A technological analysis of Colombia's cybersecurity capacity: a systemic perspective from an organizational point of view

Análisis de la capacidad de ciberseguridad para la dimensión tecnológica en Colombia: una mirada sistémica desde la organización

Análise da capacidade de segurança cibernética para a dimensão tecnológica na Colômbia: uma visão sistêmica da organização

Alexis Mauricio Serna Patiño[1]
Diana Patricia Giraldo Ramírez[2]

Received: January 15th, 2019
Accepted: March 30th, 2019
Available: May21th, 2019

How to cite this article:
A. M. Serna-Patiño, D. P. Giraldo-Ramírez, "A technological analysis of Colombia's cybersecurity capacity: a systemic perspective from an organizational point of view", *Revista Ingeniería Solidaria*, vol. 15, n.° 2, 2019.
DOI: https://doi.org/10.16925/2357-6014.2019.02.07

Research article. https://doi.org/10.16925/2357-6014.2019.02.07

[1] Universidad Pontificia Bolivariana
E-mail: alexis.serna@upb.edu.co
ORCID: https://orcid.org/0000-0002-8255-911X

[2] Universidad Pontificia Bolivariana
ORCID: https://orcid.org/0000-0002-1500-0279

Abstract

Introduction: This paper is a product of the research Project "A technological analysis of Colombia's cybersecurity capacity: a systemic perspective from an organizational point of view" developed at the Universidad Pontificia Bolivariana in the year 2018.

Objective: Starting from the Dynamics System paradigm, this study considers the technological dimension with respect to cybersecurity for incident response and critical infrastructure protection, making reference to the Cybersecurity Capability Maturity Model and the best practices defined by the National Institute of Standards and Technology - NIST.

Methodology: The research starts from the dynamics hypothesis and using the representation of a formal simulation model as its input so as to analyze different scenarios and the development of future policy in this field.

Conclusions: The risk at the organizational level represents a fundamental element for management of incidents and the protection of critical infrastructures, since it allows defining the necessary strategies, in terms of policies, guidelines, business rules, technology and other elements that allow the country to face the threats derived from interconnectivity. It is therefore necessary to develop policies aimed at organizational sensitivity in terms of cybersecurity risks.

Originality: The scenarios that we propose should assist decision makers in making investments in favor of the development and evolution of Cybersecurity in Colombia and, therefore, of the organizations that contribute to the development of the country.

Restrictions: The data we used to conclude this study, was obtained from an organization that is classified as critical to infrastructure, so it is important to obtain access to the information of the main organization in Colombia in charge of cybersecurity and other companies.

Keywords: Cybersecurity, Incident Response, Critical Infrastructure, System Dynamics.

Resumen

Introducción: Este artículo es producto del proyecto de investigación "Análisis de la capacidad de ciberseguridad para la dimensión tecnológica en Colombia: una mirada sistémica desde la organización" desarrollado en la Universidad Pontificia Bolivariana en el año 2018.

*Objetivo***:** Partiendo del paradigma de simulación de la dinámica de sistemas, éste 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 (NIST).

Metodología: 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.

Conclusión: El nivel de riesgo organizacional, representa un elemento fundamental para la respuesta a incidentes y la protección de infraestructuras críticas, dado que permite definir las estrategias necesarias, en términos de políticas, directrices, reglas de negocios, tecnología y otros elementos que contribuyen enfrentar las amenazas derivadas de la interconectividad. Es necesario desarrollar políticas dirigidas a la sensibilidad organizacional en términos de riesgos de ciberseguridad.

Originalidad: los escenarios propuestos deben contribuir a los tomadores de decisiones para hacer inversiones a favor del desarrollo y la evolución de la ciberseguridad en Colombia y, por lo tanto, de las organizaciones que contribuyen al fortalecimiento del país.

Restricciones: los datos utilizados para concluir en este estudio se obtuvieron de una organización que está clasificada como infraestructura crítica, por lo que es importante obtener acceso a la información de la organización principal de Colombia encargada de la ciberseguridad y de otras compañías.

Palabras clave: ciberseguridad, respuesta a incidentes, infraestructuras críticas, dinámica de sistemas.

Resumo

Introdução: Este artigo é um produto do projeto de pesquisa "Análise da capacidade de segurança cibernética para a dimensão tecnológica na Colômbia: uma visão sistêmica da organização" desenvolvida na Universidad Pontifícia Bolivariana no ano de 2018.

Objetivo: Partindo do paradigma da Dinâmica de Sistemas, este estudo considera a dimensão tecnológica da segurança cibernética para resposta a incidentes e proteção da infraestrutura crítica, tendo como referência o Modelo de Maturidade da Capacidade de Cibersegurança e as melhores práticas definidas pelo Instituto Nacional de Padrões e Tecnologia - NIST.

Metodologia: Partimos da hipótese da dinâmica e da representação de um modelo formal de simulação como insumo para analisar diferentes cenários e desenvolvimento de políticas futuras neste campo.

Conclusões: o nível de risco organizacional representa um elemento fundamental para a gestão de incidentes e proteção de infraestruturas críticas, pois permite definir as estratégias necessárias, em termos de políticas, diretrizes, regras de negócio, tecnologia e outros elementos que permitam enfrentar as ameaças derivadas da interconectividade. Portanto, é necessário desenvolver políticas voltadas para a sensibilidade organizacional em termos de riscos de segurança cibernética.

Originalidade: os cenários que propomos devem servir aos tomadores de decisão para fazer investimentos em favor do desenvolvimento e evolução da segurança cibernética na Colômbia e, portanto, das organizações que contribuem para o desenvolvimento do país.

Restrições: os dados que usamos para concluir neste estudo, foi obtido a partir de uma organização que é classificada como infraestrutura crítica, é importante para obter acesso à informação pública na concepção da empresa principal para gerenciamento de segurança cibernética na Colômbia e outras organizações.

Palavras-chave: segurança cibernética, resposta a incidentes, infraestrutura crítica, dinâmica do sistema.

Introduction

Cybersecurity as a general concept has been gaining relevance because of its strategic importance, both for citizens and society, for companies and for the country. In 1988 the government of the United States created the first Computer Emergency Response Team (CERT), after the MORT worm paralyzed a portion of the Internet [1]. Estonia's government suffered what is known as the biggest cyber-attack in history, where the presidency, the parliament, the ministries and two large banks were affected [2]. In July 2009, the government of the United States suffered attacks that affected the White House, the Department of Internal Security, the Department of Defense, among others. In 2010, the Spanish guard dismantled what, by then, was considered the largest Botnet or zombie computer network with more than 13 million IP addresses, distributed in 190 countries around the world [2].

According to [3], "because of increasing interconnection, information systems and networks are more vulnerable, since they are exposed to a growing number, as well as to a greater variety, of threats and vulnerabilities. This creates new challenges that must be addressed in terms of security".

In the same way, [4] refers to the importance of cybersecurity at the country level, denoting a growing increase in the budget of the nation's objectives to address the issue, particularly in the United States of America, through the creation of the United States Cyber Command; a unified command that depends on the National Security Agency of the United States.

Likewise, he denotes an increase of 8.1 %, between 2009 and 2010, of the annual cybersecurity budget, which shows an acknowledgment of the risk derived from interconnection.

Morgan [5], estimates that 51 % of the world population in the year 2017, had access to the Internet, which is equivalent to 3.8 billion users, and projected that by 2030, 90% of the population —approximately 8.5 billion people— will have such access which consequently increases the risks derived from interconnectivity.

Based on the Global Risk Report published in 2018, attacks on organizations have doubled in the last 5 years and incidents that were once considered extraordinary, today are much more commonplace [6]. For example, the ransomwares WannaCry and NotPetya, affected more than 300,000 computers in about 150 countries with losses close to US $ 300 million, generated risks of unavailability of services in multiple companies including banks, energy companies, ministries, among others.

Colombia has made evident efforts in this field, such as the generation of Conpes 3701 (giving life to the Colombian CERT), whose objective does not differ from the main definition enunciated by Cardazzone & Carlini. (n.d.), which is part of protecting the security of the national economy favoring the continuity of operations in the event of a security incident; and Conpes 3854, defining Colombia's cybersecurity policy [2], [7] to face the emerging challenges of cybersecurity. In that sense, the Colombian Government has developed important advances aligned with the Inter-American Development Bank (IDB) and Organization of American States (OAS) in terms of policies, legal frameworks and technology regarding cybersecurity. Similarly, on September 3rd, 2015, the Colombian National Operation Council (Consejo Nacional de Operación), considering Conpes 3701, approved the Cybersecurity guide through the 788 agreement. It motivates the generators, transmitters and distributors of the National Interconnected System to carry out the identification of critical assets and cyber assets, risks and vulnerabilities at the level of management of cybersecurity in

e-ISSN 2357-6014 / Vol. 15, n°. 2 / mayo 2019 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

the operations of companies, recognizing the importance of the topic in the national context.

