Methodology for Computer Security Incident Response Teams into IoT Strategy

Alejandro Enciso Bernal[1], Sergio Mauricio Martínez Monterrubio[1,2*], Javier Parra Fuente[1], and Rubén González Crespo[1] and Elena Verdú[1]

[1] Escuela Superior de Ingeniería y Tecnología, Universidad Internacional de La Rioja
Logroño, La Rioja, Spain
[e-mail: alejoeb@gmail.com; sergiomauricio.martinez@unir.net; javier.parra@unir.net; ruben.gonzalez@unir.net; elena.verdu@unir.net]

[2] Departamento de Ingeniería del Software e Inteligencia Artificial, Universidad Complutense de Madrid
Madrid, Spain

[*]Corresponding author: Sergio Mauricio Martínez Monterrubio

Received February 24, 2021; revised March 17, 2021; accepted March 24, 2021; published May 31, 2021

Abstract

At present, the Colombian government shares information on threats or vulnerabilities in the area of cybersecurity and cyberdefense, from other government agencies or departments, on an ad-hoc basis but not in real time, with the surveillance entities of the Government of the Republic of Colombia such as the Joint Command of Cybernetic Operations (CCOCI) and the Cybernetic Emergencies Response Team of Colombia (ColCERT). This research presents the MS-CSIRT (Management System Computer Security Incident Response Teams) methodology, that is used to unify the guidelines of a CSIRT towards a joint communication command in cybersecurity for the surveillance of Information Technology (IT), Technological Operations (TO), Internet Connection Sharing (ICS) or Internet of Things (IoT) infrastructures. This methodology evaluates the level of maturity, by means of a roadmap, to establish a CSIRT as a reference framework for government entities and as a guide for the areas of information security, IT and TO to strengthen the growth of the industry 4.0. This allows the organizations to draw a line of cybersecurity policy with scope, objectives, controls, metrics, procedures and use cases for the correct coordination between ColCERT and CCOCI, as support entities in cybersecurity, and the different companies (ICS, IoT, gas and energy, mining, maritime, agro-industrial, among others) or government agencies that use this methodology.

Keywords: cybersecurity, cyberdefense, CSIRT, information security, methodology

http://doi.org/10.3837/tiis.2021.05.018 **ISSN : 1976-7277**

1. Introduction

From the creation of computer networks in the 1960s to the present day, information technologies have become more robust in information security, cyber-crooks have improved their techniques and digital threats have evolved to attack data networks. According to the "Report on Cyberthreats and Trends" of the Spanish National Cryptology Centre (CCN-CERT), which analyzes the main cyber-incidents, 38,192 security incidents were managed in 2018, being an increase of 43.65% in the number of incidents detected by this organization over the previous year [1]. The Threat Landscape Report (TLR) 2018 of the European Union Agency of Cybersecurity (ENISA) [2] indicated: a) 10% of UK health organizations have been breached more than 10 times in the last year, b) 3% of T-Mobile customer records were raped in August 2018 (that is, personal information of 2.3 million of customers), c) the cost of fraud in 2018 for the U.S. is estimated to exceed $7.4 billion, 32% growth compared to the cost in 2016, d) 38% of organizations have compromised cloud user accounts, e) 30% more phishing links were detected in social networks and f) 28% more self-reported data breaches were registered in 2017-2018 compared to the previous year from the General Data Protection Regulation (GDPR) reporting committees. The security company Symantec, in its Internet Security Threat Report (ISTR) for the year 2019, shows alarming statistics about its security products: a 56% increase in web attacks, 3.7 million blocking of FormJacking attacks on antivirus products, 33% increase in mobile ransomware, 78% increase in supply chain attacks [3].

From the above information, we can see an alarming increase in costs due to information theft and breaches, types of threats and incident management; and many corporate and government companies rely on the promise of value offered by their suppliers in the different types of information security solutions. Some have the resources to be able to have a Security Operation Centre (SOC) or Computer Security Incident Response Team (CSIRT) where they can monitor and manage their IT infrastructure focusing on information security and security incident management, but small or medium sized companies do not have the capacity to access to these resources and do not introduce the protection mechanisms needed [4]. For this reason, governments have their national Cybernetic Emergencies Response Team (CERT) or CSIRT to provide support in information security incidents to government or corporate entities for the management of cyber security and cyber defense. Also, the rise of the Internet of Things (IoT), industry 4. 0 and the critical infrastructure systems used today by large mining, gas, energy, agricultural industries, and even in our homes, is becoming more present in our day to day. Although companies are looking for methods, processes, services and technological tools to protect themselves in their Technological Operations (TO) environments, it is clear that, in recent years, cyber-attackers have evolved to focus on attacks dedicated to this industry. Recently, with the COVID-19 pandemic, we have seen cases of attacks on hospital infrastructures, affecting hundreds of patients. In 2019, KASPERSKY honeypots detected around 105 million attacks on IoT devices worldwide, a seven-fold increase over 2018. These attacks came from 276,000 IPs in the first half of 2019 versus 69,000 IPs in 2018 [5], due to the security flaws in most of these devices.

It is necessary to understand the cybersecurity and cyberdefense needs of the governments and to seek collaborative support between countries, sectors and unions. This will allow us to work in a collaborative framework, such as the peaceful alliance of the Organization of American States (OAS) for member countries synergies between the Cybernetic Emergencies Response Teams (CERTs) and CSIRTs of the governments, which can work with a unique methodology, can share information at the taxonomy level about vulnerabilities and reports to

be interconnected. This is a reference for other institutions, whether public or private, that is applied to the defense, military, financial, health, education, trade, telecommunications, and IoT Industry sectors [6]. This document develops a research of the current situation of different leading countries in cybersecurity and cyberdefense, taking the best practices of each of them, and recommendations for standards, norms and references such as ISO, NIST, MITRE, ITU, with the objective of developing and applying a methodology to unify the guidelines for the CSIRT of the Colombian Government, which is approved and promoted by the Cybernetic Emergencies Response Team of Colombia (ColCERT) and the Joint Command of Cybernetic Operations (CCOCI), to serve as a reference for other institutions. The novel integration of all these best practices and standards into this methodology makes possible, with a great work ahead, that this methodology becomes an international standard.

