ANÁLISIS DE LA CAPACIDAD DE CIBERSEGURIDAD PARA LA DIMENSIÓN TECNOLÓGICA EN COLOMBIA: UNA MIRADA SISTÉMICA DESDE LA ORGANIZACIÓN

Alexis Mauricio Serna Patiño

UNIVERSIDAD PONTIFICIA BOLIVARIANA

ESCUELA DE INGENIERÍAS

MAESTRÍA EN GESTIÓN TECNOLÓGICA

MEDELLÍN

2018

ANÁLISIS DE LA CAPACIDAD DE CIBERSEGURIDAD PARA LA DIMENSIÓN TECNOLÓGICA EN COLOMBIA: UNA MIRADA SISTÉMICA DESDE LA ORGANIZACIÓN

Alexis Mauricio Serna Patiño

Trabajo de grado para optar por el título de Magíster en Gestión Tecnológica

DIRECTORA

PhD. Diana Patricia Giraldo Ramírez

UNIVERSIDAD PONTIFICIA BOLIVARIANA

ESCUELA DE INGENIERÍAS

MAESTRÍA EN GESTIÓN TECNOLÓGICA

MEDELLÍN

2018

23 de agosto de 2018

Alexis Mauricio Serna Patiño

“Declaro que esta tesis (o trabajo de grado) no ha sido presentada para optar a un título, ya sea en igual forma o con variaciones, en esta o cualquier otra universidad” Art 82 Régimen Discente de Formación Avanzada.

Firma

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN

El crecimiento acelerado de las Tecnologías de Información y Comunicación TIC, supone nuevos retos en todos los ámbitos de su gestión para garantizar el desarrollo sostenible de las organizaciones, dentro de los cuales se destaca la ciberseguridad y la infraestructura que la soporta. A partir del paradigma de simulación de la Dinámica de Sistemas, este estudio aborda la dimensión tecnológica de la ciberseguridad referido a la respuesta a incidentes y protección de infraestructuras críticas, tomando como referencia el Modelo de Madurez de la Capacidad de Ciberseguridad y las mejores prácticas definidas por el Instituto Nacional de Estándares y Tecnología. Se parte de la formulación de unas hipótesis dinámicas y la representación de un modelo formal de simulación como medio para el análisis de escenarios y formulación de políticas en este campo. El modelo propuesto evidenció la necesidad de fortalecer los elementos de medición del riesgo de ciberseguridad, así como la mejora en los tiempos de detección, contención de incidentes y restablecimiento del servicio para responder de manera más oportuna a la complejidad y cantidad de los ataques actuales.

Palabras Clave:
Ciberseguridad, respuesta a incidentes, protección infraestructuras críticas, dinámica de sistemas.

ABSTRACT

The accelerated growth of Technology ITC brings new challenges in all areas of management to ensure the economic and sustainable development of companies, within which highlights the cybersecurity and the infrastructure that supports it. Starting from the dynamics system paradigm, this study considers the technological dimension respect to cybersecurity for incident response and critical infrastructure protection, taking as reference the Cybersecurity Capability Maturity Model and the best practices defined by de National Institute of Standards and Technology. We start from the dynamics hypothesis and the representation of a formal simulation model as input to analyze different scenarios and development of future policy in this field. The proposed model evidenced the need to strengthen the cybersecurity risk measurement elements, as well as the improvement in the times of detection, containment of incidents and service recovery in order to respond in a timelier manner to the complexity and quantity of the current attacks.

Keywords:
Cybersecurity, incident response, critical infrastructure protection, system dynamics.

INTRODUCCIÓN

La ciberseguridad como concepto general, ha venido cobrando relevancia por el nivel estratégico que representa, tanto para el ciudadano, como para la sociedad, las empresas y culminando con el país. En 1988 el gobierno de los Estados Unidos generó el primer Equipo de Respuesta a Emergencias Computacionales (*Computer Emergency Response Team – CERT*), después de que el gusano *MORT* paralizara una porción de internet (Cardazzone y Carlini, n.d., p5). Por otra parte, el gobierno de Estonia sufrió el que es el mayor ataque cibernético de la historia, donde se vieron afectadas la presidencia, el parlamento, los ministerios y dos grandes bancos (Ministerio de Interior y Justicia et al., 2011). En el 2009, el gobierno de los Estados Unidos sufrió ataques que afectaron la Casa Blanca, el Departamento de Seguridad Interna, el Departamento de Defensa, entre otros. En el 2010, la guardia española desmanteló lo que, para el entonces, fue considerada la mayor *Bot net* o computadores *zombies* con más de 13 millones de direcciones IP, distribuidas en 190 países del mundo (ídem).

Con base en el Reporte de Riesgo Global, publicado en el 2018, los ataques hacia las organizaciones se han duplicado en los últimos 5 años y los incidentes que en otrora eran considerados extraordinarios, hoy ocupan un lugar más común (World Economic Forum, 2018). Por ejemplo, los ransomwares *WannaCry* y *NotPetya*, afectaron a más de 300.000 computadores en cerca de 150 países con pérdidas cercanas a los US 300 millones, generando riesgos de indisponibilidad del servicio en múltiples compañías incluyendo bancos, empresas de energía, ministerios, entre otros.

Por otra parte Morgan (2017), afirma que el 51% de la población mundial cuenta con acceso a Internet, lo que equivale a 3.8 mil millones de usuarios y proyecta que para el 2030, el 90% de la población, aproximadamente 8.5 mil millones de personas, contará con dicho acceso, lo cual, consecuentemente, aumente los riesgos derivados de la interconectividad.

Según la *Organization for Economic Co-operation and Development* (OECD) (2002, p. 8-9), la creciente interconexión de los sistemas y redes de información aumentan el nivel de exposición al riesgo de afectación de los atributos de información (Integridad, Disponibilidad y Confidencialidad – CIA), por la generación de vulnerabilidades y la proliferación y aumento de diferentes ataques cada vez más complejos, por lo cual, se generan nuevos retos que deben abordarse desde la perspectiva de seguridad de la información y ciberseguridad.

En ese mismo sentido Cort (2015) referencia la importancia de la ciberseguridad a nivel país, denotando un creciente aumento del presupuesto de los objetivos de nación para abordar el asunto, particularmente en los Estados Unidos de América, a través de la creación del Centro de Ciber Comando Unificado que depende de la Agencia de Seguridad Nacional de los Estados Unidos. De igual modo, enuncia un incremento de 8.1%, entre el año 2009 y 2010, del presupuesto anual de ciberseguridad lo que evidencia un reconocimiento del riesgo derivado de la interconexión.

Desde la gestión tecnológica se busca analizar mediante los sistemas, una mejor comprensión de los fenómenos con el fin de planificar y desarrollar soluciones tecnológicas que contribuyan a un mejor desempeño de la organización. En ese sentido se pretende, mediante la elaboración de este trabajo de grado, analizar los principales retos organizacionales que afectan al país en términos de la ciberseguridad, partiendo del *Modelo de Madurez de la Capacidad de Ciberseguridad*, propendiendo por el análisis de políticas que faciliten la toma de decisiones de largo plazo, específicamente en este campo. Por tal motivo, se utilizó una metodología sistémica que ofreciera una aproximación a las características del problema relacionado con la ciberseguridad y que facilite una perspectiva de las relaciones que pueden existir para la detección de incidentes y protección de la infraestructura crítica necesaria para el desarrollo del país. Lo anterior fue traducido en un modelo de simulación computacional, de manera que se pudieran analizar los efectos en la toma de decisiones y evaluación de políticas a largo plazo.

Este documento presenta en el Capítulo 1, un marco teórico general que permita un entendimiento de la ciberseguridad en el mundo y los esfuerzos realizados para entender el fenómeno desde los sistemas y el diseño de modelos para su abordaje. El Capítulo 2, desarrolla el enfoque de la investigación, definiendo el problema, la hipótesis y los objetivos planteados en el proyecto de investigación. El Capítulo 3 presenta la metodología utilizada para abordar el enfoque de la investigación basado en el paradigma de simulación de la Dinámica de Sistemas. En el Capítulo 4 se presentan los resultados obtenidos a partir del enfoque sistémico abordado. Finalmente se consignan las conclusiones de la investigación y se sugiere el trabajo futuro que puede complementar los resultados.

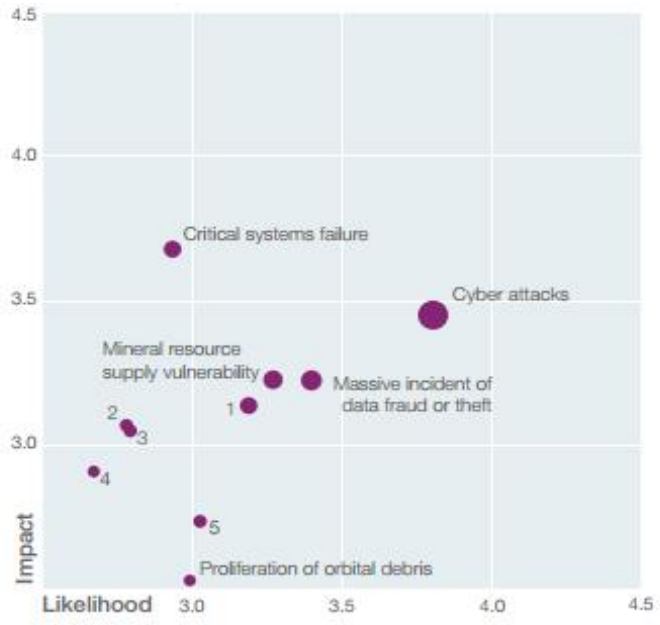
CAPITULO 1

1. MARCO TEÓRICO

Según la OECD (2012, p. 13), las amenazas cibernéticas se han desarrollado e incrementado de manera acelerada. Dichas amenazas son ejecutadas tanto por criminales como por otros países y grupos políticos que poseen diversas motivaciones como, por ejemplo: hacer dinero, el "*hacktivismo*", la desestabilización de las naciones (Estonia en 2007), ciberespionaje, sabotaje y operaciones militares.

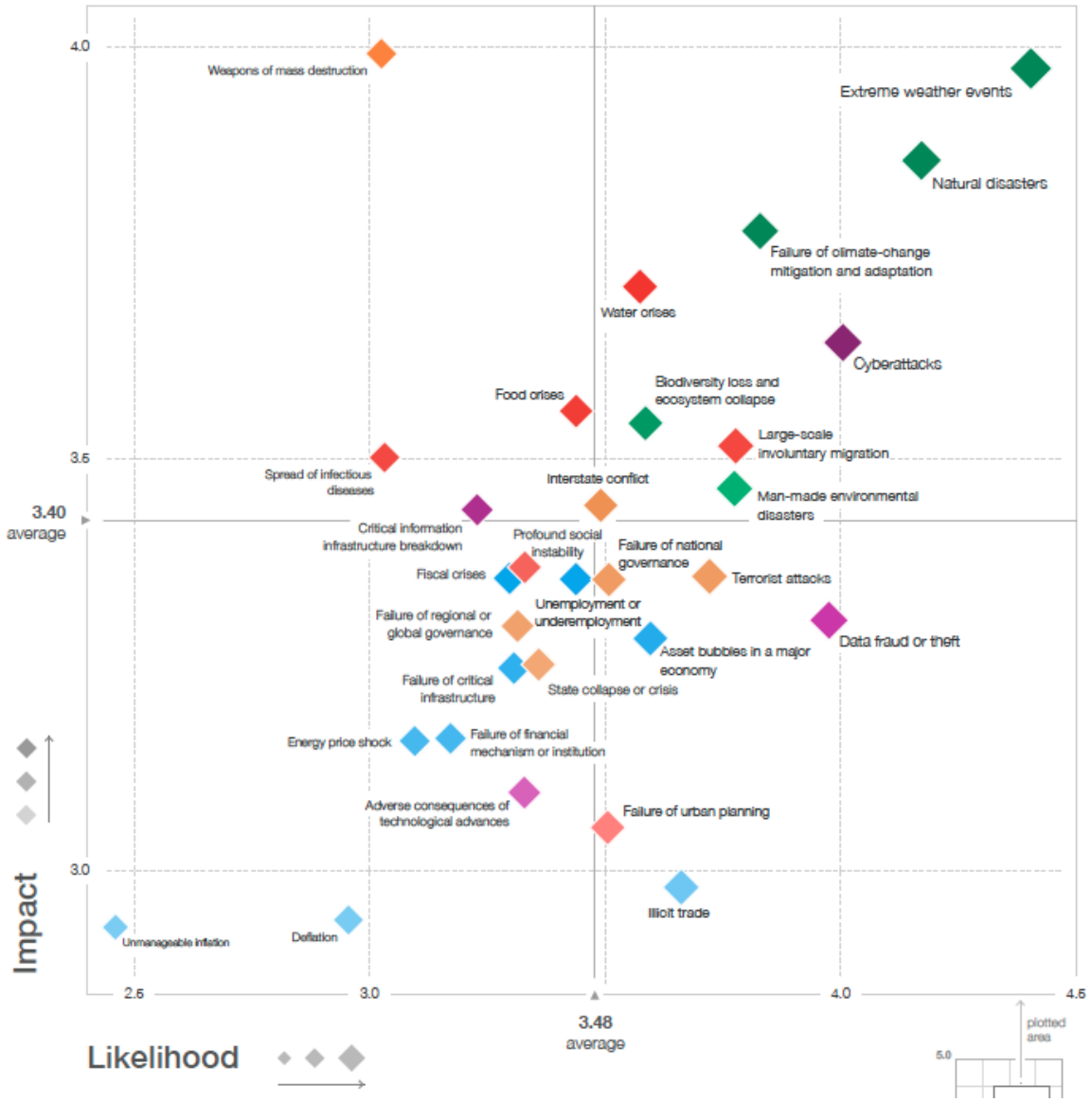
Las Figuras 1 y 2, muestran el riesgo desde su aparición en el reporte mundial del *World Economic Forum*, en el 2012 y su estado en el 2018 las cuales evidencian un creciente aumento de los ciberataques y de las fallas de los sistemas críticos que se han desplazado en la probabilidad de ocurrencia pasando de 3.7 (aproximadamente) en el 2012 a 4 para los ciber ataques y de 2.8 a 3.8 aproximadamente para las fallas de los sistemas críticos.

Figura 1. Technological Risk 2012.



Fuente: Global Risk 2012. 7th Edition. (World Economic Forum., 2012)

Figura 2. Technological Risk 2018.



Fuente: The Global Risks Report 2018. 13th edition.(World Economic Forum, 2018)

Por otra parte, con el desarrollo de las Tecnologías de Información y comunicación (TIC), el acceso cada vez más alcanzable de las tecnologías para todos los ciudadanos, la penetración de internet y los esfuerzos de los países de masificar la misma, han venido incrementando los riesgos de ciberseguridad dado que, cada vez es más fácil encontrar información para

realización de ataques cibernéticos, se desarrollan técnicas de ataques de ingeniería social, entendida como el proceso para influenciar a las personas para divulgar información sensible (Mouton, Malan, Leenen, y Venter, 2014); evolucionan herramientas donde una persona con conocimientos medios podría realizar grandes explotaciones de vulnerabilidades, es decir, aprovecharse de las debilidades de control en las tecnologías de información y/o comunicación para obtener acceso no autorizado en beneficio propio o de terceros; se hacen públicos los vectores de ataque y se convierten en herramienta de código abierto (*open source*) para uso y desarrollo público, entre otros.

En cuanto a las tecnologías de operación, el nivel de riesgo ha venido aumentando con el cambio de tecnología que se presenta en el soporte a la operación de las organizaciones, pasando de protocolos propietarios y de arquitectura cerrada, a protocolos TCP/IP, lo que conecta con internet y eleva los niveles de exposición de los mismos.

Según Miniwatts Marketing Group (2015) sobre el porcentaje de penetración de internet en el mundo, tal y como lo evidencia la Tabla 1 se encuentra que ha habido un crecimiento representativo del internet en el mundo, lo que, a su vez, representa una elevación en los niveles de riesgos asociados a la ciberseguridad en todos los entornos: social, económico, de seguridad, etc. Por lo que resulta relevante entender los componentes del sistema que ayuden en la toma de decisiones enfocadas a fortalecer la ciberseguridad.

Tabla 1. Estadísticas de uso de internet a nivel mundial.

Regiones del mundo	**Población (2018 Estimada)**	**Población % del mundo**	**Usuarios de Internet 31-dic-17**	**Penetración (% población)**	**Crecimiento 2000-2018**
Africa	1.287.914.329	16,9%	453.329.534	35,2%	9941%
Asia	4.207.588.157	55,1%	2.023.630.194	48,1%	1670%
Europa	827.650.849	10,8%	704.833.752	85,2%	570%

Tabla 1. Estadísticas de uso de internet a nivel mundial.