The complexity of cybersecurity in any environment, requires constant decision making by human beings, which can be taken even through technology. The actions derived from them can have short, medium or long term repercussions, so they must be analyzed systemically, systematically and be organized, into sets of variables or data (that changes constantly), recognizing the normal dynamics of cybersecurity in an ever-more connected world. Thus, it is necessary to address the issue using computer simulation, in order to make an understanding approach to the phenomenon generated by it, from different perspectives. For this, the System Dynamics (SD) paradigm is a fundamental tool for modeling existing relationships within the system.

[8] uses SD to demonstrate the lack of available tools when understanding the existing risk of internal threats to organizations in terms of cybersecurity; making simulations of policies and accounting for cultural, technical and procedural factors. On the other hand, Cardazzone & Carlini. (n.d.) proposed a model from the SD, to analyze the impact of some cyber-attacks on national defense systems and the way in which the organizations created to counter them (CERT) have responded to them. It is concluded that, if it is important to have appropriate mechanisms to detect attacks, it is even more relevant to determine the real impact of them in order to minimize unforeseen damage in attacks.

Other authors such as [9] have simulated, through the same SD paradigm and the theoretical combination of games, cybersecurity in the protection of critical infrastructures by defining proactive scenarios and reactive defense, recognizing attacks of increasing complexity for their detection and containment, concluding that "the cost-efficiency of periodic defenses depends on the optimization of prevention time components rather than IT (Information Technology) investments in recovery plans".

Likewise, [10] conducted a study on the ecosystem of cybersecurity in Colombia, through the SD, affirming that the created influence diagram, helps when understanding the need to prevent cybercrime, observing additionally that sovereignty is the main element that does not influence the other elements. However, they conclude that it must be the main element to be protected within the cybersecurity ecosystem in Colombia, along with resources and assets that may be affected by the commission of cybercrimes. In summary, the model shows the need to protect sovereignty and reduce cybercrimes within the modeled ecosystem.

This paper aims to recognize the current problem of cybersecurity, referring to the response to incidents and protection of critical infrastructures, as a necessary and indispensable element for the development of countries and organizations. A causal

diagram is proposed which gives a systemic view of the problem and allows for the modeling of existing relationships, collecting relevant elements for the management of cybersecurity incidents and consequently, the protection of critical infrastructures. This provides an approach that allows for the observation of the variables defined, the structure and the effects of them in the different elements, thus facilitating a discussion and serving as a foundation for future works of modeling.

[11] in their study: "Cybersecurity. Are we ready in Latin America and the Caribbean?" present the results of the evaluation of maturity in the countries of Latin America and the Caribbean under the Cybersecurity Capacity Maturity Model (CMM), developed by the Global Cyber Security Capacity Centre at Oxford University, which includes 5 dimensions. They are:

- Policy
- Society
- Education
- Legislation
- Technology

Porrúa and Contreras therefore consider that it is necessary to analyze that the variables described in the CMM cannot be either static or independent, which is a normal dynamic within the system that should assist decision makers in makeing investments in favor of the development and evolution of Cybersecurity in Colombia and, therefore, of the organizations that contribute to the development of the country.

Materials and methods

In order to promote understanding of the relationships that may exist in cybersecurity, and the complexity already mentioned, it is necessary to use tools that allow for their understanding and approximation through proven practices of modeling reality such as, for example, SD, given that, as stated by Forrester [12], these allow for the understanding and modeling of the real world.

In this sense, the SD provides elements that help in the understanding of reality to be approximated under systemic perspectives, enabling the study and elaboration of conclusions that facilitate the decision-making process.

For this research, a time horizon of 20 years measured in days was defined; the input variables and the systems and subsystems that make up the model were identified, and those excluded, the endogenous and exogenous variables; the Delphi

e-ISSN 2357-6014 / Vol. 15, n°. 2 / mayo 2019 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

method was used to identify minimum and maximum times defined in the model and the pertinent statistical analyses were carried out. Finally, we used Vensim DSS (ver. 6.3) of double precision for macOS.

In general, the research was carried out systematically under the exploratory perspective, gathering the fundamental and conceptual foundations of cybersecurity worldwide. For this, technological, surveillance was used to collect the main characteristics associated with cybersecurity; the dynamic hypotheses were formulated, the elements of the system, their relationships and the flows were identified, and then a model was proposed through the SD associated with cybersecurity in the aforementioned aspects.

Below, the most relevant aspects of the research for this article are detailed.

To contribute to the understanding of the possible relationships existing in the defined problem, the cybersecurity framework created by the National Institute of Standards and Technology of the United States (NIST), defines 5 fundamental principles. Namely: Identify, protect, detect, respond and recover, about which, [13], affirms that they are a useful tool for organizations when facing the risks of cybersecurity, seeking to face and develop continuous improvement, under international frameworks, regarding a response to incidents.

In this sense, [14] proposes the following diagram, Figure 1, for the life cycle of Incident Response:

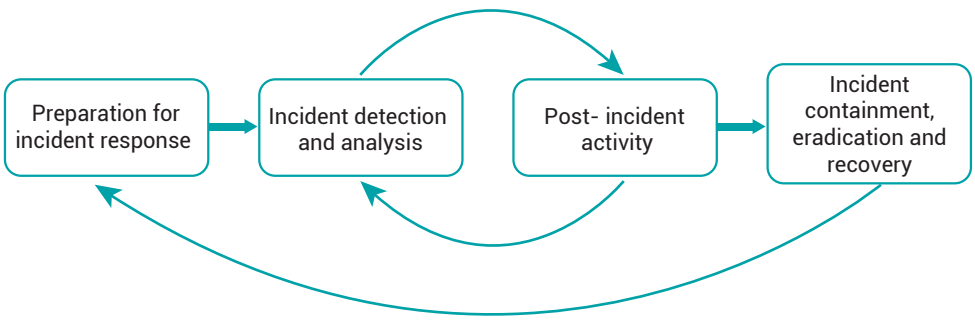


Figure 1. Life cycle of the incident response
Source: adapted from[14]

At the same time, [15], in the framework for the improvement of cybersecurity in critical infrastructures, proposes as an additional and fundamental component, risk management, as an important element for decision making, for which, the level of organizational awareness and appetite for risk, determine the level of investment and, therefore, the actions to be taken when strengthening the mechanisms defined for the hardening of controls associated with cybersecurity.

Since 1999, [16] proposed a series of practical recommendations, still valid, in order to respond to the intrusions that could arise from connectivity. In that sense, they highlighted the need to understand the extent and sources of the intrusion, as well as the imperative to protect sensitive data, systems and networks, probing for the continuity of the operation and recovery after an attack materialized. Similarly, the collection of information and evidence for subsequent investigations, including legal evidence, are highlighted as an important part in the handling of incidents. These recommendations are summarized in the Table 1.

Table 1. Summary of recommended safety practices

Category	Recommendation
Preparation	1. Establish policies and procedures to respond to intrusions
	2. Preparing to respond to intrusion
Incident response	1. Analyze all available information to characterize the intrusion.
	2. Communicate to all parties the progress of the intrusion and its status
	3. Collect and protect the information associated with the intrusion
	4. Apply short-term solutions to contain the intrusion
	5. Remove all forms of access of the attacker
	6. Return the system to the normal state of operation
Subsequent actions	1. Identify and implement safety lessons learned

Source: [16]

Analysis of data grouped by days

To facilitate the understanding of the behavior of the data in this unit of measurement, it was decided to model them with the help of the Risk Simulator tool [17]. In that sense, the data was graphed, obtaining Figure 2, where the slope of the trend line is almost zero, assuming that there are days where no events occur:

e-ISSN 2357-6014 / Vol. 15, n°. 2 / mayo 2019 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

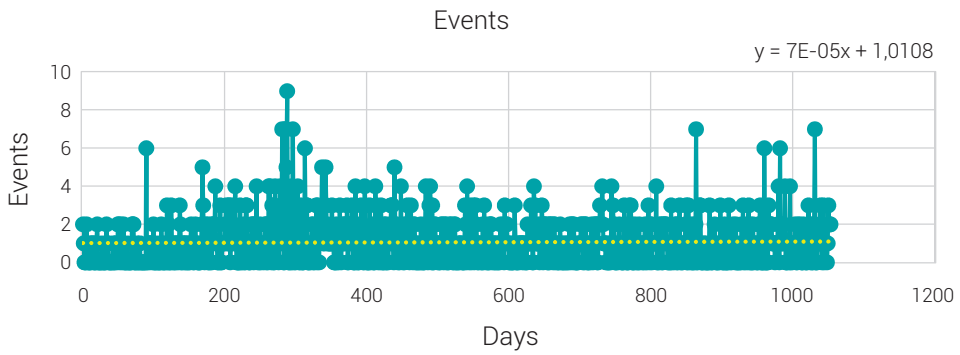


Figure 2 .Grouping of the data (events) obtained
Source: own work

With the data, the following distribution adjustment —negative binomial— was obtained for the discrete variable "Events", which is observed in Table 2.