The rest of the paper is organized as follows: section 2 describes the state of art including an analysis of different aspects in cybersecurity and cyberdefense at the level of the Colombian Government and leading nations; section 3 indicates the general and specific objectives of this work, as well as the guidelines for the development of the Management System Computer Security Incident Response Teams (MS-CSIRT) methodology proposed in this paper; section 4 describes the steps involved in the MS-CSIRT methodology; section 5 describes the experiments conducted for the evaluation of this methodology; finally, section 6 and section 7 describe the conclusions reached after this evaluation and the future work, respectively.

2. State of Art

Different aspects in cybersecurity and cyberdefense are analyzed at the level of the Colombian Government and leading nations, where their policies, objectives or procedures are validated to implement and operate a CSIRT within a national framework of cooperation between different governments and public entities. The countries analyzed are in a collaborative framework in the North Atlantic Treaty Organization (NATO), where the NATO Cooperative Cyberdefense Centre of Excellence (CCDCOE) was created as a multinational and interdisciplinary cyberdefense center where they support member countries and promote cooperation among them by a group of experts from 25 nations. In this center they carry out research, training and exercises in four basic areas: technology, strategy, operations and law [7]. The mission is to support member countries and NATO with unique interdisciplinary expertise in the field of cyberdefense research, training and exercises, covering the focus areas of technology, strategy and law. The vision is to foster the cooperation of like-minded nations by providing a unique interdisciplinary approach to the most relevant issues in cyberdefense through the undertaken research, training and exercises. NATO defined a policy and plan of action, endorsed by the Allies at the Wales Summit in September 2014, and updated in 2017. The policy defines cyberdefense as part of the Alliance's core business of collective defense, confirms that international law applies in cyberspace, and enhances NATO's cooperation with industry. Likewise, the allies are committed to improving the exchange of information and mutual assistance to prevent, mitigate and recover from cyber-attacks. The NATO Communications and Information Agency defines the Open-Source Threat Intelligent Platform (MISP) as a malware knowledge base and web platform [8, 9], where information is exchanged within the community of members, with a concept of intelligent defense in cyberdefense as defined by NATO. Below, some strategies or visions of different countries are shown.

The National Cyber Strategy of the United States (U.S.) government aims at strengthening cyber security capabilities and securing America from the threats. It promotes that all

Americans and companies take the necessary steps to enhance national cyber security [10]. The National Security Agency of the U.S is a leader in cryptology that encompasses signal intelligence as well as information security products and services (now known as cybersecurity), and enables computer network operations to gain a decision advantage for the Nation and its allies in different situations. The Cybersecurity and Infrastructure Security Agency (CISA) is the United States' risk advisor, which works with partners to defend against threats and collaborates to build a more secure infrastructure. CISA provides comprehensive cybersecurity and infrastructure security knowledge and practices to its stakeholders, and also implements it to protect critical resources [11].

According to the president's preface of the Strategic Review of the Defense and National Security of France of 2017, "Aggressive behaviors are increasingly frequent in cyberspace, with potentially terrible consequences" [12]. In this document, the French government highlights the levels of risk: 1. Cyber-attacks have increased much during the last years, with refined tools of attack. States have contributed to these changes by using cyber-weapons that, once known, can be analyzed and reused, but also by allowing attacks to be deployed across their country; 2. The tools can cause industrial damage and even, can damage infrastructure critical to the appropriate operation of societies or states. 3. The main risks happen from the difficulty of managing the attacks and their consequences. 4. Controlling the circulation of attacks, tools and weapons, and their consequences is difficult and implies general risks. These means that actions in cyberspace can cause global effects with limited resources. Specifically, the military domain is much sensitive to such threats because of the increasing dependence on weapons or command systems of digital technologies [12].

According to the National Cybersecurity Strategy for 2019, Pedro Sánchez, President of Spain, emphasizes: "Cybersecurity protects assets, but also values that are essential for a free society like the one we are. Principles that we will not renounce in this era of global transformations. The technical challenge posed by cybersecurity is varied and complex, but we have more at stake. Something that concerns moral and cultural aspects related to our way of understanding and looking at the world, which most and best defines us. In short, freedom, well-being and democracy depend on our success in designing a good cybersecurity strategy. I am convinced that, with this document, we have taken a key step to successfully face some uncertain but also fascinating years" [13].

In 2011, the Colombian Department of National Planning (DNP), through CONPES document number 3701, is dictating the Policy Guidelines for Cybersecurity and Cyber defense, included as a priority in the National Development Plan 2010-2014 "Prosperity for All," as part of the Vive Digital Plan. These guidelines are based on the fact that the Colombian government's capacity to confront cyber threats in that year was weak, and there is no national strategy in this regard. The causes and effects that will allow the development of prevention and control policies in response to the increase in computer threats are established on this basis. For the applicability of the strategy, specific recommendations are defined to be developed by entities involved directly and indirectly in this matter, as colCERT and CCOC, these will be led under the leadership of the Ministry of National Defense in coordination with other state entities. The central problem is that the capacity to face cybernetic threats has great weaknesses and there is no appropriate inter-institutional coordination. Colombia is one of the countries that did not have a national strategy on cybersecurity and cyber defense, which includes an organizational system and a regulatory and institutional framework strong enough to meet the new challenges in aspects of cyber security where a National CSIRT or CERT has been implemented.