Regiones del mundo	Población (2018 Estimada)	Población % del mundo	Usuarios de Internet 31-dic-17	Penetración (% población)	Crecimiento 2000-2018
América Latina y el Caribe	652.047.996	8,5%	437.001.277	67,0%	2.318%
Medio Este	254.438.981	3,3%	164.037.259	64,5%	4.893%
Norte América	363.844.662	4,8%	345.660.847	95,0%	219%
Oceania / Australia	41.273.454	0,6%	28.439.277	68,9%	273%
TOTAL mundial	**7.634.758.428**	**100,00%**	**4.156.932.140**	**54,40%**	**1.052%**

Fuente: Adaptado de Miniwatts Marketing Group. 2018

Latinoamérica en general, ha tenido un incremento del 2.318% de crecimiento desde el año 2000 hasta el 2018, lo cual representa un crecimiento acelerado en la penetración del internet en los países que allí se circunscriben. Por su parte, Colombia ha tenido una penetración del uso de internet de 63.2% respecto a su población (Miniwatts Marketing Group., 2018b), lo cual supone también un crecimiento proporcional de los riesgos asociados a ciberseguridad. En otras palabras, el uso de internet per sé, conlleva a riesgos de afectación a los atributos de información.

Aunque es notable el crecimiento en términos de penetración de internet en Colombia, el BID y la OEA, (2016) en su informe Seguridad Cibernética en América Latina y el Caribe, afirma que aún falta por otorgar acceso a un porcentaje representativo de la población, cerca del 47% de la población total. En otras palabras, dado que existe una cantidad de población representativa sin acceso a internet, y si Colombia pretende desarrollar este campo, como lo menciona Ministerio de Tecnologías de la Información y las Comunicaciones (2008) en su Plan Nacional de TIC (PNTIC), deberá tenerse especial atención a los temas asociados a la

ciberseguridad, procurando un crecimiento adecuado, no solo desde la tecnología, la política, legislación, sino también desde la educación, y la sociedad.

En el mismo documento, Porrúa y Contreras (2016) y dentro del modelo de madurez propuesto, establece que Colombia se encuentra en un nivel formativo en lo que respecta a tecnología: "*La tecnología y los procesos de seguridad en el gobierno y el sector privado están disponibles y desplegados; el mercado interno ofrece productos genéricos, no especializados; las ofertas no están impulsadas por el mercado; consideraciones de seguridad están integradas en el software y la infraestructura"*. Lo anterior permite suponer que se deben realizar esfuerzos estructurados y sistémicos para alcanzar niveles superiores de madurez de la ciberseguridad en Colombia.

Los datos de Colombia, proyectados por el Departamento Nacional de Planeación (2016, p. 11), muestran la perspectiva que se estima a 2020 en términos de penetración y uso de internet, asociando terminales y evidenciando la cantidad de datos posibles para dicha época. Se estima que, en el 2020, habrá un incremento del 33% en usuarios de banda ancha móvil respecto al 2015; un crecimiento del 49% en las terminales conectadas y un crecimiento del 132% en el tráfico IP de red para el espacio de tiempo mencionado.

Es posible afirmar que las TIC apoyan el crecimiento de las naciones en la era digital, propiciando la innovación y potenciando la economía de manera proporcional al crecimiento de internet, lo que incluye no solo a la sociedad sino también a los gobiernos toda vez que las TIC se convierten en elemento indefectible en el mundo actual (OECD, 2012, p. 12).

1.1 Índice Mundial de Ciberseguridad

La ciberseguridad y su avance, se ha pretendido medir desde diferentes modelos a través de diversas organizaciones. Por ejemplo, la Unión Internacional de Telecomunicaciones (ITU, 2015), desarrolló el Índice Mundial de Ciberseguridad (IMC) a través de un trabajo conjunto con la *ABI Research*, que pretende medir el nivel de compromiso de los estados soberanos

respecto a la ciberseguridad. Dicho índice se fundamenta en cinco ámbitos o dimensiones a saber: medidas jurídicas, medidas técnicas, medidas organizativas, creación de capacidades y cooperación internacional. En ese sentido, el resultado es un indicador de país que permite identificarlo en una clasificación mundial en términos de la preparación del país para atender los asuntos relacionados con la ciberseguridad. El IMC, entonces, pretende medir la existencia de estructuras nacionales para implementar y promover la ciberseguridad (ITU, 2015 p 11).

La investigación arrojó que Colombia tiene un índice de 0.588, ocupando la posición número 9 a nivel mundial, lugar que comparte con países como Dinamarca, Egipto, Francia y España. Dicho estudio está liderado por Estados Unidos de América con una puntuación de 0.824, seguido por Canadá y Australia. Lo anterior evidencia una posición relativamente importante de Colombia bajo esta medición, mostrando adicionalmente la necesidad de fortalecer algunos elementos asociados a la ciberseguridad para poder responder a los riesgos que conlleva la tecnología de manera eficiente, eficaz y oportuna.

1.2 Modelos de madurez

El *US Department of Homeland Security* (2014, p10) menciona tres modelos de madurez propuestos como se menciona en la Tabla 2. Cada modelo se enfoca en diferentes variables que finalmente pretenden determinar el nivel de madurez de la capacidad de la ciberseguridad asociados cada uno a actividades particulares.

Tabla 2. Niveles de madurez US Department of Homeland Security.

Organización	Niveles de modelo
The Newman Group	Básico
	Intermedio
Talent Strategy Advisors	Cauteloso
	Táctico
	Sólido
	Operacional

Tabla 2. Niveles de madurez US Department of Homeland Security.

Organización	Niveles de modelo
Infohrn	Optimista Inicial Intermedio Avanzado

Fuente: Adaptado de (US Department of Homeland Security, 2014)

Ahora bien, el modelo propuesto por la University of Oxford (2014, p3-4) establece 5 niveles de madurez según se observa en la Tabla 3.

Tabla 3. Modelo Universidad de Oxford.

Nivel de madurez	Descripción
1. Inicial	En este nivel existen pocos controles o son embrionarios. Podría incluir discusiones iniciales sobre la capacidad de la ciberseguridad, pero sin medidas concretas o inconmensurables.
2. Formativo	Existen algunas características de los indicadores que se comienzan a formular y a crecer, pero pueden ser ad-hoc, desorganizados, definidos pobremente o simplemente son nuevos. Sin embargo, existe evidencia clara de esa actividad
3. Establecido	Los elementos del subfactor son adecuados y funcionan. Poca decisión sobre la inversión de los diferentes elementos que lo componen. Existen indicadores funcionales y definidos
4. Estratégico	Se tienen identificadas las partes más importantes de los indicadores y cuáles son más o menos importantes en una organización o país en particular. Refleja las decisiones que se han tomado con un conjunto finito de recursos sobre los indicadores más importantes.
5. Dinámico	Existen mecanismos claros para alterar la estrategia, dependiendo de las circunstancias. Se cuenta con mecanismos claros para tomas rápidas de decisiones, reasignación de recursos, y atención constante a los cambios del entorno

Fuente: Adaptado de (University of Oxford, 2014)

Todos los modelos pretenden finalmente, proporcionar elementos de juicio para la toma de decisiones, referente a dónde se debería invertir más o cuál desempeño se debería mejorar. Se reconoce, además, que existen relaciones entre cada uno de los niveles del modelo, donde el nivel n+1 requiere del nivel n.

De igual forma, el modelo propuesto por University of Oxford, (2014, p 3), sugiere 5 dimensiones:

1. Concepción de la política de ciberseguridad y la estrategia
2. Fomentar la cibercultura responsable en la sociedad
3. Crear habilidades de ciberseguridad en la fuerza de trabajo y el liderazgo
4. Crear marcos legales y regulatorios efectivos
5. Controlar los riesgos a través de la organización, las normas y la tecnología

Cada dimensión tiene asociado un conjunto de subfactores que permitirán determinar el estado de la madurez del sistema de cada uno de ellos. La complejidad de la ciberseguridad en cualquier entorno, es decir, organizacional o de nación, requiere constantemente de la toma de decisiones por parte del ser humano, las cuales pueden ser tomadas incluso a través de la tecnología. Las acciones derivadas de ellas pueden ser de corto, mediano o largo plazo, por lo que se deben analizar de manera sistemática, sistémica y organizada, conjuntos de variables o datos que cambian constantemente, reconociendo la dinámica normal de la ciberseguridad en un mundo cada vez más conectado.

A su vez NIST (2014), en el marco de trabajo para el mejoramiento de la ciberseguridad en las infraestructuras críticas, propone como componente adicional y fundamental, la gestión de riesgos, como elemento relevante para la toma de decisiones, por lo cual, el nivel de consciencia organizacional y su apetito por el riesgo, determinarán el nivel de inversión y, por lo tanto, las acciones a llevar a cabo para robustecer los mecanismos definidos para el "*hardening*" o endurecimiento de los controles asociados a la ciberseguridad.

Existe evidencia documentada sobre esfuerzos realizados para robustecer la seguridad de la información. Por ejemplo, desde el año 1999, Kossakowski, Allen, Alberts, Cohen y Ford, proponían una serie de recomendaciones prácticas, que pueden ser aún aplicables, con el fin de dar respuesta a las intrusiones que podrían derivarse de la conectividad. En ese sentido, resaltaban la necesidad de entender la extensión y las fuentes de la intrusión, así como el imperativo de proteger los datos sensibles, los sistemas, las redes, propendiendo por la continuidad de la operación y la recuperación después de materializarse un ataque. De igual modo, la recolección de la información y de la evidencia para investigaciones posteriores, incluida la legal, son resaltadas como parte importante en el manejo de incidentes. Dichas recomendaciones son resumidas en la Tabla 4.

Tabla 4. Resumen de prácticas de seguridad recomendadas.

Categoría	**Recomendación**
Preparación	1. Establecer políticas y procedimientos para responder a intrusiones
	2. Preparación para responder a intrusiones
Manejo de incidentes	3. Analizar toda la información disponible para caracterizar la intrusión
	4. Comunicar a todas las partes el progreso de la intrusión y su estado
	5. Recolectar y proteger la información asociada con la intrusión
	6. Aplicar soluciones de corto plazo para contener la intrusión
	7. Eliminar todas las formas de acceso del atacante
	8. Retornar el sistema al estado normal de operación
Acciones posteriores	1. Identificar e implementar lecciones aprendidas de seguridad

Fuente: (Kossakowski et al., 1999)

1.3 Ciberseguridad desde la Dinámica de Sistemas

Con el panorama expuesto, es necesario abordar el tema desde la simulación computacional, con el fin de realizar una aproximación de entendimiento al fenómeno generado por la misma, desde diferentes perspectivas. Para ello, el paradigma de simulación conocido como la Dinámica de sistemas (DS) es una herramienta fundamental para modelar y simular las relaciones existentes dentro del sistema. Forrester (1992), afirma que la DS posee “una

habilidad única para representar el mundo real". En ese sentido, utilizar este paradigma permitiría tener una aproximación al entendimiento de la realidad bajo perspectivas sistémicas, posibilitando el estudio y la elaboración de conclusiones que faciliten el proceso de toma de decisiones.

Cappelli et al. (2006) utiliza la DS para evidenciar la ausencia de herramientas que permitan comprender el riesgo existente, en términos de ciberseguridad, de las amenazas internas de las organizaciones, realizando simulaciones de políticas, culturales, técnicas y factores procedimentales. Por su parte, Cardazzone y Carlini. (n.d.) propusieron un modelo a partir de la DS, para analizar el impacto de algunos ciberataques en los sistemas de defensa nacionales y la forma en cómo las organizaciones creadas para contrarrestarlos (CERT) han respondido a ellos, donde se concluye que, si bien es necesario tener mecanismos apropiados de detección de ataques, es relevante determinar el impacto real de los mismos para minimizar daños no previstos en los ataques.

Otros autores como Canzani y Pickl (2016) han simulado, a través de la DS y la combinación teórica de juegos, a la ciberseguridad en la protección de las infraestructuras críticas mediante la definición de escenarios proactivos y reactivos de defensa reconociendo ataques cada vez más complejos de detectar y contener, concluyendo que "la costo-eficiencia de las defensas periódicas depende de la optimización de los componentes de tiempo de prevención más que de las inversiones de TI (Tecnologías de Información) en los planes de recuperación".

Igualmente, Flórez et al. (2016) realizaron un estudio sobre el ecosistema de la ciberseguridad en Colombia, a través de la DS, afirmando que el diagrama de influencias creado, ayuda a entender la necesidad de prevenir el cibercrimen, observando, adicionalmente, que la soberanía es el elemento principal que no influye en los otros elementos; sin embargo, concluyen que debe ser el principal elemento a proteger dentro del ecosistema de ciberseguridad en Colombia, junto con recursos y activos que pueden verse afectados por la comisión de ciberdelitos. En resumen, el modelo muestra la necesidad de proteger la soberanía y la reducción de los ciberdelitos dentro del ecosistema modelado.

Por su parte, en el Encuentro Colombiano de Dinámica de Sistemas XIV Ecds, (2016), en la ponencia “La Seguridad de la Información desde la Dinámica de Sistemas” concluye que:

> Aunque es el primer esfuerzo por entender el comportamiento de la Seguridad de la Información mediante la DS, es interesante ver los resultados y como estos están alineados a la hipótesis planteada con el modelamiento de la Seguridad de la Información, donde se ratifica que la coexistencia entre stakeholder y atacantes, se intensifica dada la existencia de activos, por ende el stakeholder tendrá que hacer esfuerzo (inversión) en controles para mitigar la materialización del riesgo (impacto) y con ello que se degraden los activos. (Parada Serrano y Gómez Prada, 2016)

En ese sentido, se reconoce la importancia de la seguridad de la información y de la DS para comprender de manera sistémica, la complejidad asociada a la ciberseguridad, que permita aproximarse a la identificación de elementos que pueden contribuir al mejoramiento del sistema y, por ende, ofreciendo una visual de dónde se deberían invertir los recursos para mejorarla.

CAPÍTULO 2

2. ENFOQUE DE LA INVESTIGACIÓN

2.1 Problema

Colombia como país, ha realizado esfuerzos evidentes, como por ejemplo la generación del Conpes 3701 dándole vida al CERT colombiano cuyo objetivo no dista de la definición principal enunciada por Cardazzone y Carlini, (n.d.), el cual se enmarca en proteger la seguridad y la economía nacional propendiendo por la continuidad de las operaciones en caso de un incidente de seguridad; y el Conpes 3854, definiendo la política de ciberseguridad para Colombia (Ministerio de Interior y Justicia et al., 2011; Ministerio de Interior y Justicia et al., 2016) para enfrentar los desafíos emergentes de la ciberseguridad, y en ese sentido, el Gobierno colombiano ha desarrollado avances importantes alineados con el Banco Interamericano de Desarrollo (BID) y Organización de Estados Americanos (OEA) (2016) en materia de políticas, marcos legales y tecnología respecto a la ciberseguridad.

De igual manera, el Consejo Nacional de Operación, considerando el Conpes 3701, aprueba la guía de Ciberseguridad, mediando el acuerdo 788, donde motiva a los agentes generadores, transmisores y distribuidores del Sistema Interconectado Nacional a realizar la identificación de los activos y ciberactivos críticos, los riesgos y vulnerabilidades y el nivel de gestión de la ciberseguridad en las operaciones de las empresas, reconociendo así, la importancia del tema en la continuidad nacional.

Porrúa y Contreras (2016) en su estudio: Ciberseguridad. ¿Estamos preparados en América Latina y el Caribe? expone los resultados de la evaluación de la madurez en los países de América Latina y el Caribe bajo el modelo el Modelo de Madurez de la Capacidad de la

Ciberseguridad (CMM), desarrollado por el Centro Global de Capacidad sobre Seguridad Cibernética Oxford (GCSCC), el cual contempla la dimensión tecnológica como crítica.

Considerando entonces a Porrúa y Contreras, es necesario tener en cuenta que las variables descritas en el CMM no podrán ser ni estáticas ni independientes, lo cual supone una dinámica normal dentro del sistema que deberá servir a los tomadores de decisiones a realizar inversiones en pro del desarrollo y evolución de la Ciberseguridad en Colombia y, por tanto, de las organizaciones que aportan al desarrollo del país. Finalmente, con base en la revisión de la literatura, no se encuentra suficiente evidencia que muestre la dinámica del sistema asociado al modelo de madurez de la capacidad de la ciberseguridad en la dimensión tecnológica (respuesta a incidentes y protección de la infraestructura crítica nacional) que facilite la toma de decisiones para fortalecer los elementos allí consignadas y permitan tener un entendimiento de la interrelación existente en cada una de ellas.

