rna.v1i1.284

40. López, A, 1972, Acerca de la transferencia de tecnología y de la dependencia económica, Revista de la Universidad Nacional (11), Pag 7-69.

41. María José Caro Bejarano, 2011, Alcance y Ámbito de la Seguridad Nacional en el Ciberespacio, Cuadernos de Estrategia, ISSN 1697-6924, N.º 149

42. Michael E. Porter, 2008, Harvard Business Review, ISSN 0717-9952, Vol. 86, Nº. 1, 2008, Pag 58-71 https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf

43. Pablo Fernández, 2008, Métodos de Valoración de Empresas, Documento de Investigación, DI-771, Universidad de Navarra, Pag 3

44. Paul Cézanne, Bifurcaciones, 2014, La Ruta Hacia el Caos, Revista Investigación y Ciencia

45. Postel, 1980, DOD STANDARD INTERNET PROTOCOL, Information Sciences Institute University of Southern California, Pag 1-3. https://www.rfc-editor.org/rfc/pdfrfc/rfc760.txt.pdf

46. Raúl L Katz, 2009, El Papel de las TIC en el Desarrollo, Propuesta de América Latina a los Retos Económicos Actuales, Pag 16.

47. Republic Ff Turkey, Ministry Of Transport Maritime Affairs And Communications 2016-2019. National Cyber Security Strategy

48. Sánchez, 2014, M. D. L. M, Las Organizaciones Empresariales Trasnacionales como Autoridad en la Gobernanza del Ciberespacio. Universidad Autónoma de México

49. Stewart, I., & Fernández, L. 2003, 17 Ecuaciones que Cambiaron el Mundo. Crítica.

50. Torres Citraro, 2014, La Importancia de los Activos Intangibles en la Sociedad del Conocimiento, Revista La Propiedad Inmaterial n.° 18, Universidad Externado de Colombia, Pag 5-34.

51. Tracy y Wierseman, 1999, La Disciplina de los líderes del mercado

52. Uk. National Cyber Security Strategy 2016-2021

53. Wohlers, M, 2008, Convergencia tecnológica y agenda regulatoria de las telecomunicaciones en América Latina.

12 ANEXO 1.

Informe Micmac

1

SUMARIO

Presentación de las variables

Lista de variables

28. Confianza en el Mundo Digital (V1)
29. Confidencialidad de las Transacciones (V2)
30. Confidencialidad de los Servicios (V3)
31. Construcción de Defensas (V4)
32. Creación de Agencias Especializadas (V5)
33. Creación de Campañas Menores Dentro de la Estrategia (V6)
34. Creación y Aplicación de Estándares (V7)
35. Creación y Aplicación de Legislación (V8)
36. Creación y Aplicación de Regulaciones (V9)
37. Desalentar al enemigo (V10)
38. Desarrollar Tecnologías (V11)
39. Determinación de la Posición Única (V12)
40. Determinación de las Líneas de Acción (V13)
41. Determinación de los Lineamientos Estratégicos (V14)
42. Ecosistema de Seguridad (V15)
43. Identificación de la Posición en un Sector (V16)
44. Identificación de las Fuerzas Competitivas (V17)
45. Identificación de las Modificaciones en las Fuerzas (V18)
46. Incidentes de Seguridad (V19)
47. Medición del Compromiso Individual (V20)
48. Minimizar los Efectos de los Incidentes (V21)
49. Obtener Conocimiento Digital (V22)
50. Obtener Habilidad Digital (V23)
51. Obtener Manejo del Riesgo (V24)
52. Privacidad de las Transacciones (V25)
53. Privacidad de los servicios (V26)
54. Resistencia a Ciber Amenazas (V27)

Matrices de entrada

Matriz de Influencias Directas (MID)

La Matriz de Influencias Directas (MID) describe las relaciones de influencias directas entre las variables que definen el sistema.

Las influencias se puntuan de 0 a 3, con la posibilidad de señalar las influencias potenciales :

0 : Sin influencia
1 : Débil
2 : Media
3 : Fuerte
P : Potencial

Matriz de Influencias Directas Potenciales (MIDP)

La Matriz dez Influences Directes Potencialess MIDP representa las influencias y dépendancias actuales y potenciales entre variables. Completa la matriz MID teniendo igualmente en cuenta las relaciones visibles en un futuro.