Likewise, the increase in the number of Internet users, the dependence of the critical national infrastructure on electronic media and the increase in incidents and crimes against cybernetic security allow the identification of vulnerabilities of the country to cybernetic threats, such as the use of the Internet for terrorist purposes, sabotage of services, espionage and theft by electronic means, among others. And with this, three problem areas were identified: the first is that cybersecurity and cyberdefense initiatives and operations are not adequately coordinated; the second is the weakness in the supply and coverage of specialized training in cybersecurity and cyberdefense; and the third is the weakness in regulation and legislation of information and data protection. From the above, the Colombian National Council of Economic and Social Policy (CONPES) defines the objectives to strength the capacities of the State to face the threats to its security and defense in the cybernetic environment (cybersecurity and cyberdefense), creating the environment and conditions necessary to provide protection in cyberspace [14]:

1. Adopt an inter-institutional framework led by the president of the republic and an inter-sectorial commission where appropriate instances will be implemented to prevent, attend, control and generate recommendations to regulate incidents and/or cybernetic emergencies to protect the critical national infrastructure. **Fig. 1** outlines the Colombia's Cybersecurity and Cyber Defense Coordination Model.
2. Design and execute specialized training plans in cybersecurity and cyberdefense.
3. Strengthen the regulatory and compliance body on the subject.

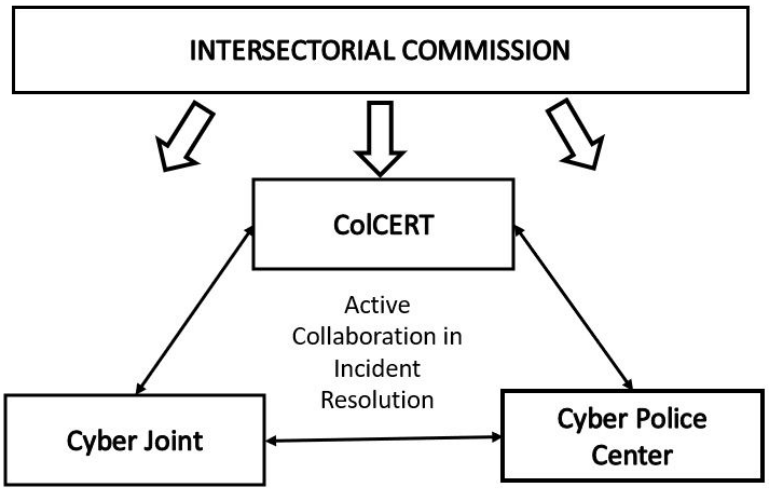

Fig. 1. Colombia's cybersecurity and cyberdefense coordination model [14].

3. Objectives and Methodology

The general objective is to create a methodology that gives the guidelines of implementation of a CSIRT for the Colombian Government, where the organizations can define policy of cybersecurity, scope, mission, vision, objectives, policies, procedures, model of maturity, controls and use cases, tools for exchange of incidents and for efficient monitoring management of incidents and vulnerabilities. To achieve this general objective, the following specific objectives have been established:

1. Identify the phases for the implementation of the methodology.
2. Create a roadmap for the implementation methodology of a CSIRT.
3. Define a maturity model for the assurance of the MS-CSIRT management.
4. Establish metrics to evaluate the level of maturity developed.
5. Understand the technical and operational needs for the CSIRTs.
6. Define CSIRT controls.
7. Determine the tools and procedures to operate a CSIRT.
8. Encourage the use of this methodology to create new CSIRTs.

The Management System of the Computer Security Incident Response Team (MS-CSIRT) allows the management and improvement of processes through the Deming Cycle [15]. This cycle is composed of four phases which are plan, do, check and act. This cycle will increase productivity in the scope defined by the organization, will eliminate repetitive processes and will improve the adaptation of processes.

The recommendations of the leading countries and the best methodological practices, as well as the guidelines for the creation of CERTs – CSIRTs are shown in **Fig. 2**. These will be the guidelines for the development of the MS-CSIRT methodology.

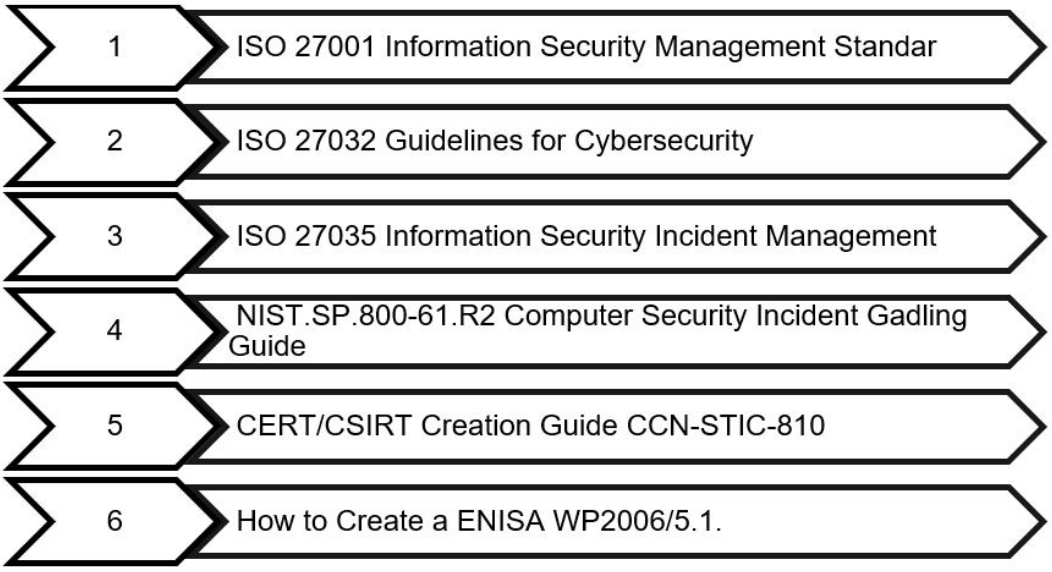

Fig. 2. Best practices for CERT - CSIRT creation.

4. Methodology Design

The steps involved in the four phases of the methodology are developed below.

4.1 Plan (MS-CSIRT)

At the beginning of this phase the organization must establish a scope for the MS-CSIRT to be the primary basis for the entire system and the context of the organizations. The scope must be approved and supported by the senior management to continue the process. The organization must already have established a policy according to ISO 27001 Information Security Management System, only then can be established the policy for a MS-CSIRT,

including the roles and responsibilities within the system and a training plan. Finally, an evaluation and assessment of the organization's risks must be developed. The definitions of the steps of the planning phase are described below.