2.2 Hipótesis

Si bien Colombia ha tenido adelantos en materia de política, legislación y tecnología para mejorar su nivel de Ciberseguridad, a partir de la modelación de la dimensión tecnológica del modelo CMM, particularmente en la respuesta a incidentes y protección de la infraestructura crítica nacional, se podría comprender, bajo la DS, las relaciones complejas que pueden existir en dicha dimensión, propendiendo por adecuar o robustecer las políticas que favorezcan el desempeño del sistema de la ciberseguridad en Colombia aplicadas en las empresas que soportan las infraestructuras críticas del país.

2.3 Objetivos

2.3.1 Objetivo General

Analizar la capacidad de la ciberseguridad en la dimensión tecnológica en lo que concierne a respuesta a incidentes y protección de la infraestructura crítica en Colombia bajo una perspectiva sistémica desde la organización.

2.3.2 Objetivos Específicos

- Realizar una descripción de las relaciones sistémicas existentes dentro del modelo CMM en la dimensión tecnológica respecto a respuesta a incidentes y protección de la infraestructura crítica nacional.

- Realizar un modelo de simulación bajo la DS para poder entender la complejidad del mismo (representar las relaciones encontradas en el objetivo 1).

- Realizar una validación del modelo a partir del comportamiento detectado en la dimensión tecnológica del modelo CMM evaluado por Porrúa y Contreras (2016).

- Analizar escenarios y posibles políticas que ayuden a un mejor desempeño del sistema en la dimensión analizada.

CAPITULO 3

3. METODOLOGÍA

En el capítulo anterior se describió el problema de investigación, con el cual fueron formulados los objetivos para desarrollar este trabajo de grado. En este capítulo se presenta la selección de la metodología a utilizar.

3.1 Selección de la metodología de investigación

Se debe puntualizar que este trabajo de grado parte del Modelo de Madurez de la Capacidad de Ciberseguridad y las mejores prácticas definidas por el Instituto Nacional de Estándares y Tecnología. Se eligió este modelo debido a que aborda de manera integral el sistema de ciberseguridad. Es un modelo amigable y transparente que fue validado por la comunidad internacional.

Se parte de un modelo de simulación, por lo que hay que entender que toda simulación parte del desarrollo de un modelo que pueda reproducir de manera aproximado el mundo real. Este proceso se realiza mediante la selección de las partes que el investigador crea significativas, acoplándolas para reproducir el comportamiento (Friedman y Cassar, 2004). Las ventajas de simular son:

- Comprender un problema real y se hace necesaria cuando las soluciones analíticas son inviables (Vennix, 1996).
- Reduce los problemas de la capacidad limitada de la mente humana cuando se hacen simulaciones mentales, por lo que los modelos computaciones se vuelven en una herramienta útil para estudiar estructuras complejas (Forrester, 1971; J.D. Sterman, 1991).

- Analizar diferentes políticas sobre las variables clave dentro de los modelos y formular estrategias que puedan ser aplicadas en el mundo real para tomar decisiones más acertadas que lleven a un mejor comportamiento del sistema (J.D. Sterman, 2000).

La selección de la metodología de simulación depende de la utilidad que tenga el modelo y de las características que tengan los sistemas. Es prioritario conocer las características del problema dentro del sistema a estudiar y cada una de las herramientas de simulación y sus aplicaciones para poder seleccionar el más adecuado para el problema a estudiar (Dyner, 1993; Dyner, Peña, y Arango, 2008).

Para la selección de la DS como paradigma a utilizar, fueron identificadas las principales características de la capacidad de ciberseguridad en la dimensión tecnológica. El principal aporte desde la DS se centra en:

- Se pueden utilizar aproximaciones continuas en su representación,
- La aleatoriedad solo puede explicar el comportamiento en el corto plazo,
- Las no-linealidades de los sistemas socio-económicos,
- Las aproximaciones lineales se dan en el corto plazo y,
- Los retardos en el sistema y los ciclos de realimentación juegan un papel fundamental dentro del problema.

3.2 Método de simulación en Dinámica de Sistemas

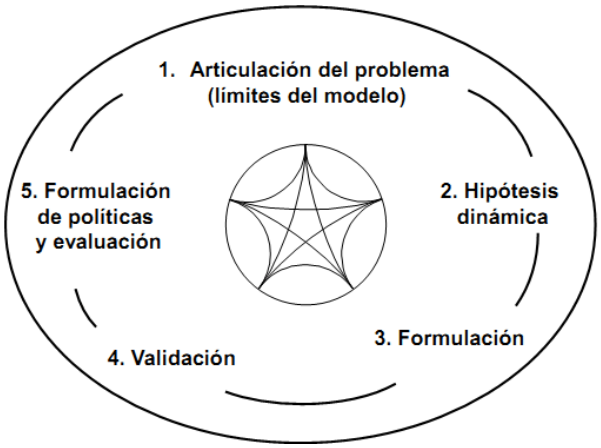
El paradigma de simulación seleccionado fue la DS, que considera para la simulación dos objetos fundamentales: los niveles (variables de estado) que se ocupan de la acumulación de la información o de material y los flujos que son los *inputs* y *outputs* de los niveles. El trasfondo matemático de estas estructuras son ecuaciones diferenciales formuladas de primer orden, no lineales.

Adicionalmente se soporta en aspectos tan importantes como los ciclos de realimentación, relaciones no lineales y retardos (Morecroft, 2007). Sterman (2003) define los diagramas causales como mapas que evidencian las relaciones causales entre las variables, donde se parte de una causa y se llega al efecto. Por otra parte, los diagramas causales permiten identificar las conexiones entre las partes del sistema, de una manera clara y concisa (Morecroft, 2015 p52). Las relaciones de causa – efecto son ilustradas a partir de flechas que parten de la primera hasta llegar a la última. La polaridad, positiva o negativa, ubicada en las partes superiores de las flechas, señala el efecto que tiene la variable causa en la variable efecto, esto es, cómo la variable x (causa) influyen en el efecto y (efecto), la cual se denota por la ecuación (1):

$$x \to +y \Rightarrow \frac{dy}{dx} > 0; x \to -y \Rightarrow \frac{dy}{dx} < 0 \qquad (1)$$

Para dicha formulación es necesario seguir un proceso iterativo que consta de los siguientes pasos según se observa en la Figura 3.

Figura 3. Proceso de Modelado en Dinámica de Sistemas



Fuente: Tomado de Sterman (2000)

3.3 Proceso de modelación en dinámica de sistemas

El proceso de modelación es iterativo y cuenta con 5 pasos, no quiere decir que se deban llevar a cabo en un orden específico dado que se puede pasar de uno a otro en cualquier momento de la modelación (Sterman, 2000).

1. ***Articulación del problema:*** Para empezar el proceso de modelación es necesario tener claro un objetivo o una pregunta para guiar la investigación. En primer lugar, se debe identificar el problema, su comportamiento y sus variaciones en el tiempo. Para cumplir este fin se pueden usar series de tiempo o descripciones del problema y a este proceso se le llama "modo de referencia". Para el proceso de validación en el que se le da confianza al modelo es necesario que la simulación sea capaz de replicar el comportamiento descrito en los modos de referencia. En esta etapa de la modelación también se debe identificar los límites del modelo, el tiempo de simulación adecuado para observar los comportamientos y el marco donde la aplicación es funcional.

2. ***Planteamiento de una hipótesis dinámica:*** Es necesario explicar el comportamiento del sistema, para ello se fórmula una hipótesis dinámica. En este paso se analizan las relaciones causales existentes en las variables que se han identificado como significativas para el modelo. Para poder realizar este paso es necesario definir cuáles son endógenas (variables explicativas y que cambiarán durante el modelo de la simulación debido a las dinámicas existentes dentro del modelo) y exógenas (variables de entrada, parámetros y que no se ven afectadas por la simulación). Una herramienta útil para este proceso son los Diagramas Causales, ya que permite observar de manera gráfica las relaciones existentes entre las variables, indicando ciclos y retardos y a partir de estos elementos explicar el comportamiento del sistema estudiado.

3. ***Formulación del modelo matemático:*** En esta etapa, se convierte la hipótesis dinámica en un diagrama de flujo en el que se formulan las expresiones matemáticas que describa las relaciones entre las variables (Dyner et al., 2008; J. Morecroft, 2007;

J.D. Sterman, 2000). En esta etapa se estiman los parámetros y los valores iniciales de los niveles, para ello existen diferentes metodologías para esta estimación (Dyner, 1993; Richardson y Pugh, 1989) . Para poder simular se debe calibrar el modelo para que pueda representar de manera adecuado el modo de referencia.

4. ***Validación del modelo:*** La Dinámica de Sistemas no es exigente de información histórica, se pueden hacer supuestos subjetivos, aunque debe anotar las limitaciones que esto conlleva. Lo anterior es debido a que los modelos bajo esta metodología no pretenden proyectar y pronosticar los valores exactos de las variables, sino que es una herramienta para probar políticas y entender el comportamiento desde la estructura (Dyner, 1993). En esta etapa se busca darle confianza y robustez al modelo, aunque cabe anotar que el modelo solo sirve para la utilidad con la que se diseñó (Forrester y Senge, 1980; Sterman, 2002). Se busca validar tanto la estructura como el comportamiento (Barlas, 1996). Brindándole confianza a la estructura, garantiza que la hipótesis dinámica planteada describe de manera adecuada el sistema real, mientras que la validación en el comportamiento trata de darle robustez a la captura de la dinámica del sistema estudiado (Barlas y Carpenter, 1990; Sterman, 2000). En este punto de la modelación se realiza análisis de sensibilidad para tener un mayor entendimiento de las dinámicas del modelo y poder identificar a que parámetros es más sensible. Los resultados de este análisis permiten la identificación de posibles puntos de apalancamiento en el mundo real o posibles debilidades en la estimación de parámetros.

5. ***Análisis de políticas:*** El análisis se centra en los nodos de decisión del modelo y estudiar los efectos producidos por los cambios estructurales y paramétricos propuestos en las políticas. Una buena política es aquella que sea insensible a los cambios en el modelo, que den una solución al problema y que evite comportamientos contra intuitivos (Forrester, 1971). En este punto se analiza el modelo bajo diferentes escenarios y el objetivo es que estos conlleven a la estabilidad y mejor comportamiento del sistema.

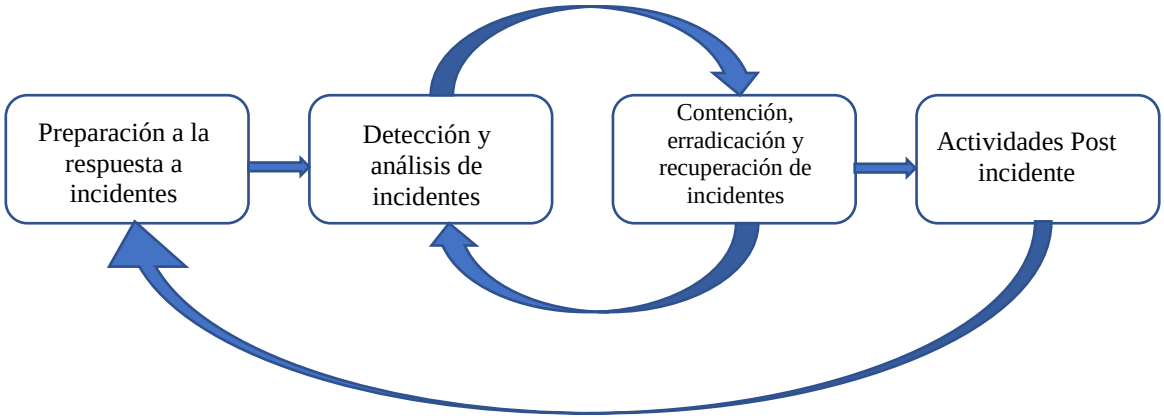
CAPITULO 4

4. RESULTADOS

Para aportar en el entendimiento de las posibles relaciones existentes en el problema definido, el marco de trabajo de ciberseguridad definido por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos – NIST por sus siglas en inglés, define 5 principios fundamentales. A saber: Identificar, proteger, detectar, responder y recuperar, sobre lo cual, Ferrillo y Veltsos (2016), afirma que son un instrumento útil para las organizaciones para hacer frente a los riesgos de ciberseguridad buscando responder a las amenazas y desarrollar el mejoramiento continuo, bajo marcos internacionales, respecto a la respuesta a incidentes y protección de infraestructuras críticas enfrentando las amenazas derivadas de la interconectividad.

En ese orden de ideas, Cichonski (2012) propone el siguiente diagrama, que se puede observar en la Figura 4, para el ciclo de vida de la Respuesta a Incidentes. Dicha propuesta representa un punto de partida relevante para el análisis y comportamiento del sistema en lo concerniente a respuesta a incidentes y protección de infraestructuras críticas.

Figura 4. Ciclo de vida de la respuesta a incidentes.



Fuente: Adaptado de Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology (Cichonski, 2012).

4.1 Horizonte de tiempo para la investigación

Para la investigación, se definió un horizonte de tiempo de 20 años medidos en días, cuya fecha inicial para el modelo, con base en los datos obtenidos es desde el 2015 y se simula hasta el 2035.

4.2 Variables y subsistemas excluidos

Para el desarrollo del modelo se identificaron las principales variables, clasificadas en endógenas y exógenas, así como los subsistemas excluidos del análisis, las cuales se identifican en la Tabla 5.

Tabla 5. Principales variables identificadas y subsistemas excluidos.

Variables exógenas	Variables endógenas	Subsistemas excluidos
Número de eventos	Incidentes detectados y analizados	Desarrollo de tecnología en hardware y software
	Incidentes en contención y erradicación	Desarrollo de tecnología para detección, contención y erradicación
	Incidentes contenidos y erradicados	Mecanismos para cálculo del nivel de riesgo organizacional
	Nivel de riesgo organizacional	Entrenamiento del equipo de respuesta a incidentes.
	Número de ciberactivos asegurados	Lecciones aprendidas

El modelo requiere de la estimación de variables continuas para acercar la problemática a la realidad. Se utilizó el método Delphi para la identificación de tiempos mínimos y máximos y se efectuaron los análisis estadísticos pertinentes, validando que los valores aleatorios calculados se ajustaran a la distribución PERT. Dicha distribución es frecuentemente utilizada para modelar la opinion de expertos y ha sido adaptada para que ellos provean estimados de

valores mínimos, más probables y máximos de las variables (Vose, 2008) y facilitar así los análisis.

4.3 Diagrama causal

El medio utilizado en esta investigación para realizar el diagrama causal y el de flujos y niveles fue mediante el software *Vensim DSS for Macintosh* versión 6.3 de doble precisión, el cual permite abarcar todas los del proceso de modelado en DS. Dicho software es utilizado para la modelación bajo este paradigma.

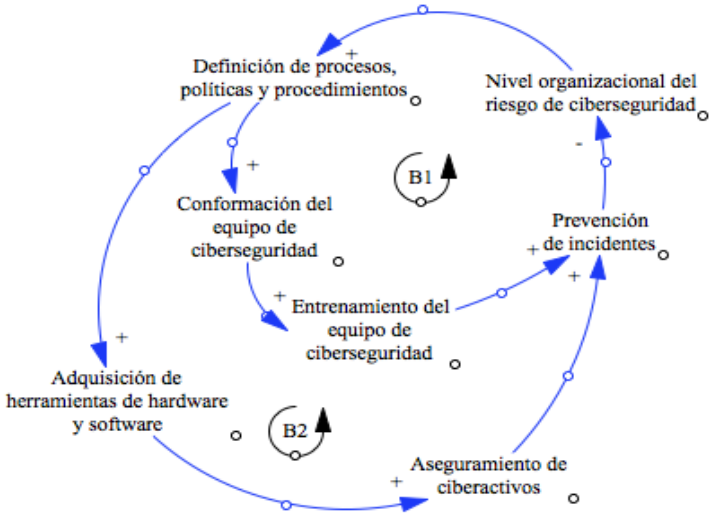
A continuación, se describe el diagrama causal propuesto, el cual agrupa las interdependencias de las diferentes variables que pueden traducirse en el modelo de flujos y niveles. En ese sentido, se identificaron 4 subsistemas denominados: Preparación, Detección y análisis de incidentes, Actividades durante el incidente y Actividades Post-incidente.