Las influencias se puntuan de 0 à 3 :

0 : Sin influencia

1 : Débil
2 : Media
3 : Fuerte

Resultados del estudio

Influencias directas
Estabilidad a partir de MID

Demuestra que toda la matriz debe converger hacia una estabilidad al final de un cierto número de iteracciones (generalmente 4 ó 5 para una matriz de 30 variables), es interesante poder seguir la evolución de esta estabilidad en el curso de multiplicaiones sucesivas. En ausencia de criterios matemáticamente establecidos, ha sido elegido para apoyarse sobre un número determinado de iteracciones.

ITERACCION	INFLUENCIA	DEPENDENCIA
1	98 %	95 %
2	99 %	101 %

Plano de influencias / dependencias directas
Este plano se determina a partir de la matriz de influencias directas MID.

Grfico de influencias directas

Este gráfico se determina a partir de la matriz de influencias directas MID.

Influencias directas potenciales

Estabilidad a partir de MIDP

Demuestra que toda matriz debe converger hacia una estabilidad al final de un cierto número de iteracciones (generalmente 4 ó 5 para une matriz de 30), es interesante poder seguir la evolución de esta estabilidad después de multiplicaciones succesivas. En ausencia de criterios matemáticamente establecidos, se elige apoyarse en un número de permutaciones (tri à bulles) necesarios en cada iteracción para clasificar, la influencia y la dependencia, del conjunto de variables.

ITERACCION	INFLUENCIA	DEPENDENCIA
1	98 %	95 %
2	99 %	101 %

Gráfico de influencias directas potenciales
Este gráfico se determina a partir de la matriz de influencias directas potenciales MIDP.

Influences indirectes

Plano de influencias / dependencias indirectas

Este plano se determina a partir de la matriz de influencias indirectas MII.

Influencias indirectas potenciales

Matriz de Influencias Indirectas Potenciales (MIIP)

La Matriz de Influencias Indirectas Potenciales (MIIP) corresponde a la Matriz de Influencias Directas Potenciales (MIDP) elevada a la potencia, por iteracciones succesivas. A partir de esta matriz, una nueva clasificación de las variables pone en valor las variables potencialmente más importantes del sistema.

Los valores representan la tasa de influencias indirectas potenciales

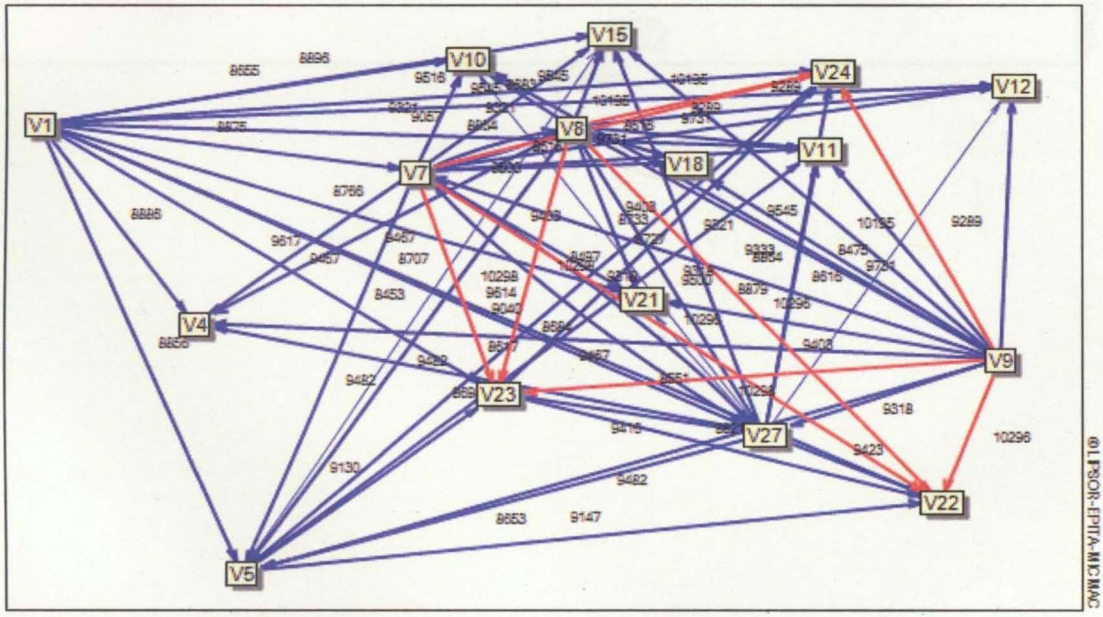
Plano de influenciass / dependencias indirectas potenciales

Este plano se determina a partir de la matriz de influencias indirectas potenciales MIIP.