4.1.1 Determination of the Scope of the CSIRT Management System

The MS-CSIRT must be established according to the context of the internal or external stakeholders, their needs and requirements regarding incident management must be understood [16, 17], the applicability and limits [16] of the MS-CSIRT must be defined [17], the scope must be aligned with the Information Security Management System and must be documented and available to the organization [17].

4.1.2 Senior Management Support

There must be commitment and leadership from the senior management to the management system of the IT security incident response team [17]. A policy must be established for the computer security incident response team and be aligned with ISO/IEC 27001 ISMS numeral 5.2 [17].

4.1.3 CSIRT Policy

It must be aligned with the policy of an information security management system according to ISO/IEC 27001 in paragraph 5.2 [17]. If not established, it must be mandatory as a fundamental basis of the MS-CSIRT. The senior management must establish a policy for the management system of the team of responses to information security incidents in accordance with the NIST.SP.800.61r2 [18] and ISO 27035 [16].

4.1.4 Roles and Responsibilities of the CSIRT

The senior management must establish the roles and responsibilities within the CSIRT: assign a person responsible for ensuring that the MS-CSIRT is in accordance with this methodology; inform the senior management about the performance of the MS-CSIRT [17]; form the team that will operate the CSIRT and the authority in each of them, this team will be formed by operations personnel within the CSIRT [18].

4.1.5 Education and Training Plan

The senior management and the person responsible for the CSIRT SG must ensure the necessary resources for an annual training plan for the team that is part of the CSIRT, as a minimum: design, creation, management and maintenance of a SOC and CSIRT, crisis management, active defense vs. passive defense, vulnerability analysis, exploitation of vulnerabilities, intelligent threat analysis, digital forensic analysis, incident management, red teams and blue teams, capture the flag, MISP [19], TheHIVE [20], Cortex [20], procedures, guides, playbooks, internal and external communication, cyber-drill and cyber-range tools. These are recommendations in accordance with what is indicated in numeral 5.7 Awareness and Training of ISO 27035 [16].

4.1.6 Risk Assessment

The assessment and treatment of information security risks must be evaluated based on the principles and guidelines established in ISO 31000 and ISO 27005: it must comply with the provisions of ISO 27001 ISMS of paragraph 6.1.2 Risk assessment of information security [17].

4.1.7 CSIRT Plan

It is required that the organization has a coordinated approach to respond to information security incidents, which allows to comply with a plan that meets the requirements according to the mission, size, structure and functions of the organization. This plan must have the necessary resources and management support and must contain at least [17, 18]: CSIRT policy, mission and vision of the CSIRT, objectives and strategies of the CSIRT, approval of the senior management, roles and responsibilities, training and awareness, internal and external communication plan, services offered by the CSIRT.

4.2 Do (MS-CSIRT)

According to what was indicated in the planning, in this phase the organization enters to establish everything defined in the section of planning and the operation of the CSIRT, within the steps that this phase has:

4.2.1 Risk Treatment Plan

A risk treatment plan defined by the organization in accordance with paragraph 6.1.3 Risk treatment of information security according to ISO 27001:2013 [17] is mandatory to have this risk treatment planned and implemented because it must ensure all measures to the confidentiality, integrity and availability of information against the treatment of information security incidents that the information security incident response team comes to treat.

4.2.2 Objectives of the Information Security Incident Response Team

The objectives of the MS-CSIRT should be defined as follows: they should be aligned with the CSIRT policy, should take into account the requirements of the information security incidents as indicated in numeral 4.2 Objectives of the ISO 27001:2013 [17], should be traceable and measurable, should be adjusted according to the results of the risk assessment and treatment, should be disclosed in the organization, be updated at least once a year, should indicate the resources, the responsible, completion of planning and evaluation of results as indicated in the Phase of Verification.

4.2.3 CSIRT Operation Model

The organization should establish the operation model that best suits its organizational structure and should be composed of Team models according to NIST SP.800-61r2 in numeral 2.4.1: central incident response team, distributed incident response teams or coordination team. The personnel that compose the team can be employees of the organization, partially or totally external, for this they must be verified in the plan of evaluation and treatment of risks. If it is a sectorial CSIRT, it can be confirmed by members of the organizations. The incident response team must operate in a 7x24 model, with local and remote availability, provide the minimum tools for the operation of the CSIRT for the exchange of information, advanced intelligence of threats and management of incidents.

4.2.4 Services Offered by the CSIRT

The main service of the CSIRT is the response to computer security incidents, additionally it can provide the following services: intrusion detection, digital forensic analysis, vulnerability analysis, training plans and education, advice on incident management, regulatory framework if a state entity.

4.2.5 CSIRT Communication Plan

The CSIRT must establish an internal and external communication plan, this in order to establish: the means for internal or external incident reporting; proactive exchange of information with other stakeholders in accordance with the communication plan to be established, with whom they should exchange information in case of a security incident; what kind of information to share according to whether it is classified, internal or public; policies or procedures for the exchange of information indicating the content of communication, when to communicate, to whom to communicate [17]; means for notification of the incident and action plans by the interested parties [21].

4.2.6 Information Exchange Techniques

The importance of information exchange lies in the successful management of reported incidents during the life cycle of the response to the incident, so that the organizations coordinate and support each other to jointly resolve the incident and provide feedback on relevant information about the incident [18].

4.2.7 Incident Report

Once the security incident is detected, it must be reported to the system and followed up for analysis, until closure. The use of TheHIVE platform is recommended in this methodology for the management of incident cases and give them an adequate treatment, for small organizations that cannot have this tool, they can use any other that adapts to the needs and that can follow up the incident report until its closure.

4.2.8 Incident Detection

The detection is done through precursor sources and indicators such as firewalls, IPS, IDS, Honeypots, SIEM, antivirus, etc., more information about the precursors and indicators can be found in NIST.SP.800-94 Systems and Intrusion Prevention Guide. Detection is done by the human personnel of the organization or external sources that see an anomalous behavior in the systems.