Table 2. Distribution adjustment results.

Concept	Result
Fitted assumption	1,05
Distribution fitted	**Negative Binomial**
Success required	2,00
Probability	0,70
Chi-squared	66,36
MAPE % for statistical Test	0,07%

Variable	Current	Theoretical
Mean	1,05	0,87
Standard Deviation	1,23	1,12
Asymmetry	1,73	1,67
Kurtosis in exceed	4,85	3,80

Source: own work

Once the distribution was identified, random data was generated for the negative binomial distribution with required successes of 2 and a probability of 0.70, obtaining the graph shown in Figure 3.

e-ISSN 2357-6014 / Vol. 15, n°. 2 / mayo 2019 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

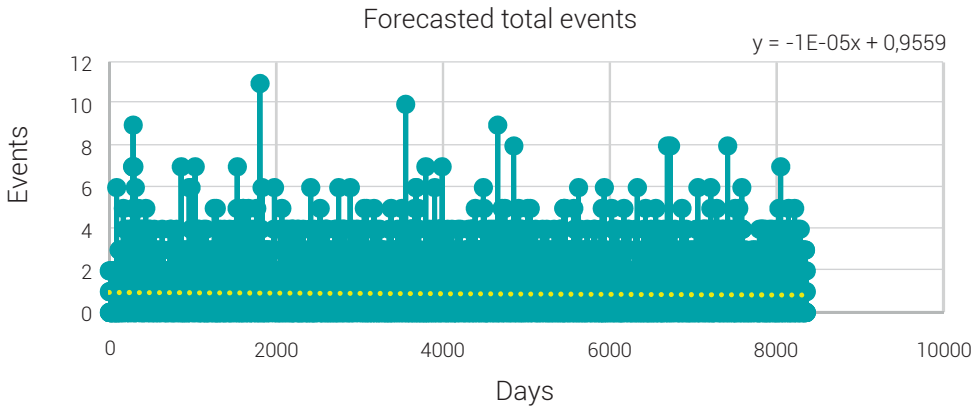


Figure 3. Data generated for 20 years (units in days)
Source: own work

The model used this unit of measurement to perform the corresponding calculations and the respective analyses.

Times to detect, analyze and contain an incident and restore service

As an international reference, the reports issued by [18], [19] show, in general, a decrease in times to identification and containment of security incidents, for example, 86 days from the intrusion to the detection in the year 2014 to 49 days in 2016 —as shown in Table 3—, so we can conclude that response times have decreased considerably, denoting a constant concern of the organizations to be more efficient in this regard.

Table 3. Days from the intrusion to Detection and containment

Year	Intrusion until Detection (days)	Intrusion until Containment (days)
2014	86	111
2015	80,5	63
2016	49	63

Source: adapted from [18], [19]

However, in the lack of measurable response times at the organizational level and interest in the proposed model, we proceeded, through the Delphi method with experts in cybersecurity, to identify the minimum and maximum times of each of the variables identified in the model. For the modeling, the PERT distribution was used as

a reference for the generation of random numbers. According to [20], this distribution is a version of the Beta distribution and requires the same parameters: minimum, most probable and maximum and can be used when the opinion of experts is available, whose equation is as follows:

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

where,

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

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

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

The values defined by the experts, through a simple average, are shown in Table 4.

Table 4. Grouping of time defined by experts.

	Min (days)	**Max (days)**
Detection time	0,01041667	0,12268519
Analysis time	0,00810185	0,11111111
Containment time	0,07291667	1,34722222
Restore service time	0,16666667	4,33333333

Source: own work

Mode and expected value were calculated as follows:

$$Mode = \frac{1}{3}(Max - Min) + Min$$

and

$$Expected\ value = \frac{Min + 4Mode + Max}{6}$$

With these parameters, random numbers were generated with the PERT distribution for the 20 years, measured in days, for the simulation and for each of the

e-ISSN 2357-6014 / Vol. 15, n°. 2 / mayo 2019 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

variables. The above was developed to generate randomness in the analysis times and reflect a closer model to reality.

Results

Causal diagram

Next, the proposed causal diagram is described, which groups together the interdependencies of the different variables that can be translated in the flows and levels model. Sterman defines the causal diagrams as simple maps that show the causal relationships between the variables that start from a cause and reach the effect [21]. On the other hand, the causal diagrams help identify the connections between the parts of the system, in a clear and concise way [22]. The cause - effect relationships are illustrated from arrows that start from the first to the last. The polarity, located in the upper parts of the arrows, describes the effect that the variable causes in the variable effect, that is, how the variable ***'x'*** —cause— influences the effect ***'y'*** —effect—, which is denoted by the following equation:

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

Figure 4, groups the first subsystem, called "Preparation" and shows the proposed relationships to have an approach to the problem and some relevant elements that precede the incidents response. As shown in cycle B1, the preparation starts from the perception of cybersecurity risk that an organization may have [23]. The level of risk that an organization can determine [24], as well as its situational awareness, will give rise to the definition of policies, processes and procedures [16] in order to establish necessary controls that favor by the reduction of the impacts if the risk materializes or the decrease in the probability of its occurrence [25]. Such control elements will lead to concrete actions such as, for example, the conformation of an incident response team [26] that allows facing the events that materialize [27].

The team, given the constant updating of techniques and vectors of attack, must periodically receive training on current trends and different methods of attack and containment [28]. Similarly, as seen in cycle B2, the presence of updated technology, in this particular case understood to be both hardware and software, offers greater coverage to critical cyber-actors, from preparation through security baselines; hardening, understood as the practice of securing systems to reduce the level of exposure

e-ISSN 2357-6014 / Vol. 15, n°. 2 / mayo 2019 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

[25], up to the monitoring and recovery of them [29]. These elements can contribute to the proper functioning of incident response from the previous preparation that must exist. However, higher levels of preparedness for handling incidents, should tend to decrease the organizational risk index, not meaning that the other elements of the system should have the same line. In any case, it must, in a permanent way, tend to strengthen them.

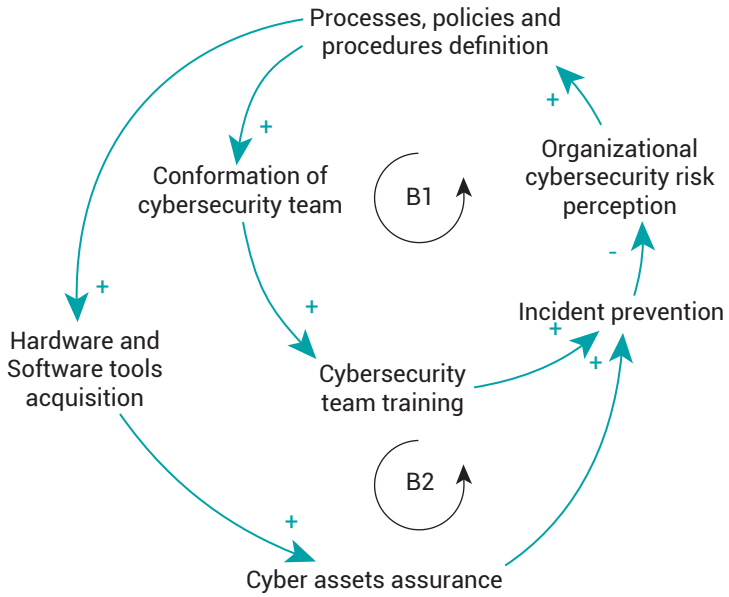


Figure. 4 Subsystem "Preparation"
Source: own work

On the other hand, Figure 5, in cycles B3 and B4, relates to the second subsystem of "incidents detection and analysis". It is the first step in the incidents response and implies the need to identify the different attack vectors since any cybersecurity incident must be detected in the shortest possible time so as to minimize the impacts that may derive from it [30]. A cybersecurity incident materializes when it is directly or indirectly affected by what is known as the triad of "Confidentiality, Integrity and / or Availability" (CIA) [31], so that its early detection is a critical success factor in the minimization of impacts [32]. Similarly, the more incidents occur, the higher the detection level of the attack vectors must be. Any attack is developed in a specific scenario that may or may not have coverage or scope in a whole network, for which, it must determine the actual distribution of the scenario where it occurs so as to limit and / or define the actions required to respond to it. In other words, a punctual analysis of

each of the attacks and correlations with other incidents or events must be performed to determine the next steps to contain and eradicate them.