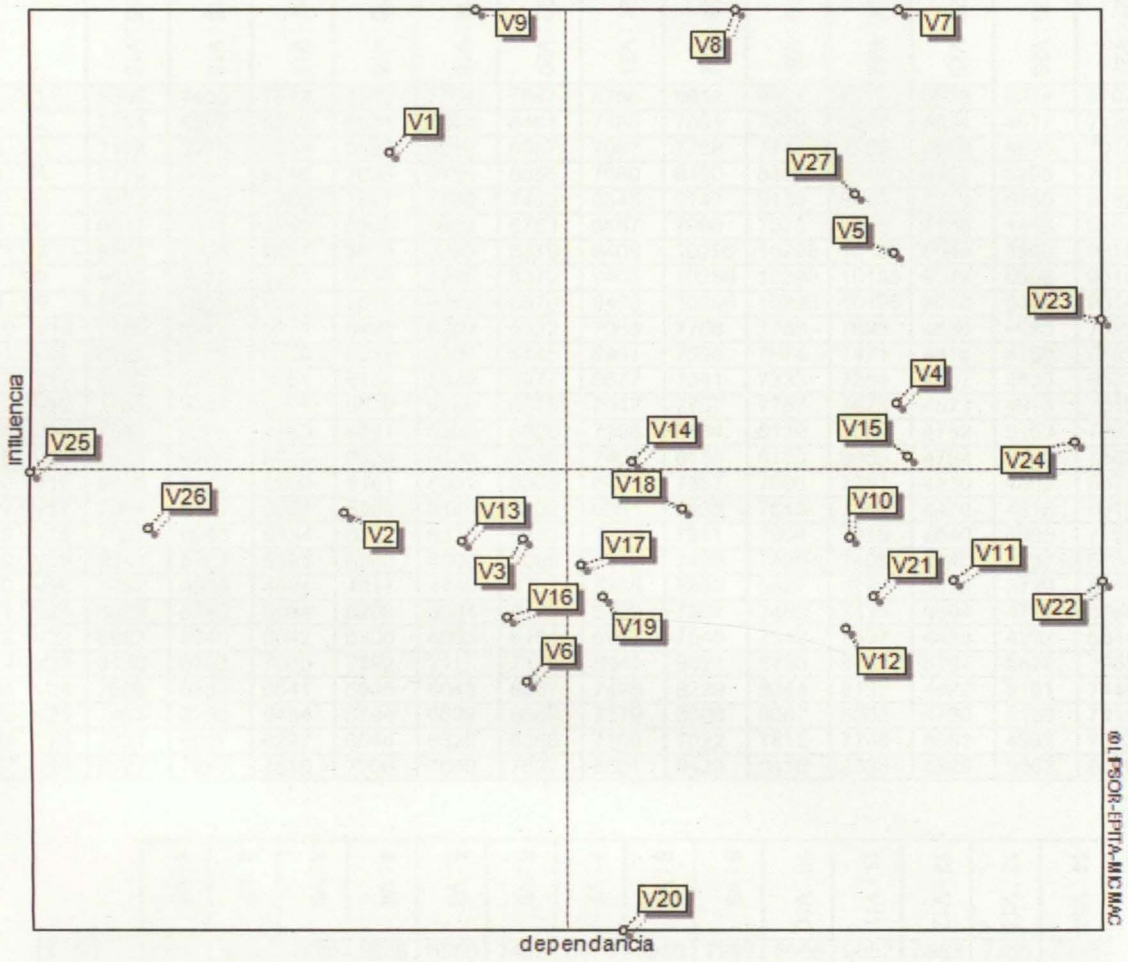
Gráfico de influencias indirectas potenciales

Este gráfico se determina a partir de la matriz de influencias indirectas MIIP.