4.2.9 Evaluation of Information Security Events

It must be assessed whether the incident is real or is a false positive, and a level of criticality to prioritize should be assigned, also the impact domain (Physical or Logical) must be assessed at the level of integrity, confidentiality and availability of information [16]. The treatment of the incident can be extended according to the recommendations of NIST.SP.800.61r2 numeral 3.5 Incident management checklist and ISO 27035 numeral 7 Evaluation and Decision Phase.

4.2.10 Response to the Information Security Incident

The necessary actions must be undertaken to respond in the containment of the incident where decisions must be taken based on the incident report for which the CSIRT must: identify the assets or information systems involved in the incident, notify the appropriate groups or members for the containment of the incident, implement new security controls in the information system.

4.2.11 Recovery of the Information Security Incident

At the time of the closure of the incident, the CSIRT must restore the systems, networks, and

information services, to their normal point of operation. The CSIRT, with those responsible for the affected system, must verify that the service or network is operating normally after its restoration point, perform functional tests, document the necessary actions to secure the system, service or networks to prevent the incident from happening again, and monitor the system, service or network.

4.2.12 Digital Forensic Analysis

The CSIRT must collect evidence from the resources affected at the time of the incident or later by judicial matters. Likewise, it must have the physical or logical tools for its treatment, considering a process or digital forensic procedure, for which the organization can be based on the ISO 27037 guide for the identification, collection, acquisition and preservation of digital evidence, or on the NIST.SP.800-86 guide to integrate forensic techniques in response to incidents.

4.2.13 Post-incident Management and Lessons Learned

Post-incident management after treatment and closure of the incident must be undertaken. The CSIRT team should meet monthly to measure the performance of the own CSIRT. Recommendations on improving incident management should be made based on monthly team or post-incident reporting meetings. The processes must be improved in the organization to avoid information security incidents if required after post-incident handling.

4.3 Check (MS-CSIRT)

The MS-CSIRT must be evaluated in its performance and effectiveness with respect to the controls implemented to measure the maturity of the system in all its phases. The method of monitoring, measurement, analysis and evaluation applied is based on COBIT 2019 [22]. Therefore, the way in which the auditor, manager or internal officer of the organization can take evidence to verify the applicability of the control to be audited are: staff interviews, document review, observation. The maturity model for the evaluation of the MS-CSIRT methodology is based on the COBIT 2019 scale (6 levels).

4.3.1 Management Reviews.

The senior management should review the management system of the CSIRT at least once a year or at other defined intervals, this ensures the convenience, adequacy and effectiveness in the continuous improvement of the system [17].

4.3.2 Individual Reviews

Any member of the organization that evidences a nonconformity to the system, shall inform the responsible of the management system and the high management unit to take the corresponding corrective or preventive actions; in the individual reviews it can be done by an external person duly authorized by the senior management.

4.3.3 Technical Reviews

According to the maturity model established in COBIT 2019.

4.3.4 Internal Audit

The organization must plan the audit at least annually or in a shorter interval if decided by the senior management. The objective of the internal audit is to evaluate if the CSIRT management

system is in accordance with the requirements of this methodology, that it is complying with the requirements given by the organization and that it is implemented and maintained effectively [17].

4.4 Act (MS-CSIRT)

As part of the process in the management system of the CSIRT, the senior management unit must worry about the continuous improvement of the system to maintain it in agreement with:

4.4.1 Non-conformities

The senior management must follow up the non-conformities with the CSIRT responsible. Within the CSIRT, a responsible must be defined to follow up and correct the non-conformity, establish a date to lift the non-conformity, re-evaluate the risks and treatments if they have an impact due to the non-conformity, periodically review the non-conformity until its closure, define the criticality of the non-conformity to assign the priority of each one, and close the non-conformity once resolved.

4.4.2 Corrective and Preventive Actions

According to the evaluation of the nonconformity, the cause of the nonconformity must be eliminated, so that it does not happen again by means of causes of the nonconformity, verification if there are the same or similar conformities, possible conformities that may occur [17].

4.4.3 Continuous Improvement

The organization must continuously improve the convenience, adequacy and effectiveness of the information security management system.

5. Experimentation and Results

With the aim to evaluate the Management System methodology for Information Security Incident Response Teams described in this paper, this section describes the experiments conducted for the evaluation of the MS-CSIRT where the behavior and maturity of the model of the management system developed in this project is evaluated against a public entity that has a CSIRT but does not have a current evaluation and measurement model. This entity is of surveillance and support to external entities and critical infrastructure categorized in the CONPES 3701 of the Government of the Republic of Colombia.

5.1 Audit of the MS-CSIRT Methodology

An external audit was carried out to this public entity of the Government of the Republic of Colombia that has a CSIRT implemented, but no analysis of its maturity system has been made. The 4 phases of the methodology described in section 4 Methodology Design of the present article were analyzed in "A Plan CSIRT", "B Do CSIRT", "C Verify CSIRT" and "D Act CSIRT". The audit was carried out by means of interviews, verification of documentation and observation method for the controls indicated in each one of the phases to verify the effectiveness of the methodology to find the level of maturity of the CSIRT, and to see the strong and weak points to take the corrective measures to the nonconformities. The first phase was to assign a schedule of interviews with those responsible for the CSIRT as follows: a) Responsible for Senior Management, b) Responsible for the Computer Security Incident

Response Centre, c) Responsible for Intelligence, d) Head of Internal and External Communications, e) Responsible for Additional Services of the CSIRT, f) Responsible for Information and Communication Technologies.

It is verified that all the controls are applicable within the organization for control verification in accordance with **Fig. 3**.

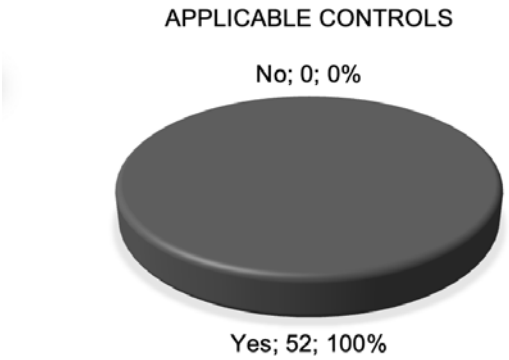

Fig. 3. MS-CSIRT applicable controls.