La Figura 5, agrupa el primer subsistema, llamado "Preparación" y muestra las relaciones propuestas para tener una aproximación al problema y algunos elementos relevantes que anteceden el manejo de incidentes. Tal y como se observa en el ciclo B1, la preparación parte de la percepción del riesgo de ciberseguridad que pueda tener una organización (García Zaballos y González Herranz, 2013, p 14). El nivel de riesgo que una organización pueda determinar (Young, 2016, p 21), así como su consciencia situacional, darán pie a la definición de políticas, procesos y procedimientos (Kossakowski, Allen, Alberts, Cohen, y Ford, 1999) para poder establecer controles necesarios que propendan por la reducción de los impactos si se materializa el riesgo o la disminución de la probabilidad de ocurrencia del mismo (Vacca, 2014, p 287). Tales elementos de control derivarán en acciones concretas como, por ejemplo, la conformación de un equipo de respuesta a incidentes (Smith, 1994) que permita hacerle frente a los eventos que se materialicen (Jindal, 2014).

El equipo, dada la constante actualización de técnicas y vectores de ataque, debe recibir de manera periódica, entrenamiento sobre las tendencias actuales y los diferentes métodos de

ataque y contención (Luiijf, 2014, p 48). De igual modo, como se observa en el ciclo B2, la presencia de tecnología actualizada, en este particular entendida como hardware y software, ofrece mayor cubrimiento a los ciberactivos críticos, desde la preparación a través de líneas base de seguridad, endurecimiento (*hardening*) entendido como la práctica de asegurar los sistemas para reducir nivel de exposición (Vacca, 2014), entre otros, hasta el monitoreo y recuperación de los mismos (Aguiar, 2017, p 8). Estos elementos, pueden contribuir al funcionamiento adecuado del manejo de incidentes desde la preparación previa que debe existir. Ahora bien, entre mayor sea el nivel de preparación al manejo de incidentes, el índice de riesgo organizacional debe tender a disminuir, no significando con ello, que los demás elementos del sistema deban tener la misma línea. En cualquier caso, se debe, de manera permanente, propender por el fortalecimiento de los mismos.

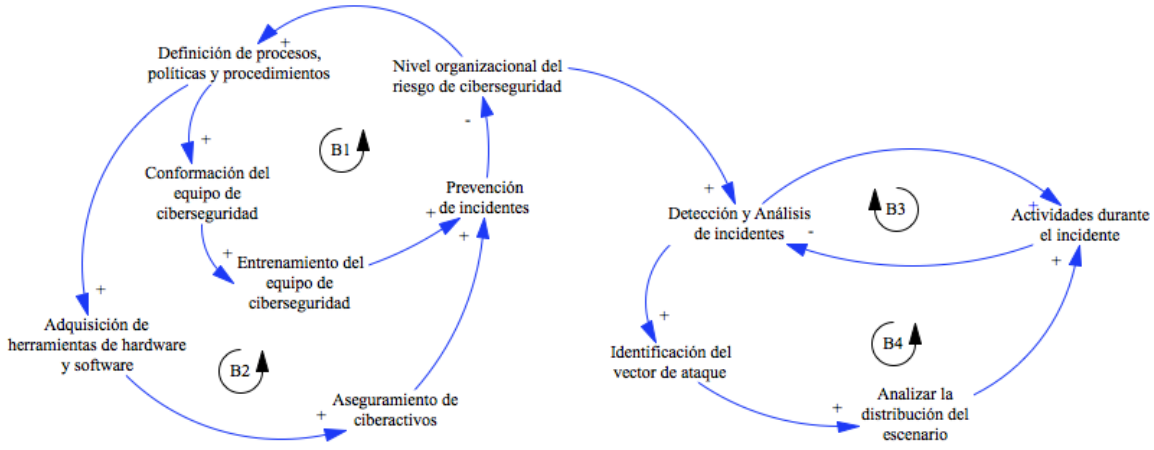
Figura 5. Subsistema Preparación.



Por otra parte, la Figura 6, en los ciclos B3 y B4, relaciona al segundo subsistema de "Detección y análisis de incidentes", es el primer paso en el manejo de incidentes propiamente dicho y supone la necesidad de identificar los diferentes vectores de ataque dado que cualquier incidente de ciberseguridad debe ser detectado en el menor tiempo posible para minimizar los impactos que se puedan derivar de él (Akhgar y Arabnia, 2014, p. 401). Un evento de

ciberseguridad puede entenderse como un cambio en las operaciones normales de la red o las tecnologías de información y comunicación que puede tener impacto en las operaciones organizacionales, incluyendo procesos misionales, capacidades o incluso en la reputación (NIST, 2014). Un incidente de ciberseguridad se materializa cuando se afecta de manera directa o indirecta a lo que se conoce como la triada CIA (Ahmad, Hadgkiss, y Ruighaver, 2012), por lo que su detección temprana resulta factor crítico de éxito en la minimización de los impactos (Adams, N. y Heard, 2014, p 36). De igual modo, entre más incidentes ocurran, mayor debe ser el nivel de detección de los vectores de ataque. Cualquier ataque se desarrolla en un escenario puntual que puede o no tener cobertura o alcance en toda una red, por cual, se debe determinar la distribución real del escenario donde acontece para limitar y/o definir las acciones a emprender para dar respuesta al mismo. En otras palabras, se debe realizar un análisis puntual de cada uno de los ataques y las correlaciones con otros incidentes o eventos para determinar los pasos siguientes para contenerlos y erradicarlos.

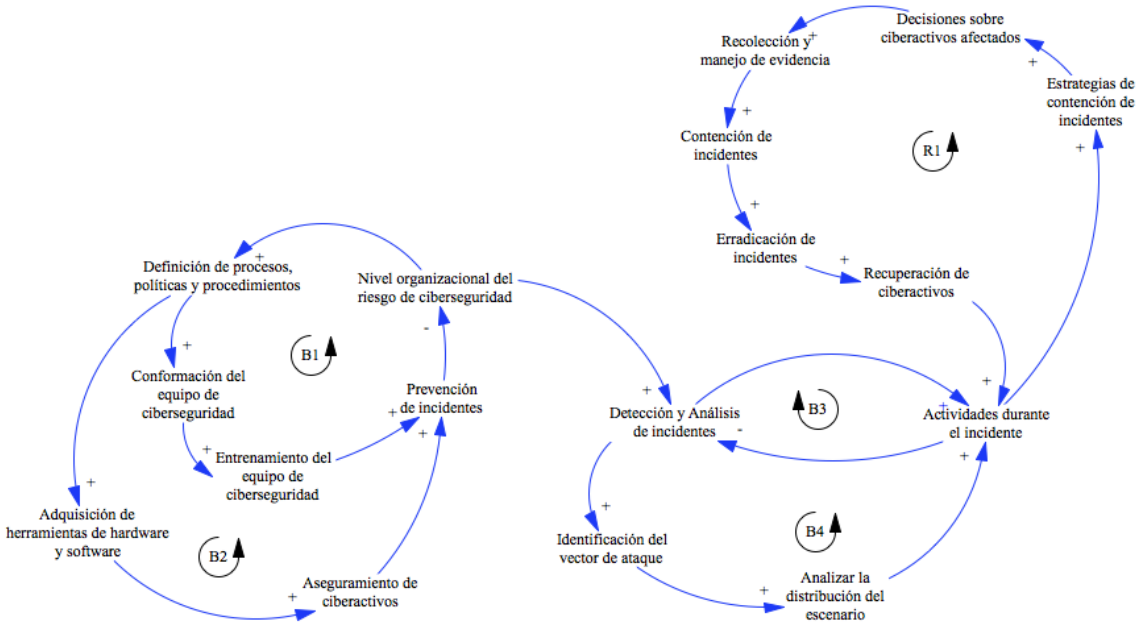
Figura 6. Agrupación de susbsistemas: Preparación, Detección y análisis.



En el tercer subsistema, en la Figura 7, “Actividades durante el incidente”, se desarrollan todas las actividades puntuales para reducir el tiempo de vida de los incidentes y retornar la red a condiciones óptimas de operación y minimizar los impactos derivados de las técnicas de ataques (Chabinsky, 2017) como se observa en el ciclo de refuerzo R1. Para ello es necesario, poder tener claridad y definición de las estrategias de contención y erradicación actuales y

poder construir, de manera ágil, aquellas nuevas en función de los diferentes tipos de ataques. Cada estrategia debe considerar el tipo de decisiones que debe tomarse sobre los ciberactivos e incluso sobre las personas de forma tal que se preserve, durante todo el tiempo, las evidencias necesarias del ataque para su posterior análisis y, si es del caso, judicialización. Así las cosas, todos los incidentes, una vez identificados y analizados, deben ser contenidos y erradicados en el menor tiempo posible, para minimizar los efectos que se derivan de ellos. La contención puede considerarse como un elemento que no soluciona de raíz el incidente, por ejemplo, asilar los ciberactivos afectados de la red, mientras que la erradicación supone la eliminación del mismo de la red (Chabinsky, 2017); por tal motivo son considerados como elementos individuales dentro del sistema. Finalmente, una vez erradicado el incidente, es necesario restablecer el ciberactivo al estado normal de operación, con los correctivos necesarios para que, por lo menos, el mismo incidente no se materialice de nuevo (Chabinsky, 2017).

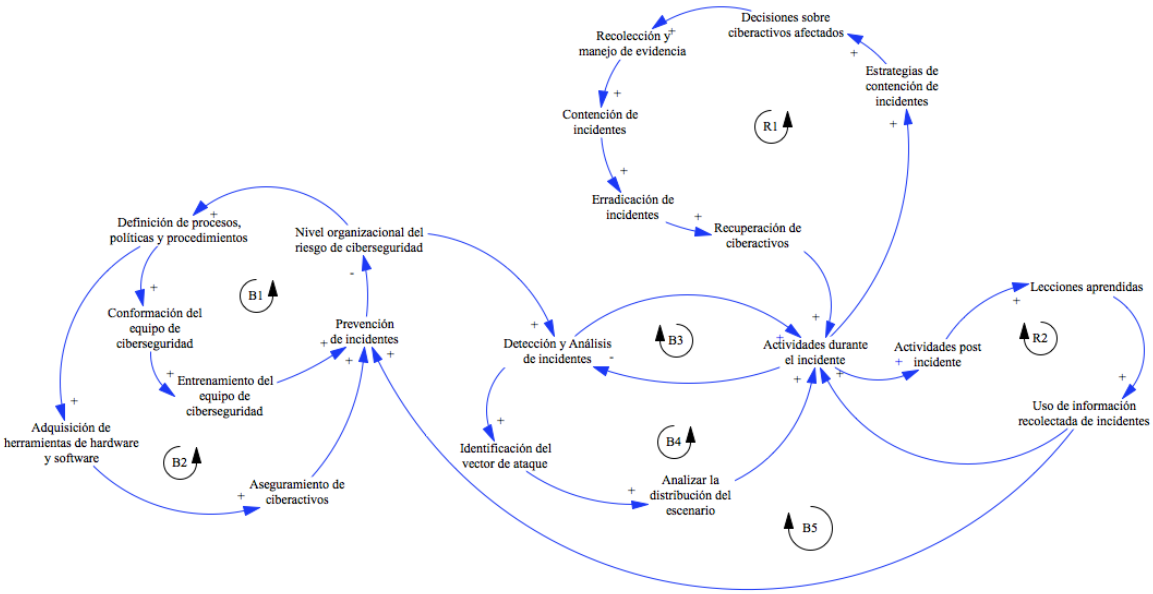
Figura 7. Agrupación de susbsistemas: Preparación, Detección y análisis y Actividades durante el incidente.



El último subsistema, “Actividades post-incidente” de la Figura 8, que se puede observar en el ciclo R2, debe permitir recopilar las lecciones aprendidas en los subsistemas precedentes, de forma tal que pueda generar conocimiento sobre las actividades ejecutadas de manera

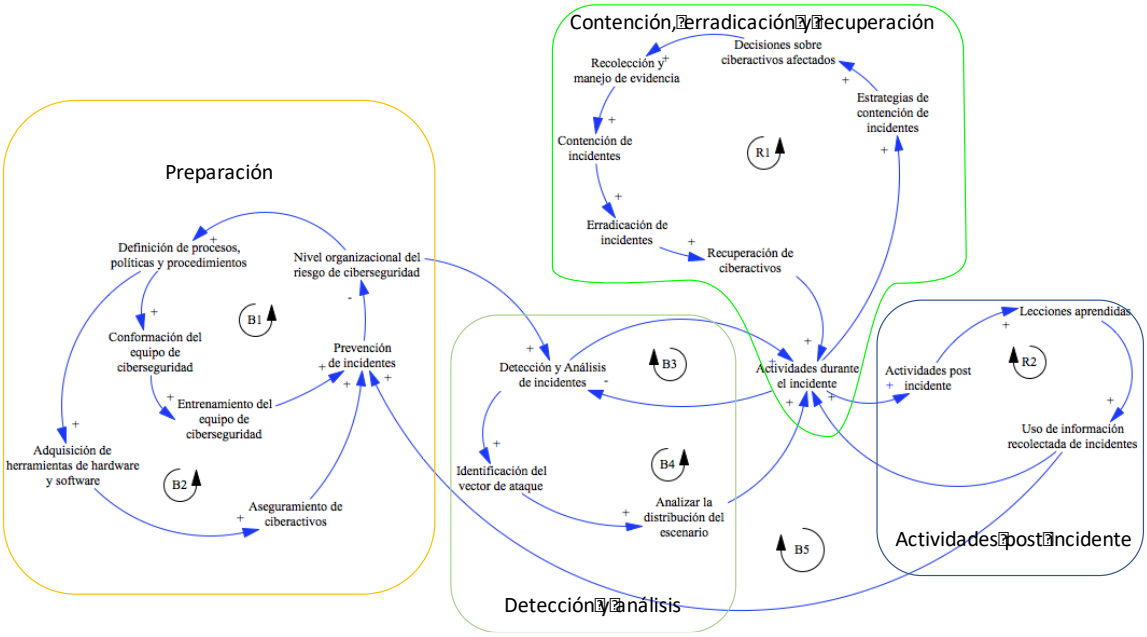
satisfactoria y aquellas realizadas inadecuadamente, otorgando elementos necesarios para enriquecer los demás componentes del sistema visto de manera holística (Cichonski, 2012).

Figura 8. Agrupación de susbsistemas: Preparación, Detección y análisis, Actividades durante el incidente y Actividades post incidente.



El diagrama causal propuesto, desarrolla los cuatro principales componentes del ciclo de vida del manejo de incidentes propuesto por la NIST, los cuales pueden ser analizados como subsistemas complementarios, que otorgan una aproximación al entendimiento del problema. La Figura 9 los agrupa en los siguientes cuadros:

Figura 9. Diagrama causal agrupado respecto al ciclo de vida de manejo de incidentes.



4.4 Diagrama de flujos y niveles

Tal y como lo afirma Sterman (2003, p. 192), la DS se basa en los Diagramas de flujos y niveles (o diagrama de Forrester) para el proceso de modelación y simulación, definidos así:

Niveles (*stock*): representados por rectángulos y sugieren un contenedor.

Flujos (*flows*): Expresan de manera explícita la variación por unidad de tiempo de los niveles. Son representados por un tubo (flecha) que apunta a un nivel y pueden ser catalogados como entrantes o salientes.

Válvulas de control de flujos.

Nubes: representan las fuentes o sumideros de los flujos.