Gráfico de influencias indirectas potenciales



Plano de influenciass / dependencias indirectas potenciales



	15 : V15	16 : V16	17 : V17	18 : V18	19 : V19	20 : V20	21 : V21	22 : V22	23 : V23	24 : V24	25 : V25	26 : V26	27 : V27
1 : V1	8896	7405	7673	8049	7774	7847	8766	9614	9617	9516	5636	6074	8707
2 : V2	7294	6077	6318	6631	6364	6461	7185	7891	7870	7804	4634	4971	7126
3 : V3	7178	5975	6214	6526	6269	6357	7067	7768	7747	7682	4559	4895	7015
4 : V4	7779	6497	6746	7038	6755	6855	7680	8400	8396	8316	4952	5295	7615
5 : V5	8453	7054	7350	7647	7360	7463	8345	9147	9130	9040	5379	5756	8282
6 : V6	6517	5442	5655	5953	5682	5753	6467	7090	7075	6985	4158	4456	6406
7 : V7	9545	7938	8221	8616	8295	8379	9403	10296	10298	10195	6049	6508	9318
8 : V8	9545	7938	8221	8616	8295	8379	9403	10296	10298	10195	6049	6508	9318
9 : V9	9545	7938	8221	8616	8295	8379	9403	10296	10298	10195	6049	6508	9318
10 : V10	7189	5973	6171	6492	6289	6322	7063	7766	7765	7698	4539	4925	7020
11 : V11	6983	5818	6020	6337	6102	6145	6901	7555	7574	7471	4418	4780	6852
12 : V12	6780	5629	5854	6151	5924	5977	6677	7341	7333	7254	4292	4630	6637
13 : V13	7165	5948	6175	6509	6283	6315	7047	7757	7757	7673	4523	4915	7019
14 : V14	7528	6248	6483	6821	6590	6626	7398	8134	8139	8052	4752	5153	7363
15 : V15	7530	6285	6528	6828	6530	6636	7468	8155	8150	8059	4794	5140	7389
16 : V16	6830	5685	5903	6181	5961	6009	6736	7387	7396	7291	4330	4662	6677
17 : V17	7064	5877	6091	6399	6140	6202	6981	7638	7643	7549	4478	4818	6919
18 : V18	7307	6083	6334	6622	6370	6453	7214	7911	7904	7818	4640	4985	7159
19 : V19	6941	5762	5995	6243	6066	6096	6812	7485	7489	7408	4386	4737	6784
20 : V20	5457	4535	4694	4917	4749	4767	5365	5855	5887	5799	3429	3729	5319
21 : V21	6929	5740	5964	6289	6084	6123	6790	7507	7485	7436	4394	4727	6765
22 : V22	6983	5840	6042	6306	6065	6161	6917	7545	7542	7497	4438	4762	6844
23 : V23	8158	6793	7030	7392	7111	7175	8041	8821	8793	8733	5167	5572	7968
24 : V24	7586	6339	6541	6905	6643	6687	7498	8229	8244	8127	4822	5191	7446
25 : V25	7463	6220	6434	6794	6522	6569	7379	8096	8087	8002	4720	5126	7311
26 : V26	7231	6011	6227	6544	6326	6366	7100	7822	7815	7746	4593	4932	7062
27 : V27	8727	7247	7516	7906	7640	7697	8551	9423	9416	9333	5529	5953	8499