5.2 Analysis of the Results of the MS-CSIRT Methodology

Fig. 4 shows the percentage of compliance by phase assessed. It shows that the planning phase has a compliance of approximately 84% against some other phases that are close to 100%, so it is the first vision for the organization. The senior management and the person responsible for the CSIRT must take corrective measures and improvement to raise the level of planning, but in retrospect we see that the whole MS-CSIRT is at an optimal performance level, as shown in **Table 1**, where there are also some improvement actions in the phase of doing and checking.

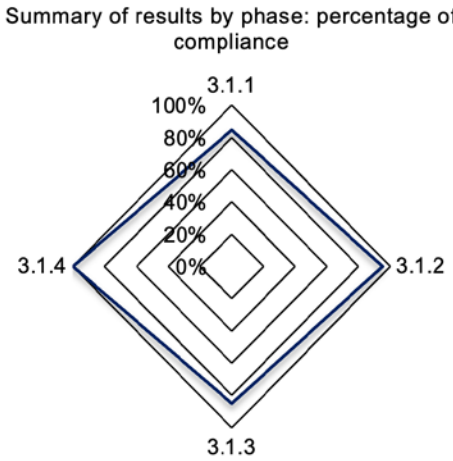

Fig. 4. Results of % compliance by phase of the MS-CSIRT.

Table 1. Results by MS-CSIRT compliance phase

MS-CSIRT implementation status results				
Summary of MS-CSIRT: 2020 results by phase	**Highest Score**	**Current score**	**Percentage**	**Maturity level**
3.1.1 CSIRT`s Plan	45	38	84%	4 - Predictable Process
3.1.2 CSIRT`s Do	140	133	95%	4 - Predictable Process
3.1.3 CSIRT`s Check	20	17	85%	5 – Optimized Process
3.1.4 CSIRT`s Act	15	15	100%	5 – Optimized Process

The senior management can take the results of **Fig. 5**, in which the percentages of compliance with MS-CSIRT controls are observed, where a high compliance with MS-CSIRT of 87% is observed throughout the system as indicated in **Table 2**. By looking at the established controls, corrective measures can be taken: assign the responsible people within the CSIRT team to follow up and close the non-conformities; define dates for the closing of the non-conformities found during the audit and thus comply with the continuous improvement of the CSIRT management system by means of an improvement plan.

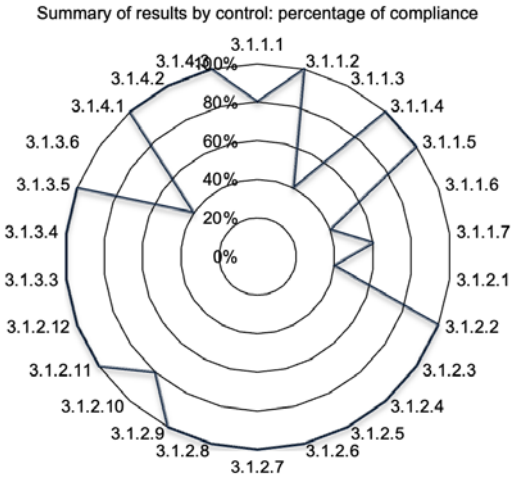

Fig. 5. Results of % compliance by phase of the MS-CSIRT.

Table 2. Results by audited control MS-CSIRT

II. Summary of MS-CSIRT :2020 results by control		**Highest Score**	**Current score**	**Percentage**	**Maturity level**
3.1.1.1	Scope of the Management System - CSIRT	5	4	80%	4 - Predictable Process
3.1.1.2	Support from Senior Management	5	5	100%	5 – Optimized Process
3.1.1.3	CSIRT Policy	10	4	40%	2 – Managed Process
3.1.1.4	Roles and Responsibilities	25	25	100%	5 – Optimized Process
3.1.1.5	Training Plan	5	5	100%	5 – Optimized Process
3.1.1.6	Risk Assessment	20	8	40%	2 – Managed Process

3.1.1.7	CSIRT Plan	10	6	60%	3 - Established Process
3.1.2.1	Risk Treatment Plan	5	2	40%	2 – Managed Process
3.1.2.2	Information Security Incident Response Team Objectives	5	5	100%	5 – Optimized Process
3.1.2.3	CSIRT operating model	35	35	100%	5 – Optimized Process
3.1.2.4	Services offered by the CSIRT	5	5	100%	5 – Optimized Process
3.1.2.5	CSIRT Communication Plan	15	15	100%	5 – Optimized Process
3.1.2.6	Information exchange techniques	15	15	100%	5 – Optimized Process
3.1.2.7	Incident detection and reporting	20	20	100%	5 – Optimized Process
3.1.2.8	Evaluation of information security events	10	10	100%	5 – Optimized Process
3.1.2.9	Information Security Incident Response	5	5	100%	5 – Optimized Process
3.1.2.10	Information Security Incident Recovery	5	4	80%	4 - Predictable Process
3.1.2.11	Digital Forensic Analysis	5	5	100%	5 – Optimized Process
3.1.2.12	Post-incident management and lessons learned.	15	15	100%	5 – Optimized Process
3.1.3.3	Management Reviews	5	5	100%	5 – Optimized Process
3.1.3.4	Individual Reviews	5	5	100%	5 – Optimized Process
3.1.3.5	Technical Reviews	5	5	100%	5 – Optimized Process
3.1.3.6	Internal Audit	5	2	40%	2 – Managed Process
3.1.4.1	Non-conformities	5	5	100%	5 – Optimized Process
3.1.4.2	Corrective and Preventive Actions	5	5	100%	5 – Optimized Process
3.1.4.3	Continuous Improvement	5	5	100%	5 – Optimized Process

Among the main findings, it was found that many processes are carried out in a way that fulfils their purpose, but there is no the necessary documentation to support such controls at the process level so there are the following nonconformities according to the findings found:

5.2.1 Scope of the CSIRT Management System

There is a global scope of the information security management system within the superior entity of this unit, but it must be extended towards the MS-CSIRT.