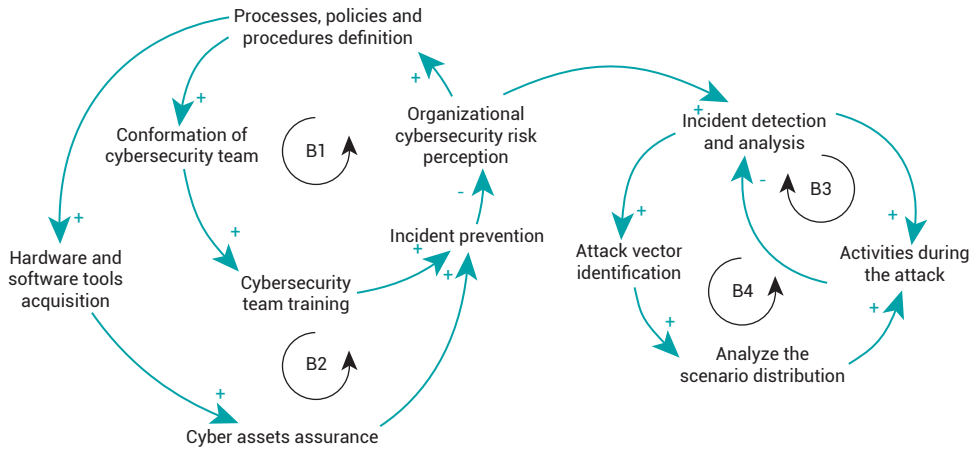


Figure 5. Grouping of subsystems: Preparation, Detection and analysis
Source: own work

In the third subsystem, in Figure 6, "Activities during the incident", all the specific activities are developed to reduce the life-time of the incidents and return the network to optimal operating conditions and minimize the impacts derived from the techniques of attack [33] as observed in the reinforcement cycle R1. For this it is necessary to be able to have clarity and definition of current containment and eradication strategies and be able to build new ones, in an agile way, depending on the different types of attack. Each strategy must consider the type of decisions that must be made about cyber-assets and even about people in such a way that the necessary evidence of the attack is preserved for its subsequent analysis and, if appropriate, judicialization. Thus, all the incidents, once identified and analyzed, must be contained and eradicated in the shortest time possible, in order to minimize the effects that derive from them. Containment can be considered as an element that does not solve the root of the incident, for example, to isolate the affected cyber-assets of the network, while eradication supposes the elimination of the problem of the network [33]; for this reason, they are considered as individual elements within the system. Finally, once the incident has been eradicated, it is necessary to restore the system to the normal state of operation, with the necessary corrective measures so that, at least, the same incident does not materialize again [33].

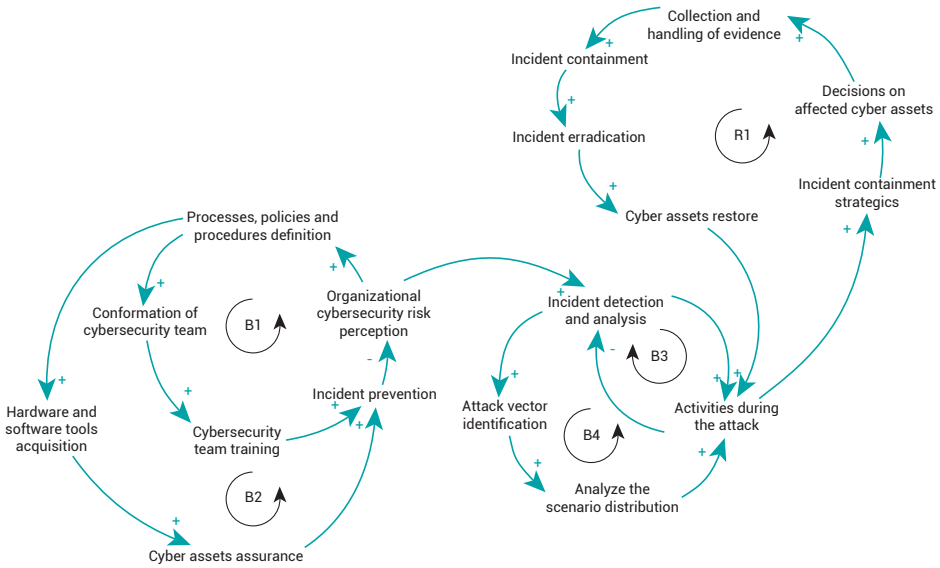


Figure 6. Grouping of subsystems: Preparation, Detection and analysis and Activities during the incident
Source: own work

The last subsystem, "Post-incident Activities" of Figure 7, which can be observed in cycle R2, should allow for the collection of the lessons learned in the preceding subsystems, in such a way that it can generate knowledge about the activities carried out satisfactorily and those carried out inadequately, providing necessary elements to enrich the other components of the system in a holistic way [14].

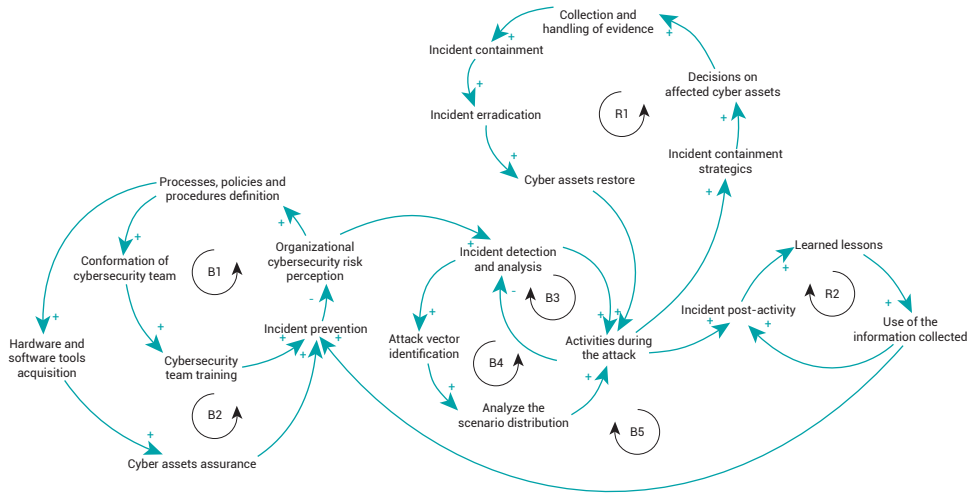


Figure 7. Grouping of subsystems: Preparation, Detection and analysis, Activities during the incident and Post-incident activities
Source: own work

The proposed causal diagram develops the four main components of the incident response life-cycle proposed by NIST, which can be analyzed as complementary subsystems, which provide an approximation to the understanding of the problem. Figure 8 groups them in the following tables:

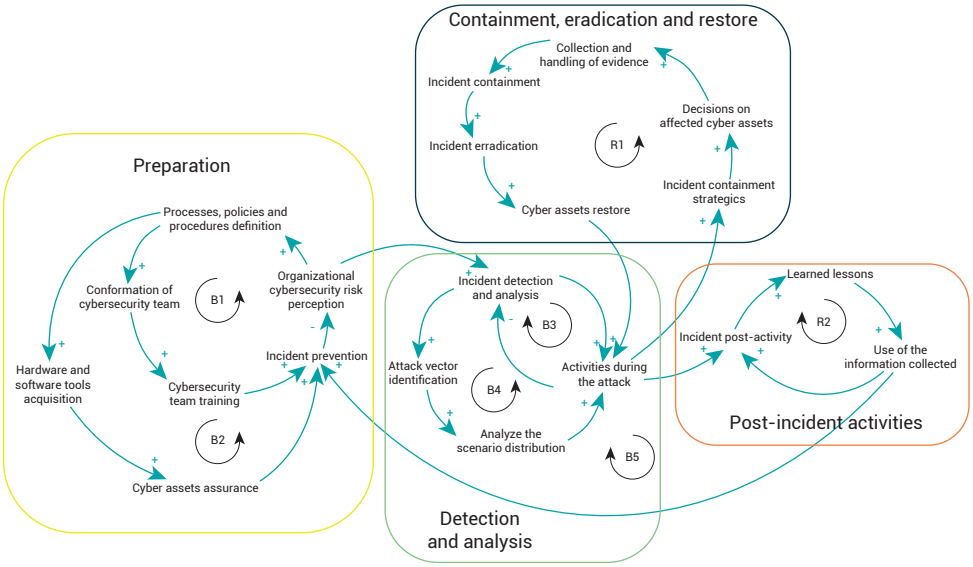


Figure 8. Causal diagram grouped with respect to the life cycle of incident response
Source: own work

Validation

Modeling with SD requires iterative processes that start from the definition of the model and can extend even after the implementation of the policies derived from it. In this sense [34], it is essential to validate the model to verify the adequacy of the model, regarding some variables, allowing the analysis of the defined relationships and the logical and experimental reality. So [34] states that the validation in SD includes two components, defined as the validation of the structure of the model and the validation of the behavior of the results of the model.

For this exercise, it was proposed to analyze: dimensional consistency, extreme conditions, integration error tests and sensitivity analysis, [35,36].

- **Dimensional Consistency:** The units of the variables defined in the model were verified, finding coherence in the defined units**.**

- **Extreme conditions:** Zero received events were assumed, within the negative binomial distribution associated with the rate of events received, observing an adequate behavior of the system where the initial unprepared events are evacuated and the curve tends to zero, as evidenced by Figures 9 and 10. It should be noted that events are considered a discrete variable, since they exist or do not exist and are always greater than or equal to zero. Likewise, it was assumed that there were no people in the team, finding that the detected unforeseen events correspond to the input data of events, that is, both distributions are very similar, as shown in Figure 11.