	1 : V1	2 : V2	3 : V3	4 : V4	5 : V5	6 : V6	7 : V7	8 : V8	9 : V9	10 : V10	11 : V11	12 : V12	13 : V13	14 : V14
1 : V1	6941	6833	7456	8886	8856	7492	8875	8288	7299	8655	9057	8683	7260	7848
2 : V2	5757	5566	6112	7229	7243	6097	7309	6726	6012	7122	7445	7082	5909	6492
3 : V3	5665	5476	6006	7116	7123	5992	7194	6619	5918	7004	7329	6960	5817	6393
4 : V4	6121	5937	6547	7736	7748	6567	7753	7200	6363	7586	7943	7579	6333	6876
5 : V5	6672	6397	7087	8359	8382	7073	8433	7808	6948	8263	8617	8219	6841	7509
6 : V6	5155	5006	5505	6498	6521	5490	6512	6047	5362	6378	6668	6366	5309	5805
7 : V7	7458	7270	8028	9467	9482	8062	9473	8864	7812	9321	9731	9289	7764	8409
8 : V8	7458	7270	8028	9467	9482	8062	9500	8837	7812	9321	9731	9289	7764	8409
9 : V9	7458	7270	8028	9467	9482	8062	9500	8864	7785	9321	9731	9289	7764	8409
10 : V10	5567	5504	6048	7177	7163	6088	7157	6722	5884	6989	7337	7020	5865	6308
11 : V11	5462	5381	5882	6978	6978	5899	6986	6488	5712	6831	7101	6820	5726	6164
12 : V12	5329	5178	5664	6754	6715	5661	6750	6294	5578	6609	6905	6584	5508	6033
13 : V13	5606	5506	5996	7180	7143	6003	7153	6653	5894	6976	7286	6967	5832	6351
14 : V14	5887	5766	6293	7521	7478	6309	7506	6979	6178	7340	7647	7314	6142	6658
15 : V15	5929	5770	6363	7515	7506	6360	7495	7012	6180	7360	7696	7368	6134	6668
16 : V16	5346	5217	5729	6796	6786	5739	6795	6361	5601	6665	6938	6671	5535	6045
17 : V17	5551	5409	5931	7041	7023	5932	7008	6576	5782	6921	7177	6880	5747	6256
18 : V18	5751	5583	6131	7282	7263	6122	7275	6792	6016	7146	7437	7117	5938	6488
19 : V19	5401	5263	5793	6894	6865	5814	6907	6436	5685	6743	7042	6751	5630	6120
20 : V20	4265	4169	4553	5414	5400	4579	5426	5015	4447	5322	5512	5293	4447	4804
21 : V21	5429	5282	5761	6908	6860	5756	6892	6450	5714	6746	7060	6718	5611	6170
22 : V22	5492	5320	5888	6947	6939	5884	6956	6495	5718	6814	7155	6835	5685	6178
23 : V23	6381	6227	6850	8097	8121	6877	8132	7575	6662	7945	8331	7946	6638	7195
24 : V24	5926	5874	6386	7588	7607	6418	7589	7064	6204	7402	7735	7430	6230	6695
25 : V25	5858	5720	6284	7436	7447	6281	7445	6948	6114	7293	7625	7284	6079	6610
26 : V26	5658	5506	6060	7206	7179	6065	7200	6727	5920	7056	7373	7037	5869	6400
27 : V27	6826	6658	7279	8693	8653	7307	8684	8093	7174	8497	8879	8475	7081	7723