5.2.2 CSIRT Policy

There is an Information Security Policy that extends the scope to the CSIRT, but a specific one must be created in Cybersecurity for the CSIRT to have its own objectives and a scope that can be measured and managed. As above mentioned, the senior management must establish a policy for the management system of the team of responses to information security incidents in accordance with the NIST.SP.800.61r2 [18] and ISO 27035 [16]. Additionally it

should include: Scope of the policy where it is indicated to whom it is addressed, how it applies and the circumstances of its use, as fundamental basis of the SG-CSIRT; Policy purpose and objectives; Mission and vision; Definition of Information Security incidents; Roles and responsibilities within the CSIRT; Training plans, training and certification of those involved in the CSIRT; Classification and prioritization of information of security incidents; Performance metrics or Service Level Agreements (SLAs) Reports and Contact Forms; Annual budgets with investment plan to maintain the SG-CSIRT in all its components; Commitment of continuous improvement of the SG-CSIRT.

5.2.3 Risk Assessment and Risk Treatment Plan

Controls of ISO 27002 are adequate at the level of management of physical and logical access controls, security policies by systems, strong cryptographic controls, user management, strong perimeter security systems for the management of internal and external network services, so that the possible risks that could be evidenced in the evaluation have been addressed.

5.2.4 CSIRT Plan

This is established, but a new one is needed to align it with the present methodology at a documentary level in a CSIRT management manual that includes the scope and policy of the organization with the CSIRT, a procedure for risk assessment, treatment and acceptance, measurement and objectives of the CSIRT. With this plan a new roadmap can be defined to increase the level of compliance and maturity of the system. The plan must identify information exchange techniques, procedures and guidelines: Information security event detection and reporting, information security event assessment, information security incident response, information security incident recovery, digital forensic analysis, lessons learned, performance evaluation, continuous improvement.

5.2.5 Information Exchange Techniques

There are strong processes and procedures for ad hoc exchange of information on security incidents, however, a plan was initiated in the present methodology where the MISP platform is implemented to interconnect with own systems and generate incident reports in an automated way generating tickets or cases through TheHive and advanced malware analysis with Cortex.

5.2.6 Information Security Incident Recovery

There are techniques for system recovery through backups, but not a possible treatment in recovery by type of incident according to the taxonomies that are defined by colCERT.

5.2.7 Internal Audits

There is no an established procedure to perform internal audits within the CSIRT, but they are correcting the nonconformity, since it came from an external audit, so they are establishing a procedure to perform an annual internal audit.

Fig. 6 shows the maturity level of the entire system in its 4 phases, where we see that the maturity level of the entire system is at 91%, so improvement actions should be taken to reassess the system and make this optimized in the following years and to keep working especially in the phase of planning and doing. **Fig. 7** shows the maturity level for control where improvement actions should be taken in each control phase to raise nonconformities.

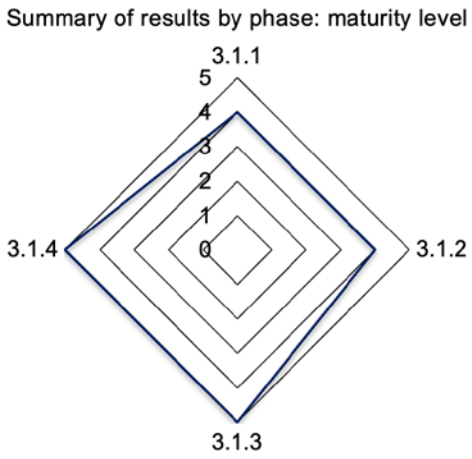

Fig. 6. Maturity level results by MS-CSIRT domain.

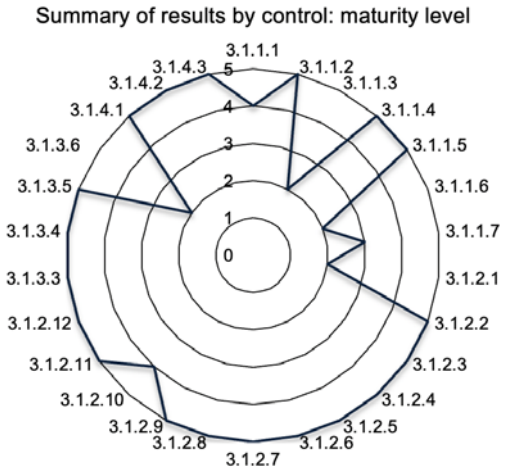

Fig. 7. Maturity level results by MS-CSIRT control.

Among the positive aspects we can observe a leadership and high commitment of the senior management in the annual resources to maintain the CSIRT at the level of technological infrastructure resources, training plans and strengthening of education of the members that belong to this CSIRT, a good platform for incident management, an optimal communications plan for the internal and external context of the organization, a system of continuous improvement by the external audits that the public entity carries out. Additionally, it has a strong service in external incident reporting that includes treatment recommendations, awareness, digital forensic analysis, ethical hacking, because external infrastructures do not offer the service of management and treatment of these incidents. Internally it offers all the mentioned services, it has an expert staff in the matter to be able to attend the CSIRT. Within the improvement actions, a CSIRT plan must be carried out in line with the present methodology, which must include a CSIRT Management Manual, including the CSIRT plan, CSIRT policy and scope, including the steps, guidelines to comply with the MS-CSIRT controls, risk assessment and treatment plan.

Currently, within the corrective actions, there is implementation and integration of the MISP, TheHive and Cortex tools, in order to improve the response, management, treatment and closure of incidents, as well as creating communities with other CSIRTs.

6. Conclusions

The Management System for Information Security Incident Response Teams (MS-CSIRT) is a methodology for organizations that have a CSIRT or CERT operating. This methodology contributes to the annual planning of the CSIRT with the necessary resources for its operation. The MS-CSIRT methodology measures the level of efficiency in the management of the system and the services offered by the CSIRTs of the organizations. The MS-CSIRT methodology also allows the evaluation of deficient points in the systems by means of management, individual and technical reviews and internal audits. The MS-CSIRT methodology, by means of the findings found, allows to obtain a trace of the four phases of this methodology that are to plan, to do, to check and to act giving fulfilment to the established controls. Likewise, the MS-CSIRT methodology develops a roadmap to raise the level of maturity of the system being analyzed by providing observations of improvement and time. The MS-CSIRT methodology indicates to senior management the steps to be taken to maintain and improve the systems by evaluating the corrective or preventive actions of the findings and obtain a continuous improvement of the systems for the operation of a CSIRT or CERT.