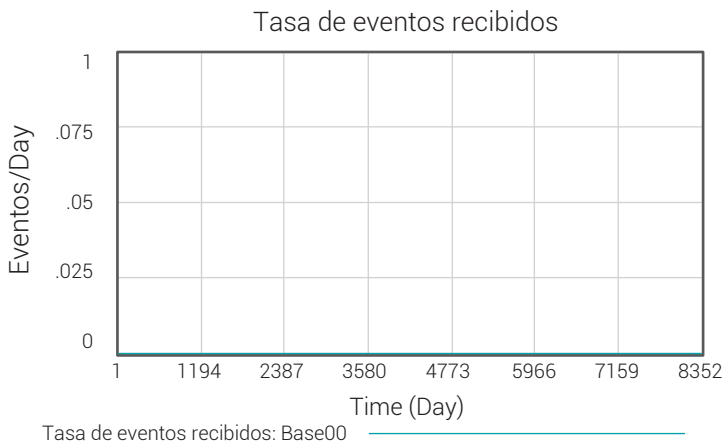


Figure 9. Rate of events received in extreme conditions
Source: own work

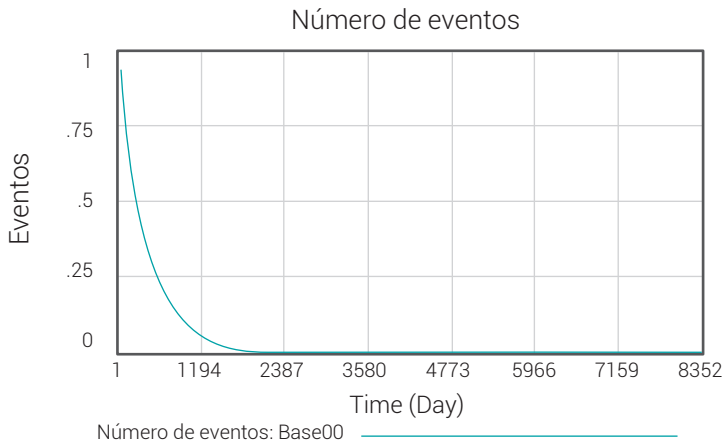


Figure 10. Number of events in extreme conditions
Source: own work

e-ISSN 2357-6014 / Vol. 15, n°. 2 / mayo 2019 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

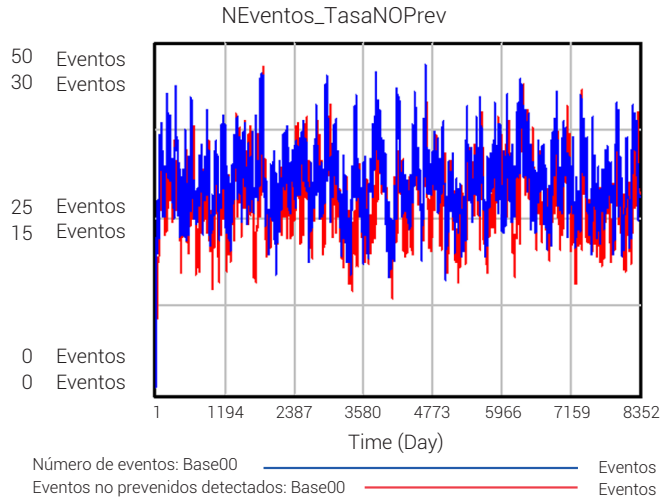


Figure 11. Total number of events and non-prevented events in extreme conditions with zero (0) people
Source: own work

Likewise, extreme times were assumed for the detection of incidents, observing a greater number of unforeseen events or incidents, as shown in Figure 12. This corresponds to the expected reality, since the later the detection time for an event, the greater the number of events that can become incidents.

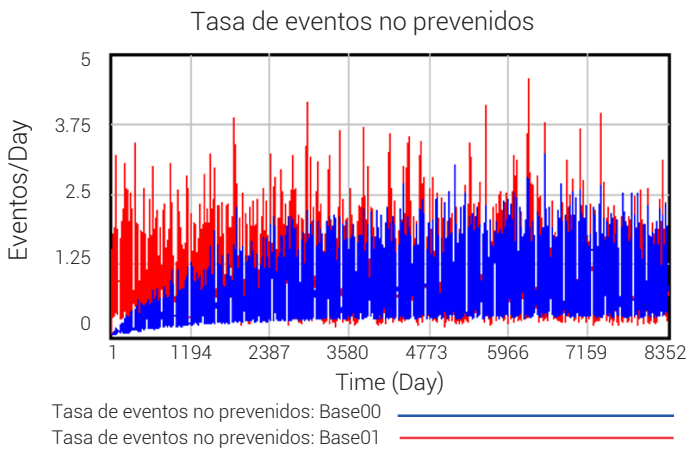


Figure 12. Rate of non-prevented events with extreme impact of detection time
Source:

- **Integration error tests:** the model was executed with the integration types Euler, RK4 Auto, Difference, RK2 Fixed, Rk2 Auto and RK4 Fixed and no sensitivity was shown in the results of the model as shown in Figure 13.

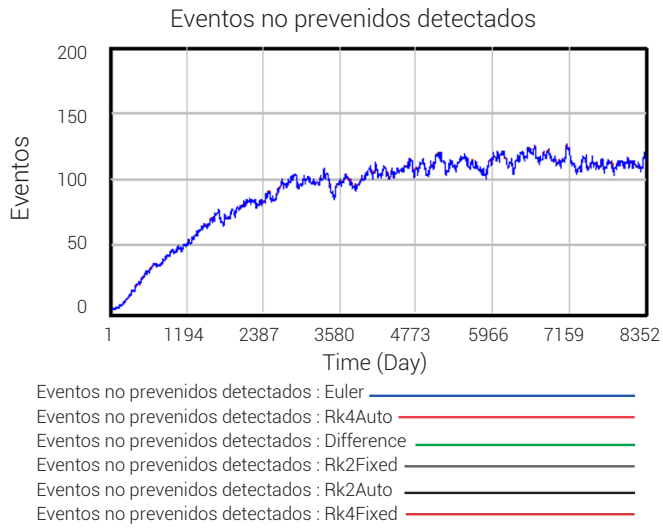


Figure 13. Integration error test.
Source: Own work

- **Sensitivity analysis:** The sensitivity analysis helps identify significant changes in the conclusions when the assumptions vary significantly [21].

The sensitivity analysis was performed under triangular distributions of the parameters that are identified in Figure 14 and with 1000 iterations.

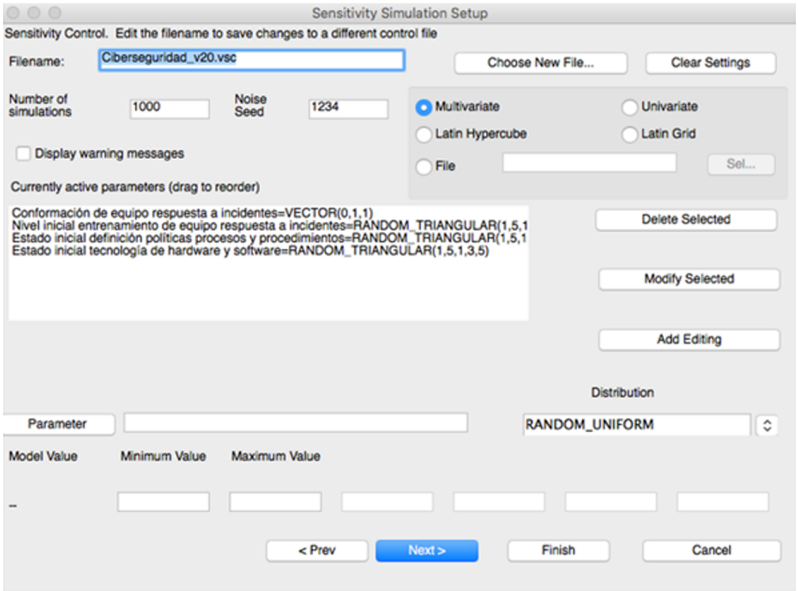


Figure 14. Definition of parameters for sensitivity analysis and their distributions
Source: own work

The results show that there is a 95 % probability that the data will behave according to the range found in the model, as shown in Figures 15, 16 and 17.