Plano de influencias / dependencias indirectas

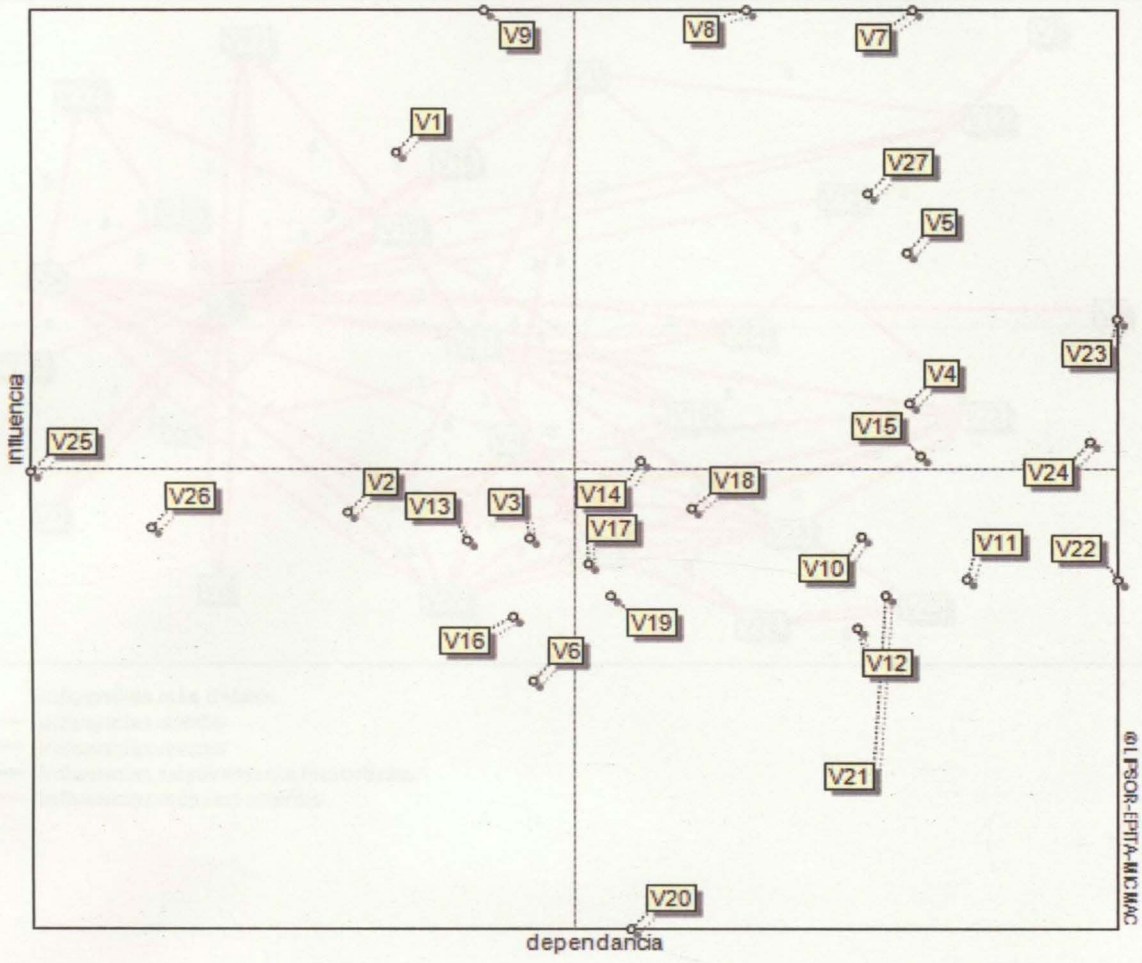