Los diagramas de flujos y niveles son la representación matemática del diagrama causal (el cual representa visualmente las hipótesis dinámicas de un problema) y permite la simulación de los elementos identificados para analizar la complejidad del problema. Los niveles acumulan o integran los flujos que reciben, de esta forma el flujo neto del nivel es la tasa de cambio del mismo y está representada, según Sterman (2003, p. 194), por la ecuación integral (2):

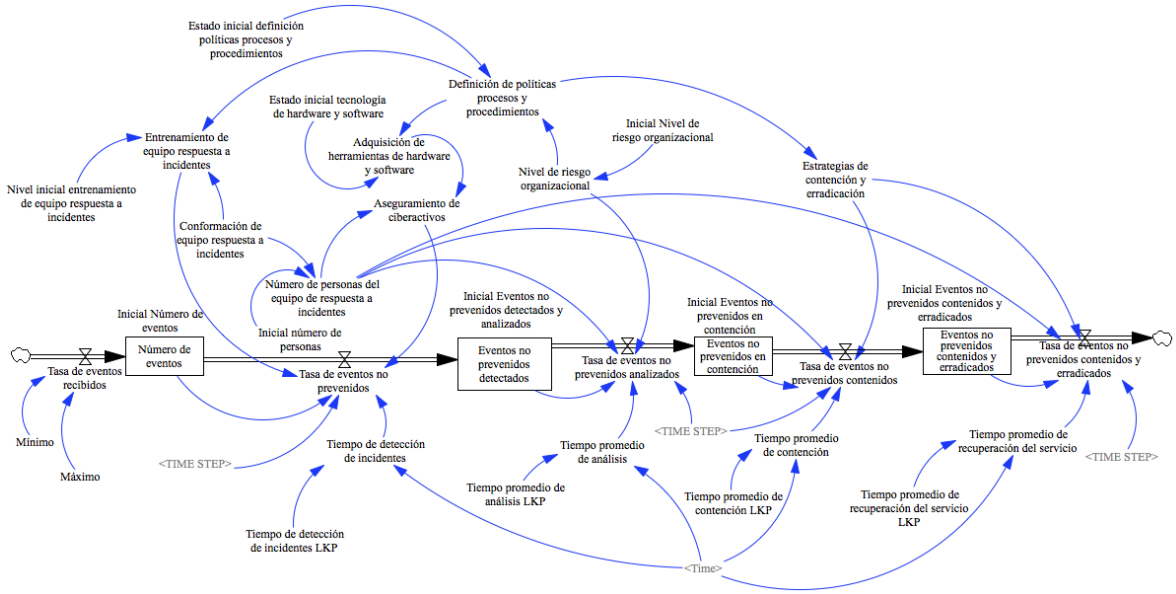
$$Nivel(t) = \int_{t0}^{t} [FlujoEntrante(s) - FlujoSaliente(s)]ds + Nivel(t0) \quad (2)$$

donde, FlujoEntrante representa el valor del flujo entrante en cualquier momento *s* entre el tiempo inicial t_0 y el tiempo actual *t*. Así las cosas, la tasa neta de cambio de cualquier nivel es el flujo entrante menos el flujo saliente, definida por la ecuación diferencial (3), entendiendo que los flujos son funciones de los niveles y de otras variables de estados y parámetros. En otras palabras, Sterman (2003, p. 197) asocia los Niveles con integrales y los Flujos con tasas o derivadas, esto es, el primero son cantidades de material u otras acumulaciones y el segundo son tasas a las cuales el sistema cambia de estado.

$$\frac{d(Nivel)}{dt} = FlujoEntrante(t) - FlujoSaliente(t) \quad (3)$$

A continuación, se ilustra en la Figura 10 el diagrama de flujos y niveles definido para el análisis del fenómeno a partir de las hipótesis dinámicas establecidas.

Figura 10 - Diagrama de flujos y niveles



4.5 Datos para el análisis

La información estadística de los incidentes de ciberseguridad es, en general, información reservada, toda vez que ella puede revelar el nivel de protección de las TI y propiciar un ataque viral al sistema como tal, según lo expone la Oficina de Estadística Nacional del Gobierno Británico (Statistics, 2017).

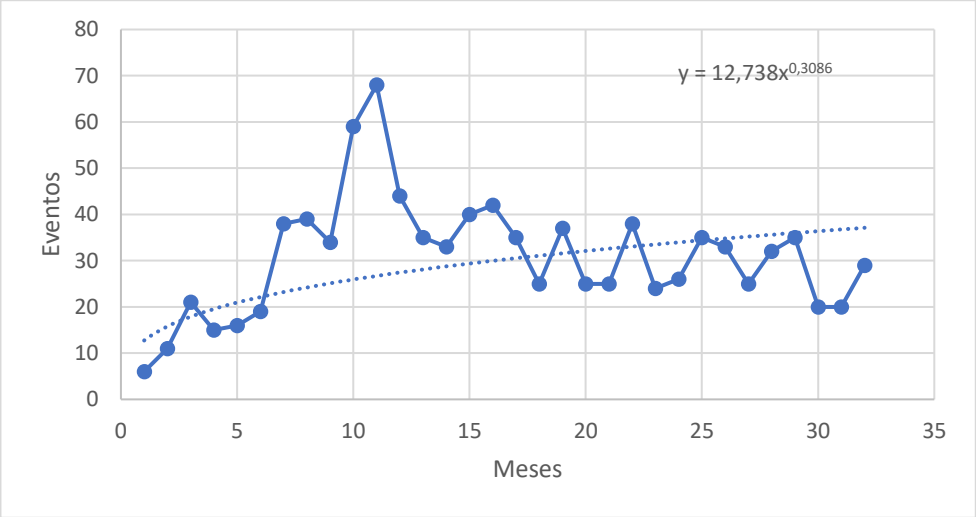
Los datos obtenidos para la modelación fueron registrados desde mayo de 2015 hasta abril de 2018, los cuales daban cuenta de los eventos ocurridos, en días específicos, en la organización objeto de estudio. Ahora bien, para la modelación de los datos se realizaron dos análisis que variaron por la unidad de medición o agrupación de los datos, los cuales fueron catalogados en meses y en días para analizar su comportamiento bajo estas dos unidades de tiempo en el modelo propuesto. A continuación, se presentan los resultados obtenidos para ambas unidades

de medida. Los datos analizados corresponden a una empresa del sector colombiano que se encuentra catalogada como una compañía con infraestructura crítica para el país.

4.5.1 Análisis de datos agrupados por meses

Para comprender el comportamiento de los eventos registrados en el tiempo especificado, de la organización objeto de análisis, y poder proyectarlos a los 20 años, se procedió a graficarlos y se obtuvo la Figura 11. Una vez surtido este proceso se pudo determinar que los datos poseen una la línea de tendencia potencial y una función de distribución $y=12{,}738x^{0{,}3086}$.

Figura 11. Distribución del número de eventos registrados



Ahora bien, para poder trabajar con la serie de tiempo necesario en el modelo, se procedió a ajustar la tendencia y la estacionalidad de ésta, de forma tal que pudiera facilitar la predicción de 240 meses más de los eventos, basados en la información histórica disponible. Se pretende entonces suavizar los picos de la gráfica, a través del suavizado de la tendencia a través de medias móviles y predecir los meses siguientes por medio de modelos de tipo paramétrico el cual, para este caso, se utilizó el modelo potencial. Se realizó el ajuste de tendencia para obtener una nueva serie de datos exentos de ella.

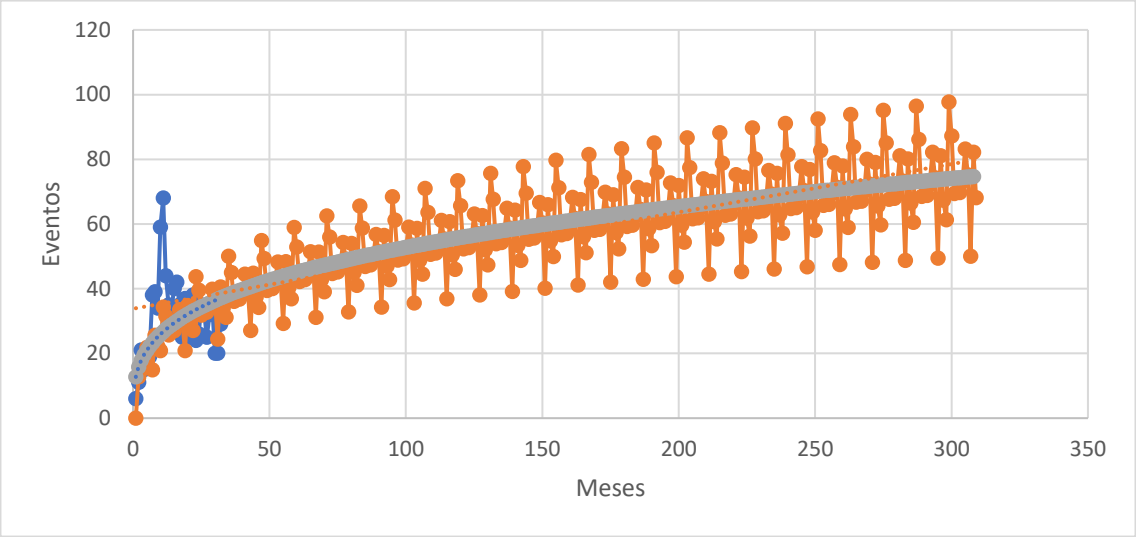
Para la proyección de los eventos en los meses sujetos de análisis, se realizaron los siguientes pasos:

1. Gráfico de la serie de tiempo con los datos obtenidos.
2. Definición de la línea de tendencia.
3. Se creó un índice de tiempo y se calculó la tendencia con base en la ecuación dada por el modelo.
4. Se determinó que la estructura de predicción responde a un modelo multiplicativo a través del cálculo de la serie de diferencias y la serie de cocientes, realizando la operación pertinente del dato consecutivo con el actual, para calcular el coeficiente de variación, el cual es el resultado del cociente de la media y la desviación estándar de la diferencia y el cociente.
5. Se eliminó la tendencia a través de la división del dato original respecto al modelo de tendencia ajustado para dar más claridad sobre el componente estacional.
6. Se calculó el índice de estacionalidad para cada uno de los meses, a través del cálculo de las medias móviles de orden 12 dada que dicho número es el periodo de estacionalidad definido, a través de la función promedio de los doce valores consecutivos.
7. Se centró la curva en orden 2, a través de la media móvil de orden 12.
8. Se calculó el promedio de cada uno de los meses y se creó un índice de la serie estacionalizada y la serie de centradas, el cual se calculó como el cociente de la serie sin tendencia y el valor de la serie centrada multiplicada por 100.
9. Sobre los índices calculados en el punto anterior, se promediaron cada uno de los meses de cada año de la serie, de forma tal que cada mes tenga su respectivo índice.
10. Dado que los índices están calculados a partir de las medias móviles centradas, se procedió a normalizarlos, corrigiendo cada uno de los valores, dividido la suma de todos los índices y multiplicando por 1200 dados los doce meses y la multiplicación previa por 100 (referente básico para el índice), obteniendo así los índices de estacionalidad.
11. Se realizó la predicción, multiplicado la tendencia de cada punto y el índice de estacionalidad que corresponde en función del mes en el que encuadra el dato disponible.
12. Se efectuó el cálculo para los 240 meses finales.

13. Para efectos del modelo final y dado que el número de incidentes es una variable discreta, se aproximó al entero más próximo.

El resultado final de la predicción puede observarse en la Figura 12.

Figura 12. Predicción del número de eventos a 240 mes más

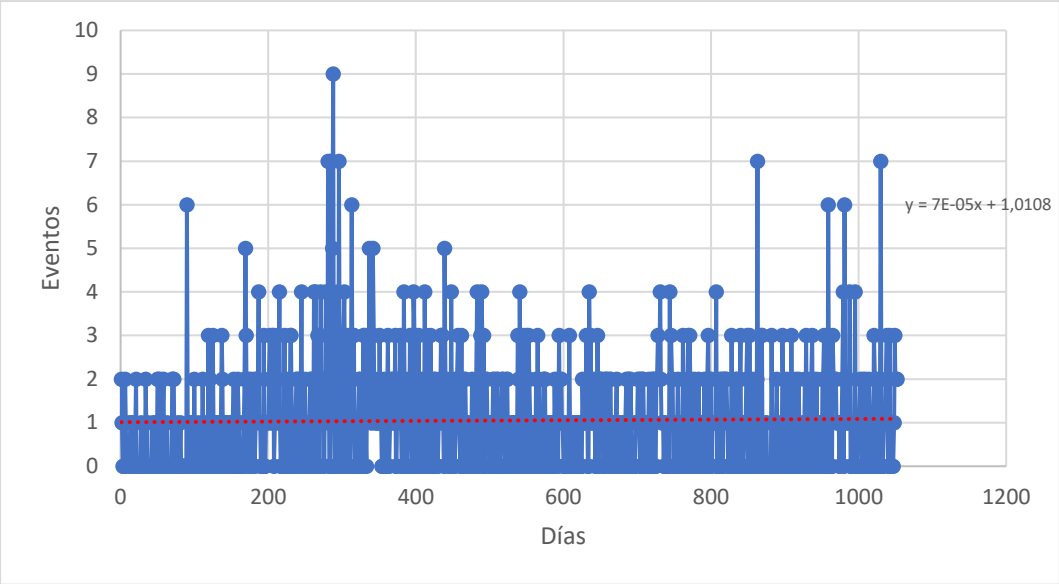


Con los datos obtenidos de la proyección de eventos agrupados por meses, el modelo de flujos y niveles propuesto arrojaba un error toda vez que los valores obtenidos bajo esta unidad de medida eran muy cercanos a cero, por lo que no fue posible realizar el análisis basado en meses.

4.5.2 Análisis de datos agrupados por días

Para facilitar el entendimiento del comportamiento de los datos en esta unidad de medida, se decidió modelarlos con la ayuda de la herramienta Risk Simulator (Real Options Valuation, 2017). En ese sentido, se graficaron los datos, obteniendo la gráfica que se observa en la Figura 13, donde la pendiente de la línea de tendencia es casi cero, asumiendo que existen días donde no ocurren eventos, los cuales fueron adicionados a los datos originales:

Figura 13. Agrupación de los datos (eventos) obtenidos



Para poder proyectar los eventos a los 20 años definidos, fue necesario determinar la distribución que los datos seguían. En ese sentido y con la ayuda de la herramienta mencionada, se obtuvo un ajuste de distribución binomial negativa para la variable discreta "Eventos", con éxitos requeridos de 2 y probabilidad de 0,7. Los resultados del ajuste de distribución, generados por la herramienta, se consignan en las tablas 6 y 7.

Tabla 6. Resultado ajuste de distribución

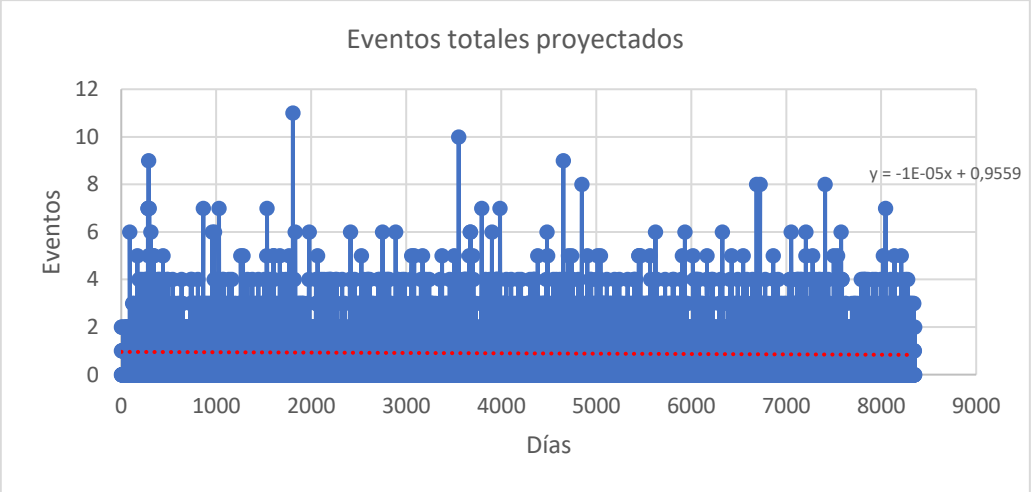
Concepto	**Resultado**
Supuesto ajustado	1,05
Distribución ajustada	**Binomial Negativa**
Éxitos requeridos	2,00
Probabilidad	0,70
Chi-Cuadrado	66,36
MAPE % para Test estadístico	0,07%

Tabla 7. Resultado ajuste de distribución variables estadísticas

Variable	Actual	Teórico
Media	1,05	0,87
Desviación Estándar	1,23	1,12
Asimetría	1,73	1,67
Kurtosis en exceso	4,85	3,80

Con estos datos, se generaron números aleatorios dentro de dicha distribución y se procedió a generar la gráfica para observar el comportamiento, la cual se consigna en la Figura 14.

Figura 14. Datos generados para 20 años (unidades en días)



El modelo utilizó esta unidad de medida para realizar los cálculos correspondientes y los análisis respectivos.

4.6 Tiempos para detectar, analizar, contener un incidente y restablecer el servicio

Como referente internacional, los reportes emitidos por Holdings (2017) y Holdings (2016) evidencian, en general, un decrecimiento en los tiempos de identificación y contención de incidentes de seguridad, pasando por ejemplo de 86 días desde la intrusión hasta la detección en el año 2014 a 49 días en el año 2016 como lo muestra la Tabla 8, por lo que se puede

concluir una disminución considerable en los tiempos, lo cual denota una preocupación constante de las organizaciones por ser más eficientes en este aspecto.

Tabla 8. Días desde la intrusión hasta Detección y contención.