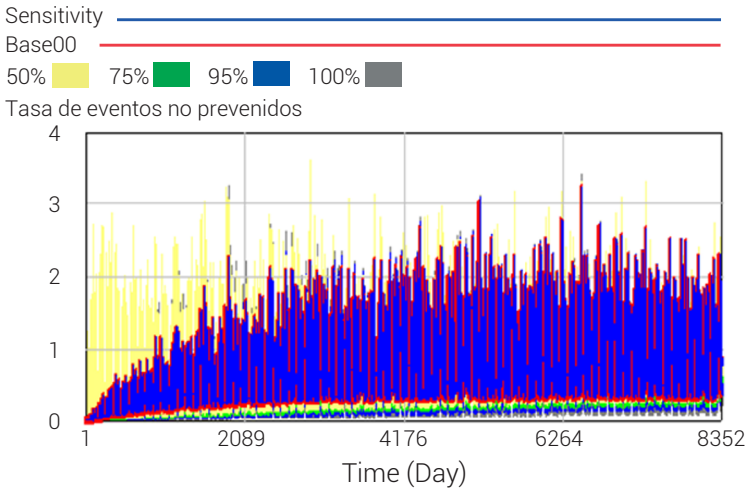


Figure 15. Sensitivity for the rate of non-prevented events.
Source: own work

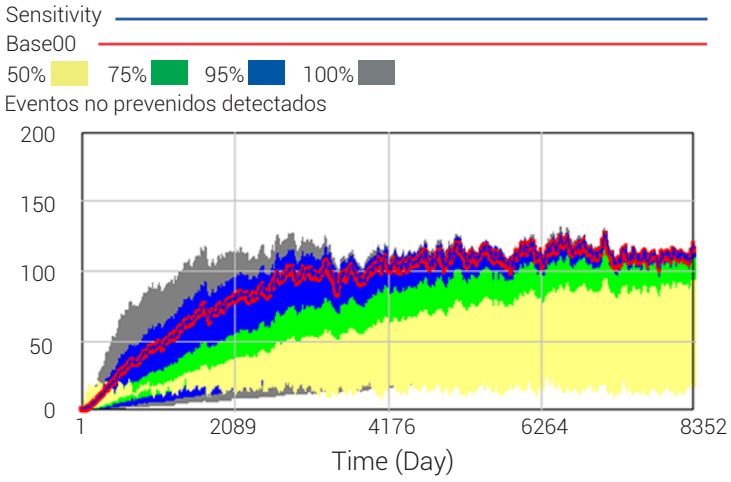


Figure 16. Sensitivity for non-prevented events that were detected
Source: own work

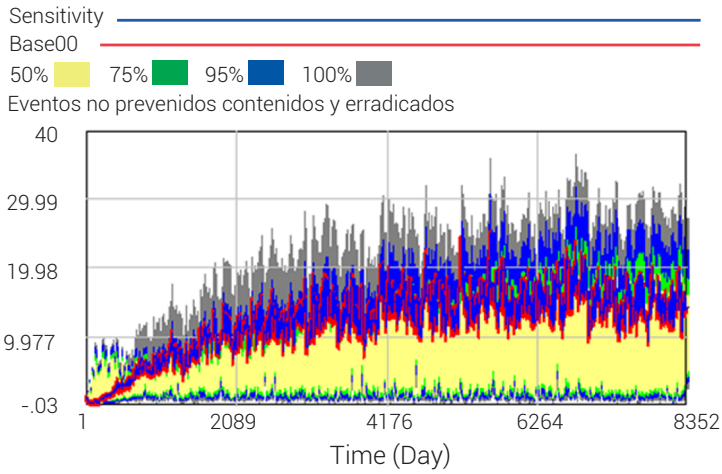
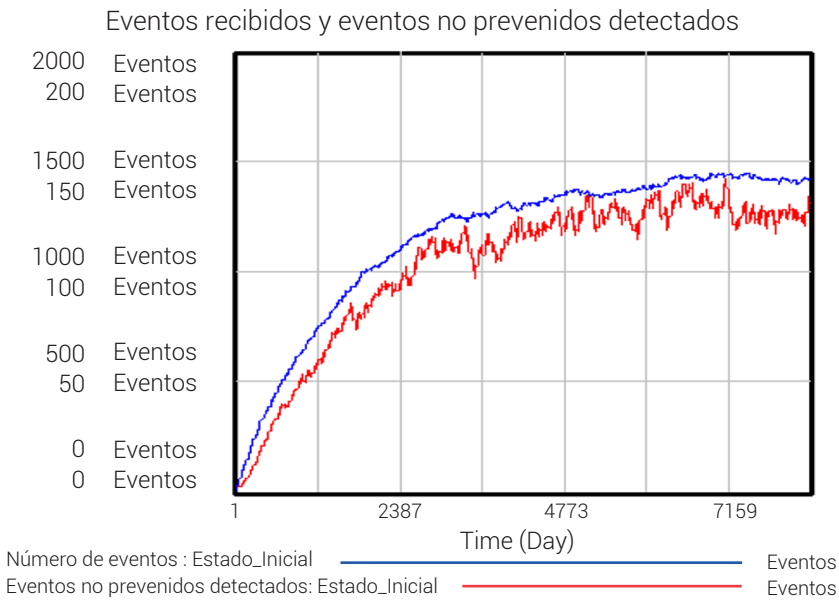


Figure 17. Sensitivity for non-prevented events that were contained and eradicated
Source: own work

The dynamics captured by the model show an increase in the number of events a company can receive under the initial conditions defined. Regarding the events, it can be concluded that they have a potential behavior, which increases the level of risk for the infrastructures of the organizations, including those critical as an unanticipated event or incident, that can compromise the continuity of the business or the CIA attributes. In this same sense, it is necessary to develop sufficient mechanisms to detect, in the shortest possible time, the incidents that may compromise the cybersecurity of the organizations. Figure 18 reflects the behavior of the system under the modeled definitions, from the events received, to those detected events or incidents that were not prevented . It is evident that the detected unforeseen events are less than the events received in the defined period.

On the other hand, unforeseen events must be contained and eradicated in the shortest time possible to reduce the impact of the natural effects that incidents produce in terms of cybersecurity. In that sense, the contained events are relatively similar to the events that are detected. However, unforeseen events involve different times of attention and containment in terms of the RTO (Recovery Time Objective) and RPO (Recovery Point Objective) and the criticality of the immersed assets, as well as the complexity of the attack, so it is not possible to have the same amount of containment and recovery of the service. This behavior can be analyzed in Figure 19.



Fiureg 18. Events received and non-prevented events.
Source: own work

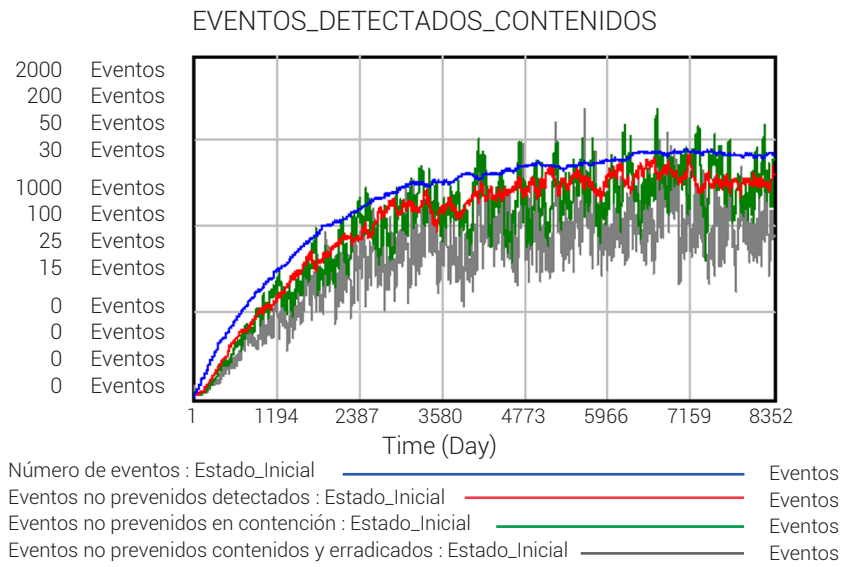


Figure 19. Events, non-prevented events, events in containment and events contained and eradicated
Source: own work

Scenarios

One of the most common tools for defining policies is the construction of scenarios. The main objective is to define the optimistic scenario and the pessimistic one regarding the parameters consigned in the model that allow for the comparison of the outputs of each of them so as to define policies that improve the solution of the problem [21].

In that sense, the model was simulated under the conditions of the pessimistic scenario and optimistic scenario that can be observed in Table 5, where it was proposed to review the behavior under unfavorable conditions or lower than the initial situation modeled and in the same way, the values of the parameters were modified to strengthen the system and analyze it from the perspective of the best scenario.

Table 5. Defining scenarios for analysis.