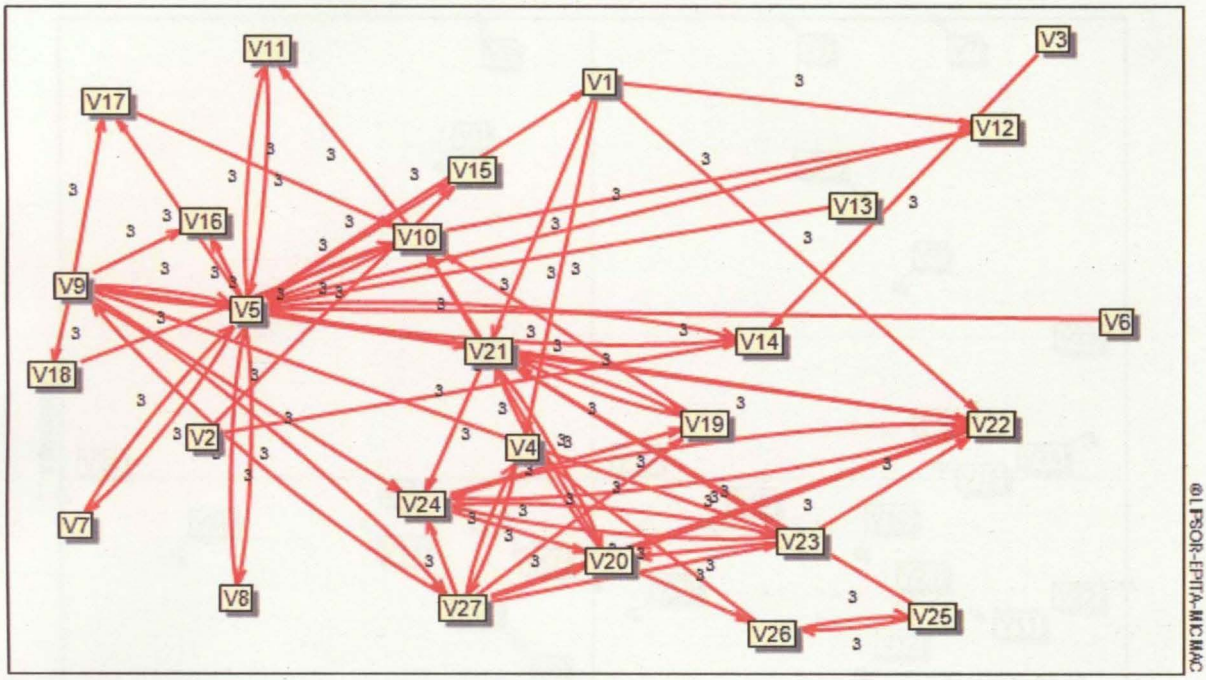
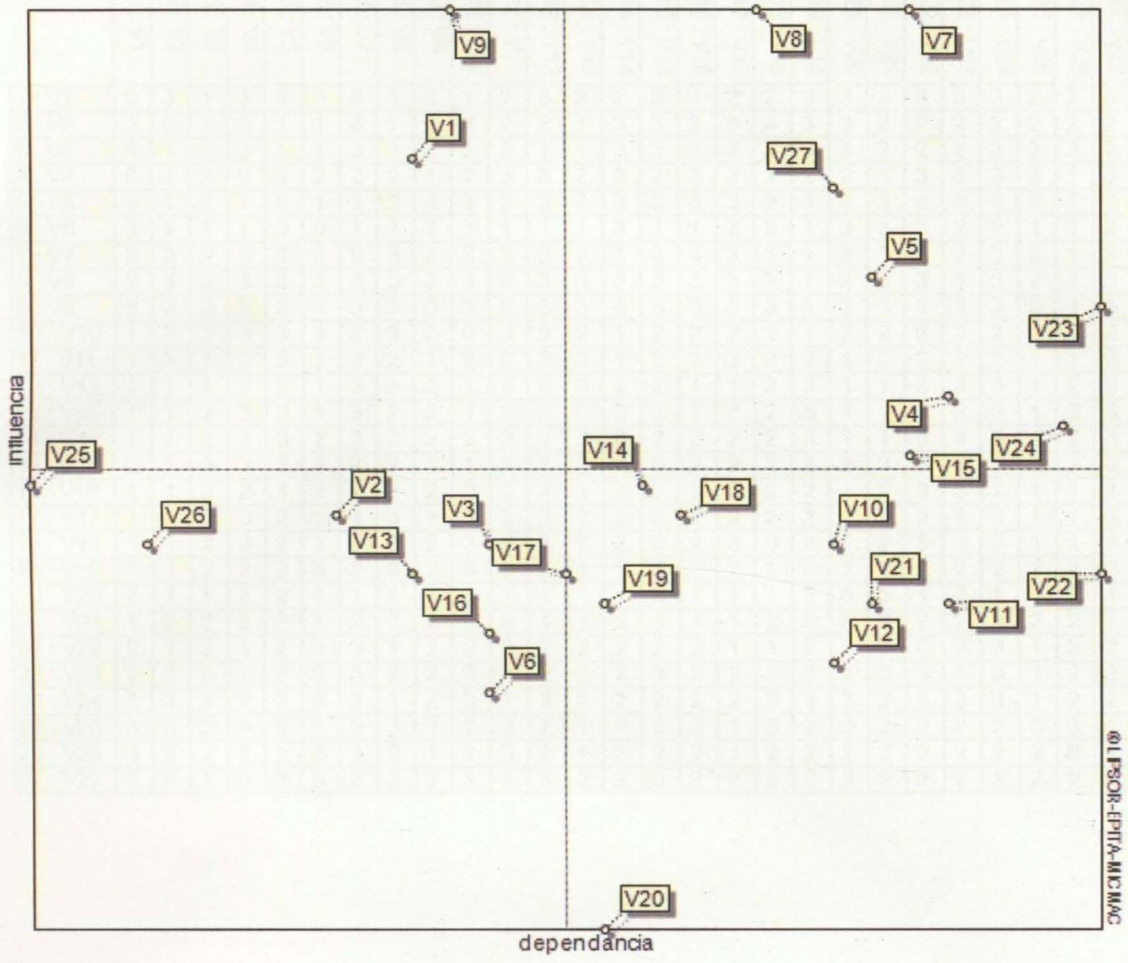