Año	Intrusión hasta Detección (días)	Intrusión hasta Contención (días)
2014	86	111
2015	80,5	63
2016	49	63

Fuente: Adaptado de Holdings, 2016, 2017

Ahora bien, ante la ausencia de tiempos de respuesta medibles a nivel organizacional y de interés en el modelo propuesto, se procedió, a través del método Delphi con expertos en ciberseguridad, a la identificación de los tiempos mínimos y máximos de cada una de las variables identificadas en el modelo. Para la modelación se utilizó la distribución PERT como referente para la generación de números aleatorios. Según Vose (2008), dicha distribución es una versión de la distribución Beta y requiere los mismos parámetros: mínimo, más probable y máximo y puede ser utilizada cuando se cuenta con la opinión de expertos, cuya ecuación (4) es la siguiente:

$$PERT(a,b,c) = Beta(\alpha 1, \alpha 2) * (c-a) + a \quad (4)$$

donde,

$$\alpha 1 = \frac{(\mu - a) * (2b - a - c)}{(b - \mu) * (c - a)}$$

$$\alpha 2 = \frac{\alpha 1 * (c - \mu)}{\mu - a}$$

$$\mu = \frac{a + 4b + c}{6}$$

Los valores definidos por los expertos, a través de un promedio simple, se consignan en la Tabla 9.

Tabla 9. Agrupación de tiempos definidos por expertos

	Mín (días)	Max (días)	Moda	Valor esperado
Tiempo de detección	0,01041667	0,12268519	0,04783951	0,054076646
Tiempo de análisis	0,00810185	0,11111111	0,04243827	0,048161008
Tiempo de contención	0,07291667	1,34722222	0,49768519	0,568479938
Tiempo restablecimiento del servicio	0,16666667	4,33333333	1,55555556	1,787037037

Se calcularon la Moda con la ecuación (5) y el Valor Esperado, ecuación (6), de la siguiente manera:

$$Moda = \frac{1}{3}(Máx - Mín) + Mín \qquad (5)$$

y

$$Valor\ Esperado = \frac{Mín + 4Moda + Máx}{6} \qquad (6)$$

Con dichos parámetros se generaron números aleatorios con la distribución PERT para los 20 años, medidos en días de la simulación y para cada una de las variables. Lo anterior se desarrolló con el fin de generar aleatoriedad en los tiempos sujetos de análisis y reflejar así un modelo más cercano a la realidad, toda vez que no es posible considerar que existe un solo tiempo promedio de atención de los incidentes dado que algunos pueden ser más complejos que otros desde su detección hasta su erradicación.

4.7 Prueba de Kolmogorov – Smirnov

Con el fin de validar el ajuste en los datos generados para los tiempos, se procedió a aplicar la prueba de Kolmogorov – Smirnov (K-S) para determinar si los datos, en efecto, se ajustaban a la distribución utilizada.

El procedimiento K-S es un test no paramétrico que prueba que una variable *X* continua, se ajusta a una distribución dada *f(x)* (Coss, 2005). En este sentido, se pretende determinar si los números aleatorios generados mediante una función *f(x)* se ajustan a la distribución definida $f_0(x)$, que para el caso de estudio se utilizó PERT. En otras palabras, en la hipótesis nula se desea probar si los números aleatorios calculados *x*, se ajustan a la distribución PERT. Las pruebas de hipótesis se definen como sigue:

$H_0: f(x) = f_0(x), \forall x$

$H_1: f(x) \neq f_0(x)$, *para algunas x*

La prueba de bondad de ajuste, tal y como lo menciona Vose (2008) proveen la probabilidad de que los datos generados de manera aleatoria a partir de una distribución ajustada, produzcan un valor estadístico tan bajo como para los valores observados. Para la comparación es necesario definir los valores críticos para la prueba de hipótesis y son determinados por el nivel de confianza α. Vose (2008), afirma en algunos casos es necesario modificar el test estadístico para lo cual define las fórmulas consignadas en la Tabla 10 que se define a continuación:

Tabla 10. Fórmulas para ajuste del test Kolmogorov – Smirnov K-S

Distribución	**Test estadístico modificado**
Normal	$\left(\sqrt{n} - 0.01 + \frac{0.85}{\sqrt{n}}\right) * Dn$
Weibull y valores extremos	$\sqrt{n}Dn$
Todas las demás	$(\sqrt{n} + 0.12 + \frac{0.11}{\sqrt{n}})Dn$

Fuente: Vose (2008)

donde *Dn* es el estadístico no modificado de K-S y *n* el tamaño de la muestra.

Coss, (2005) define los valores del estadístico K-S como se describe en la Tabla 11:

Tabla 11. Estadístico K-S para diferentes valores del nivel de significancia y tamaño de la muestra

n	α= 10%	α= 5%	α= 1%
30	0.220	0.242	0.290
35	0.210	0.230	0.270
40		0.210	0.252
50		0.188	0.226
60		0.172	0.207
70		0.170	0.192
80		0.150	0.180
90		0.141	
100		0.134	
Fórmula aproximada para n > 100	$\frac{1.22}{\sqrt{n}}$	$\frac{1.36}{\sqrt{n}}$	$\frac{1.63}{\sqrt{n}}$

Fuente: Coss, (2005)

Para determinar el valor del estadístico K-S ajustado que permita determinar la adecuación de los valores aleatorios generados, dentro de la distribución especificada, se siguió el procedimiento definido por Coss, (2005) a través de los siguientes pasos:

1. Se ordenaron los datos aleatorios de cada uno de los tiempos definidos para el modelo.
2. Se calculó la distribución acumulada de los números generados bajo la ecuación (7).

$$Fn(x) = \frac{i}{n} \qquad (7)$$

   donde *i* es el número que ocupa el valor *x* del vector ordenado obtenido en el punto 1 y n el tamaño de la muestra.

3. Se calculó el estadístico Kolmogorov – Smirnov bajo la siguiente ecuación (8):

$$D_n = \text{Max} \left| f_n(X_i) - X_i \right|, \ \forall x \qquad (8)$$

4. Se comparó el estadístico obtenido con los valores críticos modificados (utilizando la fórmula de la distribución diferente a Normal y Weibull).

Los resultados obtenidos de la prueba se consignan en la siguiente Tabla 12.

Tabla 12. Resultados prueba K – S

Variable	K-S Calculado α =0.5%	K-S Ajustado	Comparación
Tiempo de Detección Aleatorio	0.914170737	1.361803679	MENOR
Tiempo de Análisis Aleatorio	0.920330922	1.361803679	MENOR
Tiempo de contención Aleatorio	0.627722656	1.361803679	MENOR

Con los datos obtenidos es posible concluir que el estadístico K-S calculado para las variables de la Tabla 10 son menores al K-S crítico, por lo que se puede afirmar que los datos provienen de la distribución definida PERT, es decir, se acepta la hipótesis nula.

4.8 Validación

La modelación con DS requiere de procesos iterativos que comienzan desde la definición del modelo y pueden extenderse incluso hasta después de la implementación de las políticas derivadas del mismo (Giraldo, 2013). En ese sentido es indispensable validar el modelo para verificar la adecuación de éste, frente a cambios de algunas variables, permitiendo el análisis de las relaciones definidas y la realidad lógica y experimental. En ese sentido Giraldo (2013) afirma que la validación en DS incluye dos componentes, definidos como validación de la estructura del modelo y la validación del comportamiento de los resultados del modelo.

Para este ejercicio se propuso analizar: consistencia dimensional, condiciones extremas, pruebas de errores de integración y análisis de sensibilidad.

4.8.1 Consistencia Dimensional

La herramienta *Vensim DSS*, utilizada para el desarrollo del trabajo, verifica de manera automática las ecuaciones del modelo, analizando la consistencia en las unidades de medida definidas. Con dicha característica, se verificaron las unidades de las variables, encontrando coherencia en ellas.

4.8.2 Condiciones extremas

Se supuso cero eventos recibidos, dentro de la distribución binomial negativa asociada a la tasa de eventos recibidos, observando un comportamiento adecuado del sistema donde se evacúan los eventos no prevenidos iniciales y la curva tiende a cero, como se evidencia en la Figura 15 y la Figura 16. Es de anotar que los eventos son considerados una variable discreta, toda vez que existen o no existen y siempre son mayores o iguales a cero. De igual modo, se supuso la no existencia de personas en el equipo encontrándose que los eventos no prevenidos detectados corresponden a los datos de entrada de eventos, es decir, ambas distribuciones son muy similares, como se observa en la Figura 17.

Figura 15. Tasa de eventos recibidos en condiciones extremas

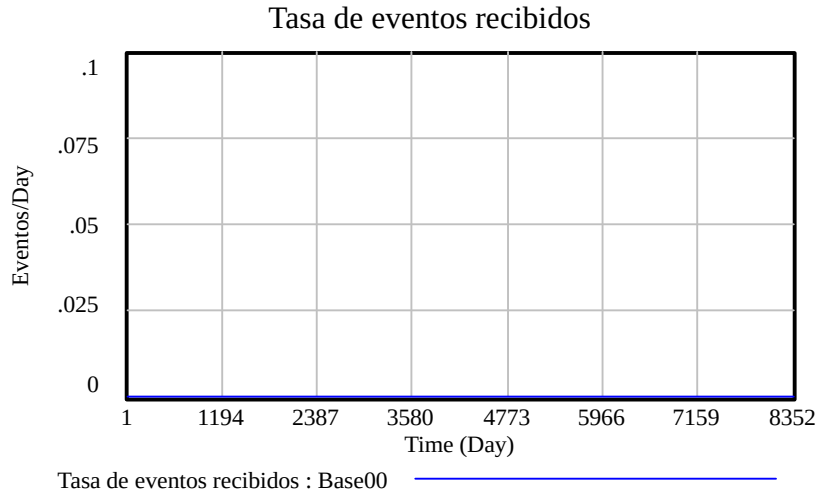


Figura 16. Número de eventos en condiciones extremas

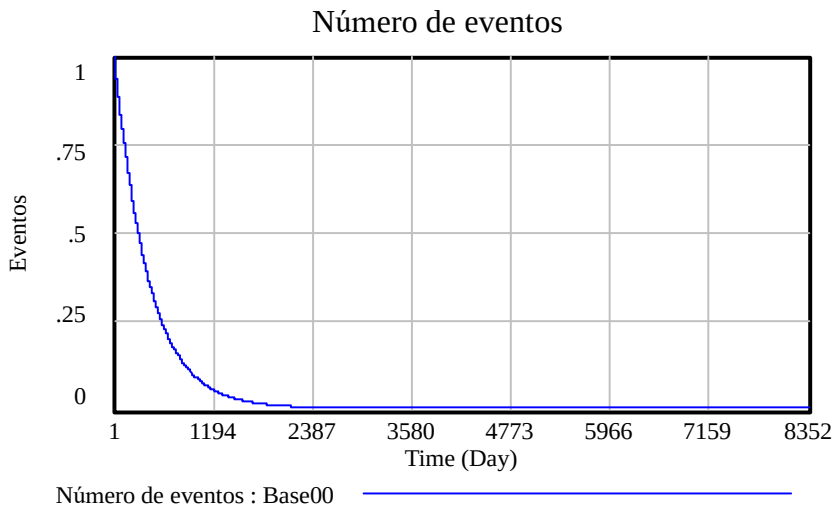
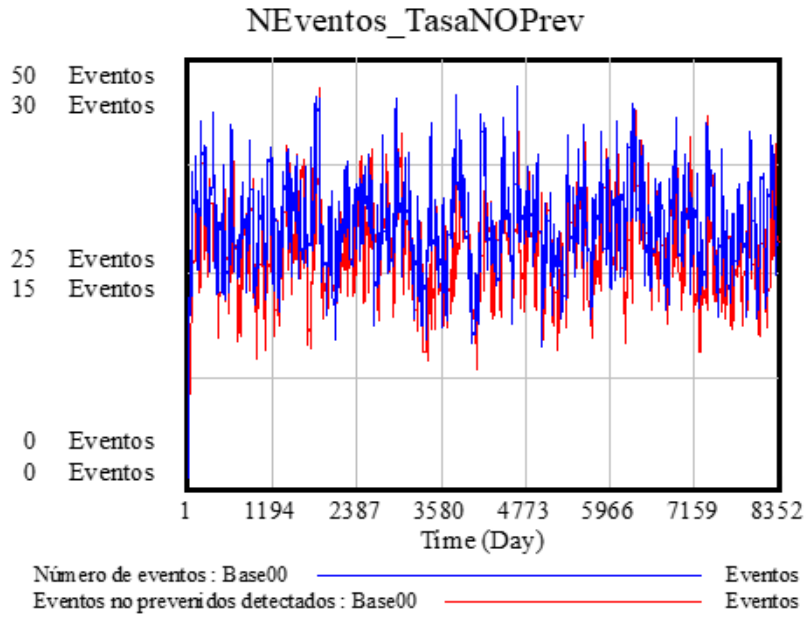


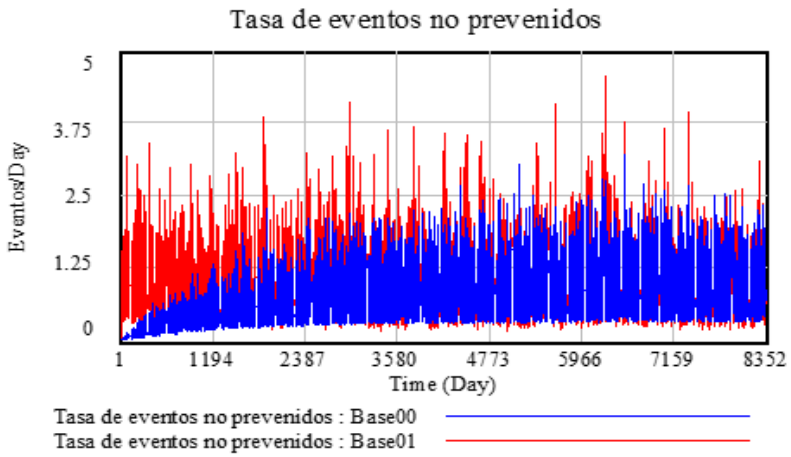
Figura 17. Número de eventos y Eventos no prevenidos en condiciones extremas con cero (0) personas



De igual manera, se consideraron tiempos extremos para la detección de incidentes, observándose una mayor cantidad de eventos no prevenidos o incidentes, como se muestra en la Figura 18, lo cual corresponde con la realidad esperada, toda vez que a mayor cantidad de

tiempo que se tarde en detectar un evento, mayor es el número de eventos que puede convertirse en incidentes.

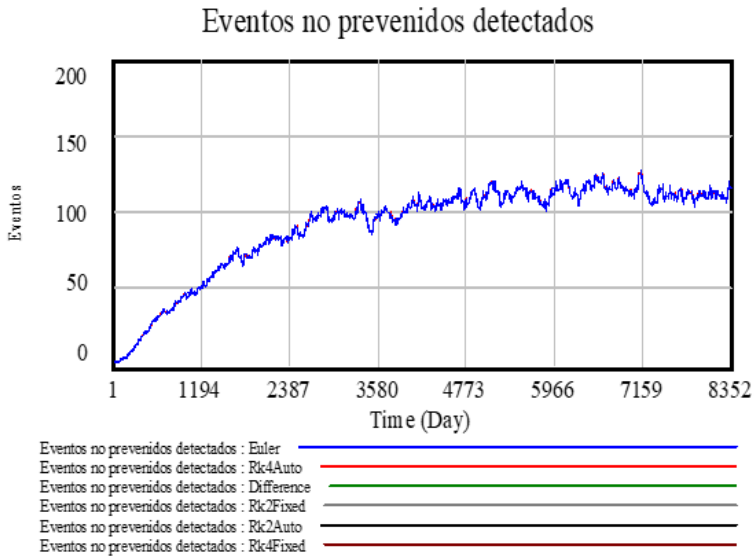
Figura 18. Tasa de eventos no prevenidos con afectación extrema del tiempo de detección



4.8.3 Pruebas de errores de integración

Se ejecutó el modelo, a través de la herramienta definida, con los tipos de integración Euler, RK4 Auto, Difference, RK2 Fixed, Rk2 Auto y RK4 Fixed y no se evidenció sensibilidad en los resultados del modelo como se muestra en la Figura 19.