Parameter	Initial	Pessimist	Optimist
Initial state of hardware and software technology	2	1	4
Conformation of incidents response team	1	1	1
Initial state definition policies processes and procedures	2	1	4
Initial number of people	7	7	8
Initial level of incident response team training	3	1	4
Initial Level of organizational risk	0.47	0.57	0.37

Source: own work

Pessimistic scenario

In this scenario, the technology is assumed to have higher level of obsolescence, a lower definition of internal controls in terms of cybersecurity, understood as a lower level of policies, processes and procedures, a lower level of training and an increase in the risk level that can be determined by the complexity of the attacks. This facilitates the materialization of unforeseen events or incidents and therefore the impact of technology in general as well as critical infrastructures. Figure 20 shows the behavior of the system with the defined parameters.

e-ISSN 2357-6014 / Vol. 15, n°. 2 / mayo 2019 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

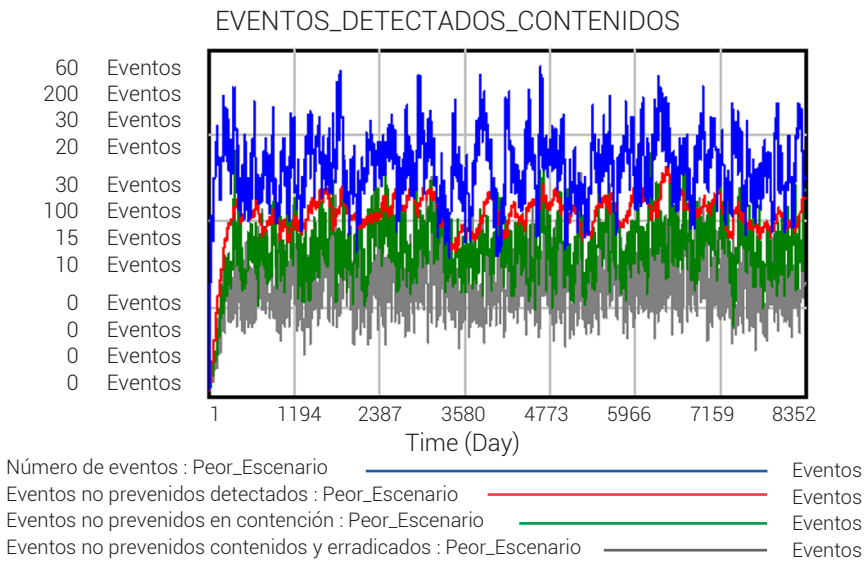


Figure 20. System behavior in the pessimistic scenario
Source: own work

The graph shows a greater number of events with a lower detection capacity and, therefore, a lower number of incidents contained and eradicated, which significantly increases the risk of loss of business continuity, as well as affecting the CIA attributes.

Optimistic scenario

Under this perspective, the detection number of unforeseen events is practically equal to the incidents that are generated, which reduces the possibility of materialization of damages to the technology, since early detection facilitates the operation or decision making for the containment of them, thus minimizing the risks derived from the attack. Figure 21 shows the behavior of the system under the given conditions.

e-ISSN 2357-6014 / Vol. 15, n°. 2 / mayo 2019 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

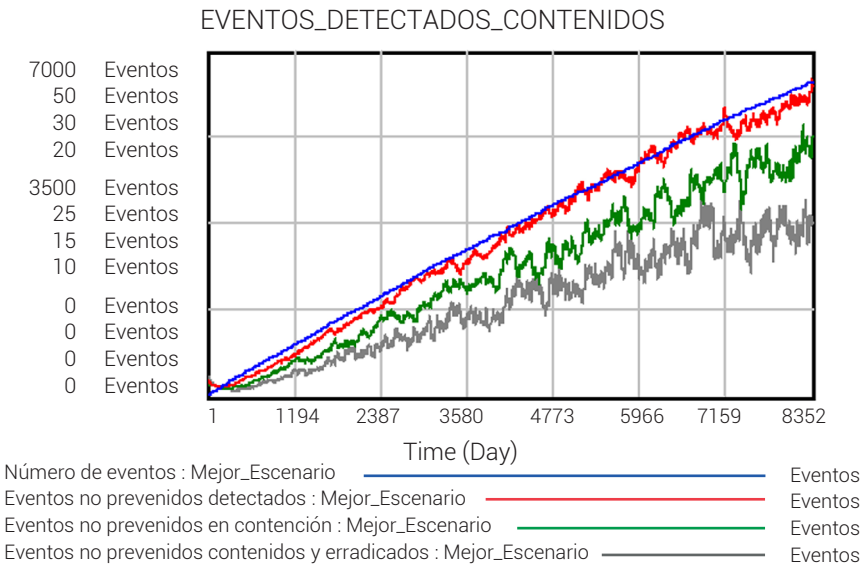


Figure 21. System behavior in the optimistic scenario
Source: own work

It is, therefore, necessary to improve the analysis, containment and recovery times of the service that allows responding to incidents that are derived from the events against the network in such a way that the risks of affecting the technology and the business in its critical infrastructures are reduced.

Optimization strategy

The Vensim's tool of "Policies Optimization ", allows for the development a non-linear multi-objective optimization [9] of the elements defined in the system. The purpose defined was to minimize the rate of non-prevented events and to maximize the rate of analyzed non-prevented events and the containment and eradication rates of non-prevented, oscillating between the parameters shown in Table 6.

Table 6. Oscillation of parameters for the optimization of the policy

Minimum	Parameter	Maximum
1	Initial state of hardware and software technology	5
0	Conformation of incident response team	1
1	Initial state definition policies processes and procedures	5
1	Initial number of people	9
1	Level of incident response team training	5
0.3	Initial Level of organizational risk	0.9

Source: own work

e-ISSN 2357-6014 / Vol. 15, n°. 2 / mayo 2019 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

The maximum values found by the algorithm used by Vensim are detailed below. Similarly, Figure 22, helps review the behavior of the system under the conditions provided by the tool. It is striking that the level of organizational risk is a fundamental element in incident response and the protection of critical infrastructures, since they define the level of action of the companies, demonstrated through investment in technology, training of personnel and the definition of policies, processes and procedures aimed at addressing the risks of affecting the business due to non-continuity of operations or alterations to information. The results of the optimization are described below:

- Initial state of hardware and software technology = 5
- Conformation of incident response team = 1
- Initial state definition policies, processes and procedures = 5
- Initial number of people = 9
- Initial level of incident response team training = 5
- Initial Organizational risk level = 0.3

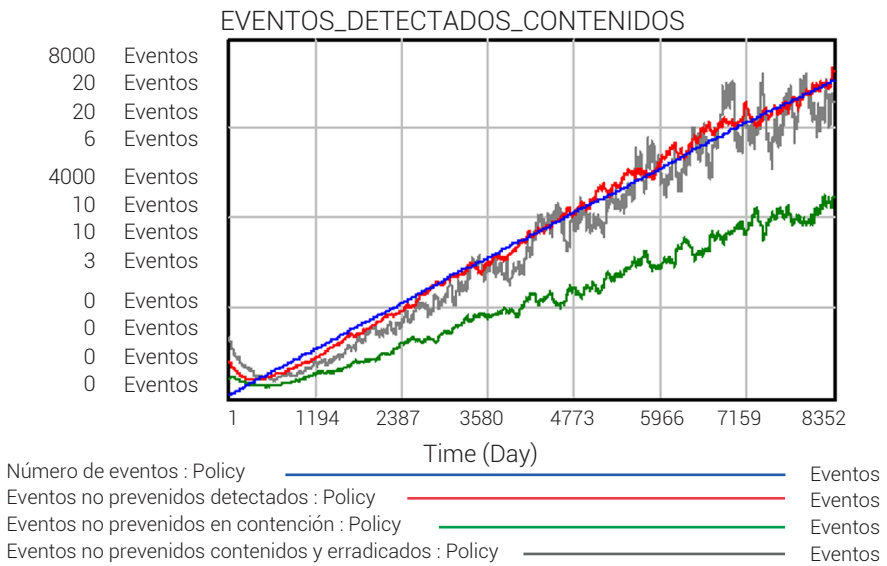


Figure 22. System behavior with optimized policy
Source: own work

Conclusions

With the above data, it is possible to conclude that the organizational risk levels represent a fundamental element for the management of incidents and the protection of critical infrastructures, since it allows for the definition of necessary strategies,

e-ISSN 2357-6014 / Vol. 15, n°. 2 / mayo 2019 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

in terms of policies, guidelines, business rules, technology and other elements that help face the threats derived from interconnectivity. In this sense, it is necessary to develop policies aimed at organizational sensitivity in terms of cybersecurity risks, to have state-of-the-art technology that allows for the early detection of unforeseen events, to strengthen business policies and guidelines, and to support a qualified and permanent team trained, so that they can deal with the complexity of the attacks to which the companies are exposed.

It is necessary then to have sufficient tools —either procedural, manual or automatic—, that allow for the evaluation of the level of exposure or risk to organizations, trying to optimize the attention times of each of the non-prevented events, thus reducing the possible effects to their technology by cybernetic attacks. That said, the protection of critical infrastructures will not only depend on preventive controls, but it is also essential to develop strategies for the early detection of incidents that allow for adequate action on behalf of the members of the organizations to attend to them.