Gráfico de influencias directas potenciales



Influencias más débiles
Influencias débiles
Influencias medias
Influencias relativamente importantes
Influencias más importantes

Plano de influencias / dependencias directas



	1 : V1	2 : V2	3 : V3	4 : V4	5 : V5	6 : V6	7 : V7	8 : V8	9 : V9	10 : V10	11 : V11	12 : V12	13 : V13	14 : V14	15 : V15	16 : V16	17 : V17	18 : V18	19 : V19	20 : V20	21 : V21	22 : V22	23 : V23	24 : V24	25 : V25	26 : V26	27 : V27
1 : V1	0	3	1	3	3	3	3	3	3	1	2	3	3	2	3	2	2	2	3	3	3	3	3	3	2	2	3
2 : V2	3	0	1	3	1	1	3	1	2	2	2	2	1	3	3	2	3	2	3	3	2	2	2	2	2	2	2
3 : V3	3	1	0	3	1	1	3	1	2	2	2	1	1	3	3	2	3	2	3	3	2	2	2	2	2	2	2
4 : V4	2	1	2	0	3	2	2	2	1	2	3	3	2	2	2	3	3	2	2	2	3	3	3	3	2	1	3
5 : V5	3	1	2	1	0	1	3	3	3	3	3	3	2	3	3	3	3	2	1	2	3	3	3	3	2	1	3
6 : V6	3	2	1	1	3	0	1	1	3	3	1	1	1	3	1	1	2	3	1	3	3	3	2	2	1	1	2
7 : V7	3	3	3	3	3	3	0	3	3	3	3	3	3	3	3	3	3	3	1	2	3	3	3	3	2	1	3
8 : V8	3	3	3	3	3	3	3	0	3	3	3	3	3	3	3	3	3	3	1	2	3	3	3	3	2	1	3
9 : V9	3	3	3	3	3	3	3	3	0	3	3	3	3	3	3	3	3	3	1	2	3	3	3	3	2	1	3
10 : V10	1	3	2	3	3	3	2	3	2	0	3	3	2	1	2	2	2	2	1	2	2	2	2	2	1	1	2
11 : V11	1	3	1	3	3	1	3	2	1	2	0	3	3	1	2	2	2	2	2	1	2	2	3	2	1	1	3
12 : V12	1	1	1	2	2	1	3	2	2	1	3	0	3	2	2	1	1	2	3	1	1	3	3	3	1	2	3
13 : V13	1	1	2	3	3	1	3	2	2	1	2	2	0	2	2	2	2	2	3	1	1	3	3	3	1	2	3
14 : V14	1	1	2	3	3	2	3	2	2	2	2	2	3	0	2	2	2	2	3	1	1	3	3	3	1	2	3
15 : V15	2	1	3	3	2	1	2	2	1	1	3	3	2	2	0	2	2	2	2	2	3	3	3	3	2	2	3
16 : V16	1	1	3	2	1	2	2	3	2	2	2	3	1	3	2	0	2	2	2	1	2	3	3	2	1	1	2
17 : V17	1	2	2	3	2	1	1	3	1	3	2	3	2	2	2	2	0	2	2	1	2	3	3	3	1	1	3
18 : V18	1	1	2	3	2	1	1	3	2	3	2	3	2	2	2	2	3	0	2	2	2	3	3	3	1	1	3
19 : V19	1	1	2	2	2	3	2	3	2	3	3	2	1	1	3	1	2	1	0	2	3	2	2	2	2	2	2
20 : V20	2	1	1	2	2	3	1	1	1	3	1	1	1	1	3	1	1	1	2	0	3	1	2	1	1	3	1
21 : V21	1	2	1	3	2	1	2	3	2	3	3	1	1	2	3	1	1	2	3	3	0	2	2	3	2	2	1
22 : V22	2	1	3	1	2	3	3	1	2	2	3	2	2	2	2	2	1	1	2	3	3	0	2	3	1	2	2
23 : V23	2	2	3	1	3	3	3	2	2	3	3	2	2	2	3	2	2	3	2	3	3	3	0	3	1	2	2
24 : V24	1	3	3	1	3	3	3	1	2	3	1	2	2	2	2	2	2	3	3	3	2	3	3	0	1	2	2
25 : V25	3	3	2	3	2	1	3	3	1	2	3	2	1	2	2	2	1	3	2	2	3	2	2	2	0	3	1
26 : V26	3	2	2	3	2	2	3	3	1	2	3	2	1	2	2	2	1	2	2	2	2	2	2	2	3	0	1
27 : V27	2	2	1	3	3	3	2	3	3	3	3	3	2	2	3	2	2	3	3	3	2	3	3	3	2	2	0