Figura 19. Prueba de errores de integración



4.8.4 Análisis de sensibilidad

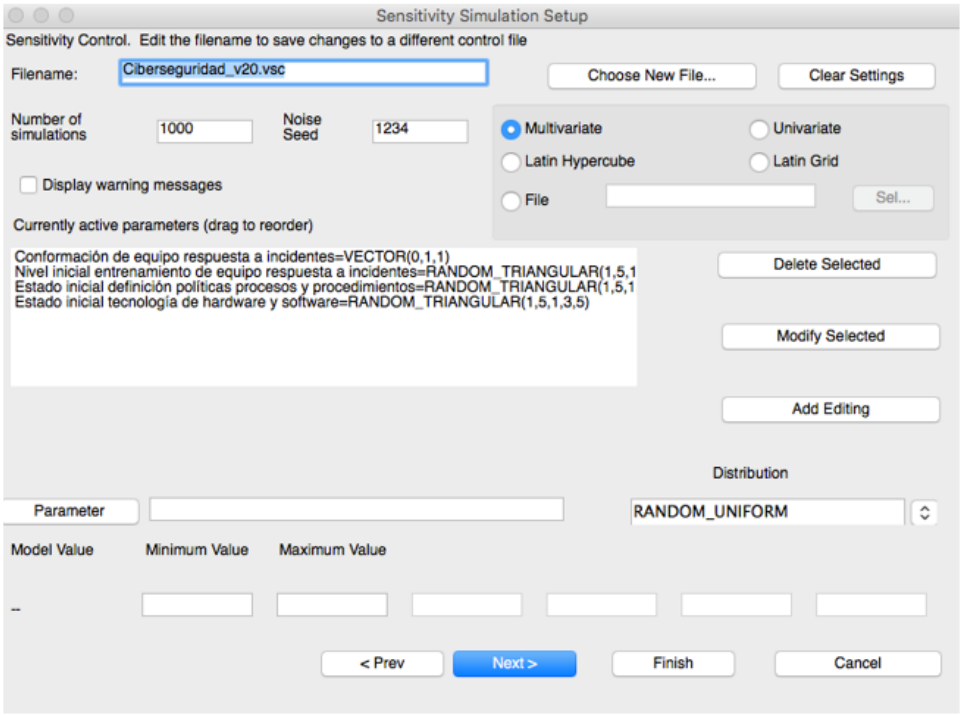
El análisis de sensibilidad permite identificar cambios significativos en las conclusiones cuando varían los supuestos de manera significativa. De igual modo muestra el comportamiento del modelo bajo la variación de los parámetros (Sterman, 2003). En ese sentido, este análisis permite probar la robustez de las conclusiones derivadas del modelo respecto a la incertidumbre definida en los parámetros estimados.

Según Sterman (2003), existen 3 tipos de análisis de sensibilidad:

1. Sensibilidad numérica: existe cuando un cambio en los supuestos, generan cambios numéricos en los resultados. Todos los modelos poseen sensibilidad numérica.
2. Sensibilidad de comportamiento: se presenta cuando un cambio en los supuestos, modifica el comportamiento generado por el modelo.
3. Sensibilidad de políticas: se origina cuando un cambio en los supuestos reversa el impacto o el objetivo deseado de las políticas.

Para efectos de este estudio, se realizó el análisis de sensibilidad de comportamiento, bajo distribuciones triangulares de los parámetros que se identifican en la Figura 20 y con 1000 iteraciones, para fortalecer las conclusiones con base en la incertidumbre de las variables y analizar los resultados generados.

Figura 20. Definición de parámetros para análisis de sensibilidad y sus distribuciones



Los resultados encontrados denotan que existe un 95% de probabilidad de que los datos se comporten según el rango encontrado en el modelo tal y como se evidencia en las Figura 21, 22 y 23.

Figura 21. Sensibilidad para la tasa de eventos no prevenidos

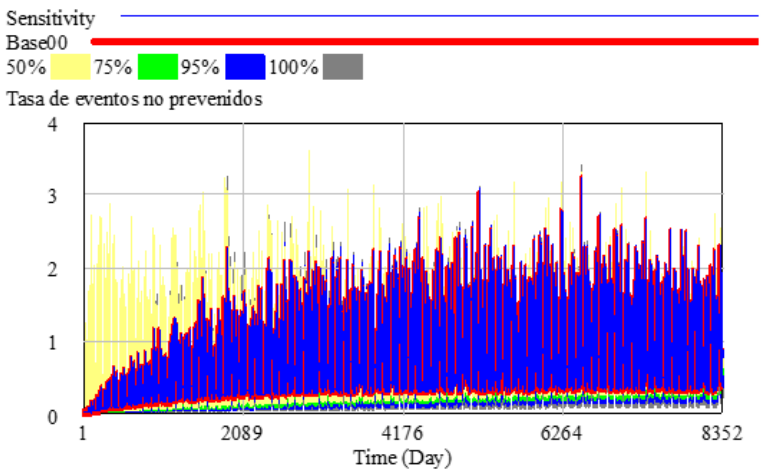


Figura 22. Sensibilidad para Eventos no prevenidos detectados

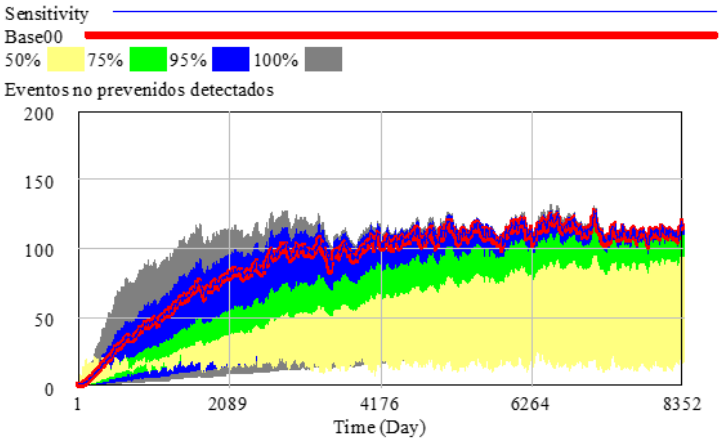
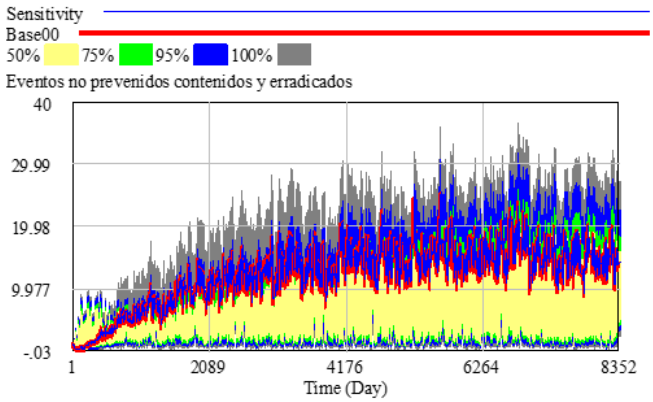


Figura 23. Sensibilidad para Eventos no prevenidos contenidos y erradicados

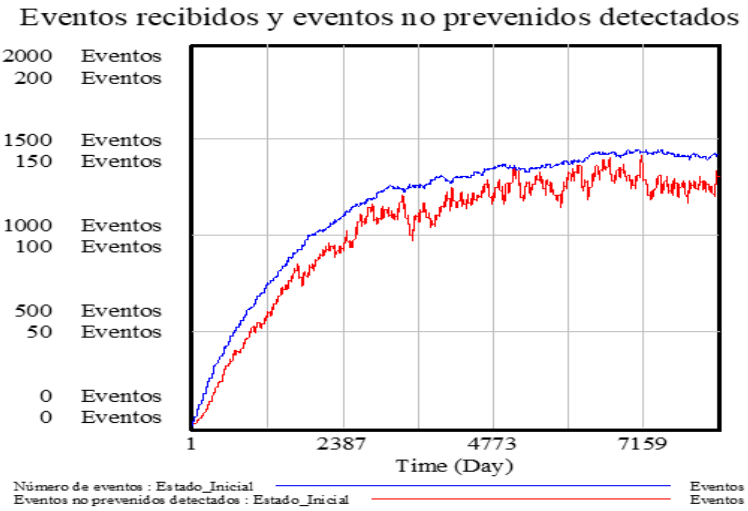


La dinámica capturada por el modelo evidencia un crecimiento del número de eventos que pueden recibir una compañía bajo las condiciones iniciales definidas. De los eventos, puede concluirse que tienen un comportamiento potencial, lo que aumenta el nivel de riesgo para las infraestructuras de las organizaciones, incluyendo aquellas críticas en tanto que un evento no prevenido, o incidente, puede comprometer la continuidad del negocio o los atributos CIA.

En ese mismo sentido, es necesario desarrollar mecanismos suficientes que permitan detectar, en el menor tiempo posible, los incidentes que pueden comprometer la ciberseguridad de las organizaciones. La Figura 24, refleja el comportamiento del sistema bajos las definiciones modeladas desde los eventos recibidos hasta aquellos eventos no prevenidos detectados o

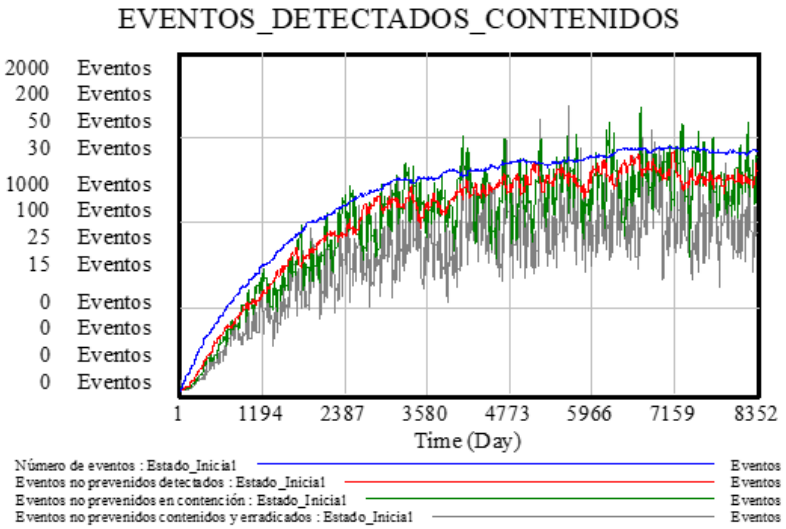
incidentes. Se evidencia que los eventos no prevenidos detectados son menores a los eventos recibidos en el lapso definido.

Figura 24. Eventos recibidos y eventos no prevenidos



Por otra parte, los eventos no prevenidos deben ser contenidos y erradicados en el menor tiempo posible para disminuir el impacto de los efectos naturales que los incidentes producen en términos de ciberseguridad. En ese sentido, los eventos en contención son relativamente similares a los eventos que son detectados. Ahora bien, los eventos no prevenidos suponen tiempos diferentes de atención y contención en términos de los RTO (Tiempo objetivo de recuperación por sus siglas en inglés) y RPO (Punto objetivo de recuperación por sus siglas en inglés) y de la criticidad de los activos inmersos, así como de la complejidad del ataque, por lo que no es posible tener la misma cantidad de contención y recuperación del servicio. Dicho comportamiento se puede analizar en la Figura 25.

Figura 25. Eventos, eventos no prevenidos, eventos no prevenidos en contención y eventos no prevenidos contenidos y erradicados



4.9 Escenarios

Una de las herramientas más comunes para la definición de políticas es la construcción de escenarios. El objetivo principal es definir el escenario optimista y el pesimista respecto a los parámetros consignados en el modelo que permitan comparar las salidas de cada uno de ellos para definir políticas que favorezcan la solución del problema. (Sterman, 2003).

En ese sentido, se simuló el modelo bajo las condiciones de escenario pesimista y escenario optimista que se pueden observar en la Tabla 13, donde se propuso revisar el comportamiento bajo condiciones desfavorables o inferiores a la situación inicial modelada y en la misma vía, se modificaron los valores de los parámetros para robustecer el sistema y analizarlo bajo la perspectiva del mejor escenario.

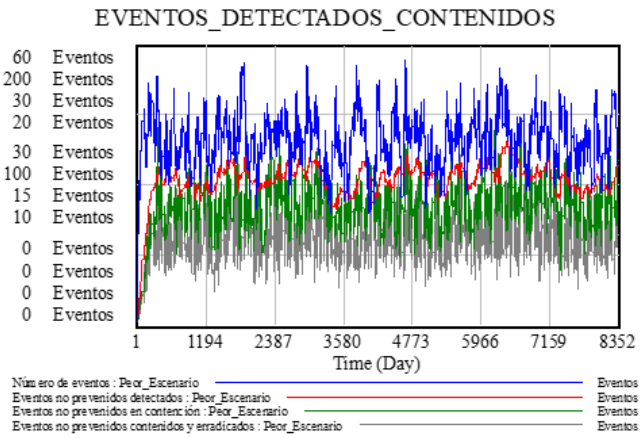
Tabla 13. Definición de escenarios para el análisis

Parámetro	Inicial	Pesimista	Optimista
Estado inicial tecnología de hardware y software	2	1	4
Conformación de equipo respuesta a incidentes	1	1	1
Estado inicial definición políticas procesos y procedimientos	2	1	4
Inicial número de personas	7	7	8
Nivel inicial entrenamiento de equipo respuesta a incidentes	3	1	4
Inicial Nivel de riesgo organizacional	0.47	0.57	0.37

4.9.1 Escenario Pesimista

En este escenario, la tecnología se supone con un nivel de obsolescencia mayor, una menor definición de controles internos en términos de ciberseguridad, entendidos como un menor nivel de políticas, procesos y procedimientos, un menor nivel de entrenamiento y un aumento del nivel de riesgo que puede ser determinado por la complejidad de los ataques lo que facilita la materialización de eventos no prevenidos o incidentes y por tanto la afectación de la tecnología en general así como las infraestructuras críticas. La Figura 26, evidencia el comportamiento del sistema con los parámetros definidos.

Figura 26. Comportamiento del sistema en el escenario pesimista

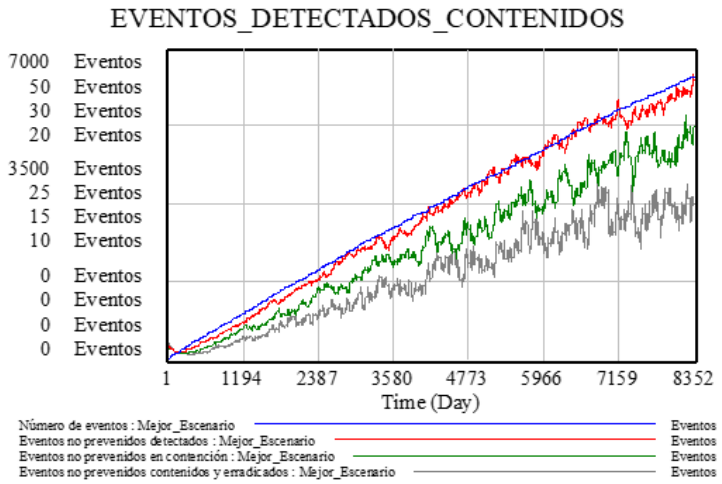


La gráfica evidencia un número mayor de eventos con una menor capacidad de detección y, por tanto, una cantidad inferior de los incidentes contenidos y erradicados, lo que aumenta notablemente el riesgo de pérdida de continuidad del negocio, así como afectación a los atributos CIA.

4.9.2 Escenario optimista

Bajo esta perspectiva, el número de detección de eventos no prevenidos es prácticamente igual a los incidentes que se generan, lo que reduce la posibilidad de materialización de afectaciones a la tecnología, toda vez que la detección temprana facilita la operación o la toma de decisiones para la contención de los mismos, minimizando así los riesgos derivados del ataque. La Figura 27 permite observar el comportamiento del sistema bajo las condiciones dadas.

Figura 27. Comportamiento del sistema en el escenario optimista



Resulta entonces necesario mejorar los tiempos de análisis, contención y recuperación del servicio que permita responder a los incidentes que se derivan de los eventos contra la red de

forma tal que se reduzcan los riesgos de afectación a la tecnología y al negocio en sus infraestructuras críticas.

4.10 Estrategia de optimización

La herramienta de "Optimización de políticas" de Vensim permite desarrollar una optimización multiobjetivo no lineal (Canzani y Pickl, 2016) de los elementos definidos en el sistema. El propósito definido consistió en minimizar la tasa de eventos no prevenidos y maximizar las tasas de eventos no prevenidos analizados y eventos no prevenidos contenidos y erradicados oscilando los parámetros que se observan en la Tabla 14.