As future work, it is proposed that the model be complemented with other elements defined in the CMM and systems excluded in this analysis, that assist in understanding cybersecurity in a holistic way and facilitate the creation of policies aimed at strengthening the security of companies and their competitiveness, measured not only individually but at the country level. Similarly, the model can be enriched by considering variables such as: the times and points of objective restoration derived from the continuity of the business and the business impact analysis, the criticality of the non-prevented event and therefore its priority of attention.

References

[1] A. Cardazzone and C. Carlini, *Understanding security policies in the Cyber warfare domain through system dynamics*, no. 1, p. 5. [Online]. Available: https://www.systemdynamics.org/assets/conferences/2014/proceed/papers/P1262.pdf

[2] Ministerio de Interior y Justicia *et al.*, *Conpes 3701 Lineamientos de Política para Ciberseguridad y Ciberdefensa,* p. 43, 2011. [Online]. Available: https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

[3] OCDE, *Directrices de la ocde para la seguridad de sistemas y redes de información,* pp. 1–12, 2002. [Online]. Available: https://www.oecd.org/sti/ieconomy/34912912.pdf

[4] R. Cort, E*stado actual de la política pública de ciberseguridad y ciberdefensa en Colombia*, no. 14, p. 4, 2015. [Online]. doi: http://dx.doi.org/10.15425/redecom.14.2015.06

[5] S. Morgan, *2017 Cybercrime Repor*t, p. 14, 2017. [Online]. Available: https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf

[6] World Economic Forum, *The global risks report 2018,* p. 6, 2018. [Online]. Available: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

[7] Ministerio de Interior y Justicia *et al.*, C*onpes 3854 - Política Nacional De Seguridad Digital*, p. 63, 2016. [Online]. Available: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

[8] D. M. Cappelli, A. Desai, A. P. Moore, T. J. Shimeall, E. A. Weaver, and B. J. Willke, "Management and Education of the Risk of Insider Threat (MERIT)," *Proc. 24th Int. Conf. Syst. Dyn. Soc.*, vol. 0389, pp. 52–53, 2006. [Online]. Available: https://apps.dtic.mil/dtic/tr/fulltext/u2/a632604.pdf

[9] E. Canzani and S. Pickl, "Cyber Epidemics: Modeling Attacker-Defender Dynamics in Critical Infrastructure Systems," in *Advances in Human Factors in Cybersecurity*, pp. 377–389. vol 501,.2016, [Online]. doir: https://doi.org/10.1007/978-3-319-41932-9_31

[10] A. Flórez, L. Serrano, U. Gómez, L. Suárez, A. Villarraga, and H. Rodríguez, "Analysis of Dynamic Complexity of the Cyber Security Ecosystem of Colombia," *Futur. Internet*, vol. 8, no. 3, p. 33, 2016. [Online]. Available: https://res.mdpi.com/futureinternet/futureinternet-08-00033/article_deploy/futureinternet-08-00033.pdf?filename=&attachment=0

[11] M. Porrúa and B. Contreras, C*iberseguridad ¿Estamos preparados en América Latina y el Caribe?*, pp. 37 - 46, 2016. [Online]. Available: https://publications.iadb.org/publications/spanish/document/Ciberseguridad-%C2%BFEstamos-preparados-en-Am%C3%A9rica-Latina-y-el-Caribe.pdf

[12] J. W. Forrester, *System Dynamics, Systems Thinking, and Soft OR,* vol. 10, no. 2, pp. 1–14, 1992. [Online]. doi: https://doi.org/10.1002/sdr.4260100211

[13] P. A. Ferrillo and C. Veltsos, "Next-Level Cybersecurity Incident Response Trends 2016.," *Corp. Gov. Advis.*, vol. 24, no. 3, pp. 6–8, 2016. [Online]. Available: https://www.dandodiary.com/2016/03/articles/cyber-liability/guest-post-next-level-cybersecurity-incident-response-trends-2016/

[14] P. Cichonski, "Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology," *NIST Spec. Publ.*, vol. 800–61, p. 79, 2012. [Online]. doi: https://doi.org/10.6028/NIST.SP.800-61r2

[15] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," *Natl. Inst. S*, pp. 1–41, 2014. [Online]. doi: https://doi.org/10.6028/NIST.CSWP.04162018

[16] K. Kossakowski, J. Allen, C. Alberts, C. Cohen, and G. Ford, R*esponding to Intrusions.*,February, p. 44, 1999. [Online]. Available: https://resources.sei.cmu.edu/asset_files/SecurityImprovementModule/1999_006_001_16679.pdf

[17] Real Options Valuation, R*isk Simulator*. 2017. [Online]. Available: https://www.software-shop.com/producto/risk-simulator

[18] T. Holdings, *Trustwave global security report*. p. 21, 2016. [Online]. Available: https://www2.trustwave.com/GSR2016.html

[19] T. Holdings, *Trustwave Global Security Report*. p. 16, 2017. [Online]. Available: https://www2.trustwave.com/2017-Trustwave-Global-Security-Report.html

[20] D. Vose, *Risk Analysis - A quantitative guide*, John Wiley & Sons, Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, England, p. 405, 2008.

[21] J. D. Sterman, *Systems Thinking and Modeling for a Complex World*. pp. 166 - 167, 2003.

[22] J. D. W. Morecroft, *Strategic modelling and business dynamics. A feedback system aproach*. pp. 55 - 57, 2015.

[23] A. García Zaballos and F. González Herranz, From Cybersecurity to Cybercrime: A Framework for Analysis and Implementation, September, p. 14, 2013. [Online]. Available: https://publications.iadb.org/publications/english/document/From-Cybersecurity-to-Cybercrime-A-Framework-for-Analysis-and-Implementation.pdf

[24] C. Young, *Information Security Science: Measuring the Vulnerability to Data Compromises*. p. 21, 2016.

[25] J. Vacca, *Cyber Security and IT Infrastructure Protection*. Steven Elliot, p. 287, 2014.

[26] D. Smith, "Forming an Incident Response Team," *Proc. FIRST Annu. Conf.*, no. January 1995, pp. 1–37, 1994. [Online]. Available: http://tech.uh.edu/conklin/IS7033Web/7033/Week11/form-irt.pdf

[27] H. Jindal, "Cyber security: Risk management," *J. Insur. Inst. India*, no. June, pp. 95–103, 2014. [Online]. Available: http://web.a.ebscohost.com.consultaremota.upb.edu.co/ehost/pdf-viewer/pdfviewer?vid=0&sid=4b2b548e-fc7e-4283-aac0-b677603fe726% 40sdc-v-sessmgr05

[28] E. Luiijf, *Cyber Crime and Cyber Terrorism Investigator's Handbook*, p. 48, 2014. [Online]. doi: https://doi.org/10.1016/B978-0-12-800743-3.00003-7

[29] A. Aguiar Rodríguez, "Understanding the dynamics of Information Security Investments. A Simulation-Based Approach," Universitetet i Bergen,Radboud Universiteit Nijmegen, p. 8, 2017. [Online]. Available: http://www.scopus.com/inward/record.url?eid=2-s2.0-67249152401&partnerID=40&md5=c9da6feaf998ef1eac82ba852ac50af8

[30] B. Akhgar and H. R. Arabnia, *Emerging Trends in ICT Security Emerging Trends in ICT Security*, p. 401, 2014. [Online]. doi: http://dx.doi.org/10.1016/B978-0-12-411474-6.00006-2

[31] A. Ahmad, J. Hadgkiss, and A. B. Ruighaver, "Incident response teams - Challenges in supporting the organisational security function," *Comput. Secur.*, vol. 31, no. 5, pp. 643–652, 2012. [Online]. doi: http://dx.doi.org/10.1016/j.cose.2012.04.001

[32] N. Adams, N. & Heard, *Data Analysis For Network Cyber-Security*, p. 36, 2014. [Online]. doi: https://doi.org/10.1142/p919

[33] S. Chabinsky, "NIST CRIED: The Four Steps of Incident Mitigation," *SecurityMagazine.com*, March, pp. 1 - 2, 2017. [Online]. Available: http://web.a.ebscohost.com.consultaremota. upb.edu.co/ehost/pdfviewer/pdfviewer?vid=0&sid=ffe0a307-b06e-43d6-b88d-d8e3269f-98c3%40sessionmgr4008

[34] D. P. Giraldo, *Análisis de la dinámica de la seguridad alimentaria en un país en desarrollo -caso colombiano-*. Tesis Doctoral, Escuela de Ingeniería. Universidad Pontificia Bolivariana, p. 114, 2013.

[35] J. F. Herrera-Cubides, P. A. Gaona-García, C. E. Montenegro-Marín, S. Sánchez-Alonso, y D. Martin-Moncunill, "Abstraction of linked data's world", Visión electrónica, vol. 13, no. 1, pp. 57-74, feb. 2019. https://doi.org/10.14483/22484728.14397

[36] C. H. Caicedo y A. Smida, "Intensidad informacional para la longitudinalidad asistencial en sistemas de salud", Visión electrónica, vol. 10, no. 1, pp. 83-95, jun. 2016. https://doi.org/10.14483/22484728.11612