Tabla 14. Oscilación de parámetros para la optimización de la política

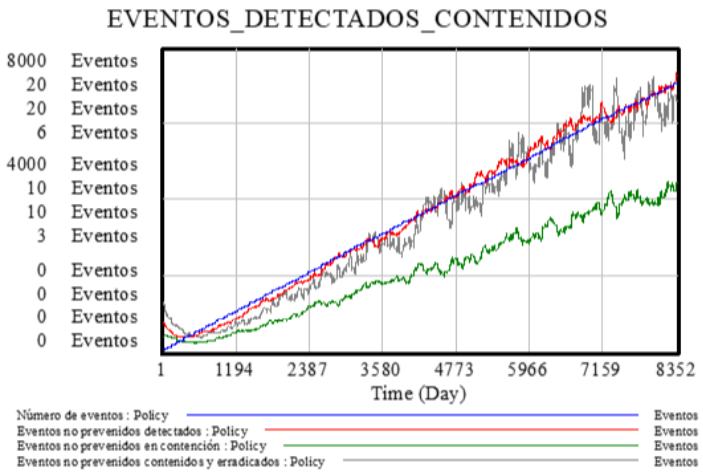
Mínimo	Parámetro	Máximo
1	Estado inicial tecnología de hardware y software	5
0	Conformación de equipo respuesta a incidentes	1
1	Estado inicial definición políticas procesos y procedimientos	5
1	Inicial número de personas	9
1	Nivel de entrenamiento de equipo respuesta a incidentes	5
0.3	Inicial Nivel de riego organizacional	0.9

Los valores máximos encontrados por el algoritmo utilizado por Vensim se detallan a continuación. De igual forma, la Figura 28, permite revisar el comportamiento del sistema bajo las condiciones arrojadas por la herramienta. Llama la atención que el nivel de riesgo organizacional constituye un elemento fundamental dentro de la respuesta a incidentes y la protección de infraestructuras críticas, toda vez que definen el nivel de actuación de las empresas, entendido como inversión en tecnología, personal entrenado y capacitado y la

definición de políticas, procesos y procedimientos encaminados a hacerle frente a los riesgos de afectación del negocio por no continuidad de las operaciones o alteraciones a la información. Los resultados de la optimización se describen a continuación:

- Estado inicial tecnología de hardware y software = 5
- Conformación de equipo respuesta a incidentes = 1
- Estado inicial definición políticas procesos y procedimientos = 5
- Inicial número de personas = 9
- Nivel inicial entrenamiento de equipo respuesta a incidentes = 5
- Inicial Nivel de riesgo organizacional = 0.3

Figura 28. Comportamiento del sistema con política optimizada



5 CONCLUSIONES

Este trabajo pretendió tener una aproximación a la problemática derivada de la interconectividad a nivel mundial y particular en una empresa del sector colombiano en lo concerniente a la ciberseguridad, analizada desde la respuesta a incidentes y la protección de infraestructuras críticas. Esta última afectada directamente por los incidentes de seguridad o eventos no prevenidos que pueden aumentar la probabilidad de afectación a la continuidad de los negocios que son soportados con tecnología.

Se propuso un modelo de largo plazo, con base en el paradigma de DS que permitió identificar las conexiones relevantes dentro del problema y el comportamiento de las variables bajos las relaciones definidas. Es así como se ofrece una perspectiva para continuar investigando, bajo este paradigma, las relaciones existentes para todos los componentes de la ciberseguridad a nivel organizacional y de país.

El modelo permitió identificar aspectos importantes para hacer frente desde la organización, evidenciando la necesidad de fortalecer principalmente, pero sin exclusión de los demás elementos, la medición del nivel de riesgo de ciberseguridad, los tiempos de detección de incidentes, contención y erradicación, dado que no es posible prevenir todos los eventos de seguridad que se materializan pues ellos son cada vez más diversos en cantidad y complejidad. La detección temprana, por lo tanto, se convierte en un factor fundamental pues permitirá tomar decisiones oportunas sobre los ciber activos afectados y consecuentemente sobre la infraestructura.

Es necesario medir de manera constante las variables definidas en el modelo que permita analizar los elementos más relevantes a considerar en la toma de decisiones. Este fue, quizás, el elemento más complejo dentro de la modelación, por el tratamiento dado a los datos

relacionados con la ciberseguridad. Complementar el modelo, no solo desde la estructura, sino desde el comportamiento, facilitarán la toma de decisiones encaminadas a fortalecer los elementos de control necesarios para hacer frente a los problemas asociados a la ciberseguridad.

En ese sentido y con los datos anteriores, es posible concluir que el nivel de riesgo organizacional representa un elemento indefectible para el manejo de incidentes y la protección de infraestructuras críticas, toda vez que permite definir las estrategias necesarias, en términos de políticas, lineamientos, reglas de negocio, tecnología y demás componentes que permitan hacer frente a las amenazas derivadas de la interconectividad. Se hace necesario, entonces, desarrollar políticas encaminadas a la sensibilidad organizacional frente a los riesgos de ciberseguridad, contar con tecnología de vanguardia que permita la detección temprana de eventos no prevenidos, robustecer las políticas y lineamientos empresariales, así como apoyar un equipo calificado y permanentemente capacitado, de manera que puedan hacer frente a la complejidad de los ataques a los que las empresas se ven inmersas.

Es fundamental definir herramientas suficientes como por ejemplo de tipo procedimentales, manuales o automáticas, que permitan evaluar el nivel de exposición o riesgo de las organizaciones, procurando optimizar los tiempos de atención de cada uno de los eventos no prevenidos, reduciendo así los posibles efectos a los que conlleva una afectación de la tecnología por ataques cibernéticos. Dicho esto, la protección de las infraestructuras críticas no dependerá solamente de los controles preventivos, sino que se hace indispensable desarrollar estrategias de detección temprana de los incidentes que permitan la actuación adecuada por parte de los miembros de las organizaciones para atenderlos.

6 TRABAJO FUTURO

Se propone como trabajo futuro, complementar el modelo con los demás elementos definidos en el CMM y los sistemas excluidos en este análisis, definidos previamente, que permitan comprender la ciberseguridad de manera holística y facilite la creación de políticas encaminadas a robustecer la seguridad de las compañías y su competitividad, medidas no solo de manera individual sino a nivel país. De igual manera, el modelo puede ser enriquecido considerando variables como: los tiempos y puntos de restauración objetivo derivados de la continuidad del negocio y el análisis de impacto del negocio, la criticidad del evento no prevenido y por tanto su prioridad de atención.

Resulta igualmente necesario, aplicar el modelo a diferentes empresas catalogadas como compañías con infraestructuras críticas para el país, así como en la entidad centralizadora de control de los elementos relacionados con la ciberseguridad en Colombia, que permita definir, con datos a nivel país, el comportamiento del sistema y proponer políticas encaminadas a fortalecerlo.

7 BIBLIOGRAFIA

Adams, N. & Heard, N. (2014). *Data Analysis For Network Cyber-Security*. https://doi.org/10.1007/s13398-014-0173-7.2

Aguiar Rodríguez, A. (2017). *Understanding the dynamics of Information Security Investments. A Simulation-Based Approach*. Universitetet i Bergen,Radboud Universiteit Nijmegen.

Ahmad, A., Hadgkiss, J., & Ruighaver, A. B. (2012). Incident response teams - Challenges in supporting the organisational security function. *Computers and Security*, *31*(5), 643–652. https://doi.org/10.1016/j.cose.2012.04.001

Akhgar, B., & Arabnia, H. R. (2014). *Emerging Trends in ICT Security Emerging Trends in ICT Security*. https://doi.org/http://dx.doi.org/10.1016/B978-0-12-411474-6.00006-2

Anonymous. (2012). Cybersecurity Policy Making at a Turning Point. *OECD Digital Economy Papers*, (211), 0_1,2,4-56. https://doi.org/http://dx.doi.org/10.1787/5k8zq92vdgtl-en

Barlas, Y. (1996). Formal aspects of model validity and validation in system dynamics. *System Dynamics Review*, *12*(3), 183–210. https://doi.org/10.1002/(SICI)1099-1727(199623)12:3<183::AID-SDR103>3.0.CO;2-4

Barlas, Y., & Carpenter, S. (1990). Philosophical roots of model validation : two paradigms. *System Dynamics Review*, *6*(2), 148–166.

Canzani, E., & Pickl, S. (2016). Cyber Epidemics: Modeling Attacker-Defender Dynamics in Critical Infrastructure Systems. In D. Nicholson (Ed.), *Advances in Human Factors in Cybersecurity* (pp. 377–389). Orlando. https://doi.org/10.1007/978-3-319-41932-9

Cappelli, D. M., Desai, A., Moore, A. P., Shimeall, T. J., Weaver, E. A., & Willke, B. J. (2006). Management and Education of the Risk of Insider Threat (MERIT). *Proceedings of the 24th International Conference of the System Dynamics Society*, *0389*, 52–53.

Cardazzone, A., & Carlini, C. (n.d.). Understanding security policies in the Cyber warfare domain through system dynamics, (1).

Chabinsky, S. (2017). NIST CRIED: The Four Steps of Incident Mitigation.

SecurityMagazine.Com, (March).

Cichonski, P. (2012). Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology. *NIST Special Publication, 800–61*, 79. https://doi.org/10.6028/NIST.SP.800-61r2

Cort, R. (2015). Estado actual de la política pública de ciberseguridad y ciberdefensa en Colombia, (14). Retrieved from http://web.b.ebscohost.com.consultaremota.upb.edu.co/ehost/detail/detail?sid=ff4d4e87-e990-4955-8b8a-0f533b23e547@sessionmgr120&vid=0&hid=118&bdata=Jmxhbmc9ZXMmc2l0ZT1laG9zdC1saXZl#AN=113860736&db=a9h

Coss, R. (2005). Simulacion un enfoque practico.

Dyner, I. (1993). *Dinámica de Sistemas y Simulación Continua en el Proceso de Planificación*. Medellín: Copilito.

Dyner, I., Peña, G. E., & Arango, S. (2008). *Modelamiento para la Simulación de Sistemas Socio-Económicos y Naturales*. Medellín: Universidad Nacional de Colombia Sede Medellín.

Ecds, X. I. V. (2016). Encuentro Colombiano de Dinámica de Sistemas, *1631*.

Ferrillo, P. A., & Veltsos, C. (2016). Next-Level Cybersecurity Incident Response Trends 2016. *Corporate Governance Advisor*, *24*(3), 6–8. Retrieved from http://0-search.ebscohost.com.pugwash.lib.warwick.ac.uk/login.aspx%3Fdirect%3Dtrue%26db%3Dbth%26AN%3D114737834%26site%3Deds-live&group=trial

Flórez, A., Serrano, L., Gómez, U., Suárez, L., Villarraga, A., & Rodríguez, H. (2016). Analysis of Dynamic Complexity of the Cyber Security Ecosystem of Colombia. *Future Internet*, *8*(3), 33. https://doi.org/10.3390/fi8030033

Forrester, J. W. (1971). Counterintuitive behavior of social systems. *Theory and Decision*, *2*(2), 109–140. https://doi.org/10.1016/S0040-1625(71)80001-X

Forrester, J. W. (1992). System Dynamics, Systems Thinking, and Soft OR, *10*(2), 1–14.

Forrester, J. W., & Senge, P. (1980). Tests for building confidence in system dynamics models. *TIMS Studies in the Management Sciences*, *14*, 209 – 228.

Friedman, D., & Cassar, A. (2004). *Economic Lab: An Intensive Course in Experimental*

Economics. London: Routledge.

García Zaballos, A., & González Herranz, F. (2013). From Cybersecurity to Cybercrime: A Framework for Analysis and Implementation, (September). Retrieved from http://publications.iadb.org/handle/11319/5998

Giraldo, D. P. (2013). *Análisis de la dinámica de la seguridad alimentaria en un país en desarrollo -caso colombiano-. Tesis Doctoral*. Escuela de Ingeniería. Universidad Pontificia Bolivariana.

Holdings, T. (2016). *Trustwave global security report*. *Retrieved June*.

Holdings, T. (2017). *Trustwave Global Security Report*.

ITU. (2015). Índice Mundial de ciberseguridad y perfiles de ciberdefensa. Retrieved from http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-S.pdf

Jindal, H. (2014). Cyber security: Risk management. *Journal of the Insurance Institute of India*, (June), 95–103. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=edsnbk&AN=14F5FC14D0FA4870&site=eds-live

Kossakowski, K., Allen, J., Alberts, C., Cohen, C., & Ford, G. (1999). Responding to Intrusions., (February), 44. Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA360500

Luiijf, E. (2014). *Cyber Crime and Cyber Terrorism Investigator's Handbook*. *Cyber Crime and Cyber Terrorism Investigator's Handbook*. https://doi.org/10.1016/B978-0-12-800743-3.00003-7

Ministerio de Interior y Justicia, Exteriores, M. de R., Nacional, M. de D., Comunicaciones, M. de T. de la I. y las, Seguridad, D. A. de, Planeación, D. N. de, & General, F. (2016). CONPES 3854 - POLÍTICA NACIONAL DE SEGURIDAD DIGITAL. Retrieved from https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf

Ministerio de Interior y Justicia, Ministerio de Relaciones Exteriores, Ministerio de Defensa Nacional, Ministerio de Tecnologías de la Información y las Comunicaciones, Departamento Administrativo de Seguridad, Departamento Nacional de Planeación, & Fiscalía General. (2011). Conpes 3701 Lineamientos de Política para Ciberseguridad y

Ciberdefensa, 43. Retrieved from http://www.mintic.gov.co/index.php/docs-normatividad?task=download.file&fid=46.741&sid=54

Ministerio de Tecnologías de la Información y las Comunicaciones. (2008). Plan Nacional de Tecnologías de la Información y las Comunicaciones.

Miniwatts Marketing Group. (2018a). Internet Usage Statistics. Retrieved from https://www.internetworldstats.com/stats.htm

Miniwatts Marketing Group. (2018b). Uso de internet y estadísticas de población para Sur América. Diciembre 31 de 2017. Retrieved from https://www.internetworldstats.com/stats15.htm#south

Morecroft, J. (2007). *Strategic Modelling and Business Dynamics: A Feedback Systems Approach*. John Wiley & Sons.

Morecroft, J. D. W. (2015). *Strategic modelling and business dynamics. A feedback system aproach*.

Morgan, S. (2017). 2017 Cybercrime Report, 14. Retrieved from https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf

Mouton, F., Malan, M. M., Leenen, L., & Venter, H. S. (2014). Social engineering attack framework. *2014 Information Security for South Africa - Proceedings of the ISSA 2014 Conference*. https://doi.org/10.1109/ISSA.2014.6950510

NIST. (2014). Framework for Improving Critical Infrastructure Cybersecurity. *National Institute of S*, 1–41. https://doi.org/10.1109/JPROC.2011.2165269

OCDE. (2002). Directrices de la ocde para la seguridad de sistemas y redes de información, 1–12.

Parada Serrano, D. J., & Gómez Prada, U. E. (2016). La Seguridad de la Información desde la Dinámica de Sistemas. *Ponencia Presentada Al XIV ECDS - 2016*.

Porrúa, M., & Contreras, B. (2016). Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? Retrieved from https://publications.iadb.org/handle/11319/7449?locate-attribute=en&locale-attribute=pt&locale-attribute=es&

Real Options Valuation. (2017). Risk Simulator.

Richardson, G., & Pugh, I. A. (1989). *Introduction to system dynamics modeling*. Waltham:

Pegasus Communications.

Smith, D. (1994). Forming an Incident Response Team. *Proceedings of the FIRST Annual Conference*, (January 1995), 1–37.

Statistics, O. of N. (2017). Cyber Attacks 2012 to 2017. Retrieved from https://www.ons.gov.uk/aboutus/transparencyandgovernance/freedomofinformationfoi/cyberattacks2012to2017

Sterman, J. D. (1991). A Skeptic's Guide to Computer Models. In G. P. RICHARDSON (Ed.), *Modelling for Management*. Aldershot, UK: Dartmouth Publishing Company.

Sterman, J. D. (2000). *Business Dynamics* (McGraw Hil). New York.

Sterman, J. D. (2002). All models are wrong: reflections on becoming a systems scientist. *System Dynamics Review*, *18*(4), 501–531. https://doi.org/10.1002/sdr.261

Sterman, J. D. (2003). *Systems Thinking and Modeling for a Complex World*.

University of Oxford. (2014). Cyber Security Capability Maturity Model (CMM), (Cmm), 1–45. Retrieved from http://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM Version 1_2_0.pdf

US Department of Homeland Security. (2014). Department of Homeland Security Cybersecurity Capability Maturity Model White Paper.

Vacca, J. (2014). *Cyber Security and IT Infrastructure Protection*. (N. McFadden, Ed.). Steven Elliot.

Vennix, J. (1996). *Group Model-Building: Facilitating Team Learning Using System Dynamics*. Chichester: John Wiley & Sons.

Vose, D. (2008). *Risk Analysis - A quantitative guide*. (L. John Wiley & Sons, Ed.) (Third edit). John Wiley & Sons, Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, England.

World Economic Forum. (2012). *Global Risks 2012*. *Continuity Central*. Retrieved from http://continuitycentral.com/news06097.html

World Economic Forum. (2018). *The global risks report 2018, 13th edition*. https://doi.org/978-1-944835-15-6

Young, C. (2016). *Information Security Science: Measuring the Vulnerability to Data Compromises*. Retrieved from https://books.google.com/books?id=eUq0CwAAQBAJ