In order for the MS-CSIRT methodology to be successful in the cyber security framework of the Government of the Republic of Colombia, support must be provided by a) Ministry of Information and Communication Technologies, b) Ministry of National Defense, c) Colombian Computer Emergency Response Group colCERT, d) Joint Cyber Command (CCOCI) and e) Colombian Police Cyber Centre. To be implemented by government entities and those defined as critical infrastructure or private entities, for the exchange of information on information security incidents through the MISP platform, management of computer incidents with the TheHive platform and advanced intelligence on Cortex threats are recommended in order to achieve the objectives of the national government of Colombia for the strengthening of cyber security in the country according to the policies established in the CONPES 3701, 3854 and 3995. The aim is to increase the collaborative agreement between the organizations for the strengthening of the cyber security in Colombia for the structures of national government, private and civil corporations, of information technologies and of environments and devices IoT or ICS.

The effectiveness of the MS-CSIRT has been demonstrated through an audit to a public entity of the Government of Colombia that monitors the activity of national organizations and critical infrastructure ICS. Auditing the CSIRT established in that public entity, it is observed that it has a high maturity model with respect to the MS-CSIRT.

7. Future Work

Future work includes seeking support from the Government of the Republic of Colombia on behalf of the Ministry of Information Technology and Communications, Ministry of National Defense, Colombia's Cybernetic Emergency Response Group colCERT, Joint Command of Cybernetic Operations, Cybernetic Police Centre, so that this methodology is adopted and implemented by more institutions of the defense sector, public, mixed and private.

This methodology can be applied in other organizations in other countries in the region where more tests can be carried out for its consolidation, as well as continuous reviews for the improvement of the MS-CSIRT with the support of international organizations such as the OAS in its information security department of the member countries of the Pacific alliance, so that it can be replicated in the rest of the countries in the region and have a strengthening and interconnection in the digital security of Latin America.

Also, it is intended to create a future collaborative environment to create and evaluate a MS-CSIRT oriented to ICS and IoT devices, between governments, international security organizations, ICS and IOT manufacturers, and companies working in this kind of environments [4], to promote a growth in security in this branch creating exclusive taxonomies [23] and galaxies in these environments within MISP, TheHIVE and cortex.

Acknowledgement

This work has been made possible by the support of SECTEI (*Subsecretaría de Ciencia, Tecnología e Innovación de la Ciudad de México*) for the second author during his postdoctoral studies at the Universidad Complutense de Madrid.

References

[1] National Cryptologic Center – CERT, "Cyberthreats and trends 2019," CERT, Spain, 2019. [Online]. Available: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3767-ccn-cert-ia-13-19-ciberamenazas-y-tendencias-resumen-ejecutivo-2019/file.html

[2] L. Marinos and M. Lourenço, "ENISA threat landscape report 2018," European Union Agency for Cybersecurity, Greece, 2019. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

[3] Symantec Corporation, "Internet Security Threat Report," Symantec Corporation, vol. 24, 2019. [Online]. Available: https://docs.broadcom.com/doc/istr-24-2019-en

[4] M. A. López, J. M. Lombardo, M. López, C. M. Alba, S. Velasco, M. A. Braojos, and M. Fuentes-García, "Intelligent Detection and Recovery from Cyberattacks for Small and Medium-Sized Enterprises," *Int. J. Interact. Multimed. Artif. Intell.* vol. 6, no. 3, pp. 55-62, 2020. Article (CrossRef Link)

[5] D. Demeter, M. Preuss, and Y. Shmelev, "IoT: a malware story," AO Kaspersky Lab., 2020. [Online]. Available: https://securelist.com/iot-a-malware-story/94451/

[6] D. Dejene, B. Tiwari, and V. Tiwari, "TD^{2}SecIoT: temporal, data-driven and dynamic network layer based security architecture for industrial IoT," *Int. J. Interact. Multimed. Artif. Intell.*, vol. 6, no. 4, pp. 146-156, 2020. Article (CrossRef Link)

[7] CCDCOE, "Cooperative cyberdefense centre of excellence," CCDCOE, Estonia, 2020. [Online]. Available: https://ccdcoe.org/about-us/

[8] I. Burak Tolga and G. Faith-Ell, "Information Sharing Framework for Penetration Testing," NATO Coop. Cyber Defense Centre of Excellence, 2020. [Online]. Available: https://www.ccdcoe.org/uploads/2020/04/Paper_version_Final3.pdf

[9] MISP Threat Sharing, "MISP communities," MISP, 2021. [Online]. Available: https://misp.github.io/misp-website/communities

[10] White House, "National Cyber Strategy of United States of America," WH, Washington, DC, 2018. [Online]. Available: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

[11] Cybersecurity & Infrastructure Security Agency, "Cybersecurity Framework," CISA, 2020. [Online]. Available: https://us-cert.cisa.gov/resources

[12] Ministry of Defense of France, Defense and National Security, "Strategic Review of Defence and National Security 2017 Key Points," DICoD - Bureau des éditions, 2017. [Online]. Available: https://otan.delegfrance.org/2017-Strategic-Review-of-Defence-and-National-Security
[13] Ministry of the Presidency, Relations with the Courts and Equality, "National Cybersecurity Strategy," 2019. [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/information-systems-defence-and-security-frances-strategy/@@download_version/c7d0d0671bbc4756afd87513675d58eb/file_en
[14] National Planning Department, "CONPES 3701 policy guidelines for cybersecurity and cyberdefense," NPD, Colombia, 2011. [Online]. Available: https://mintic.gov.co/portal/inicio/3510:Conpes-3701-de-2011
[15] W. E. Deming, "Quality, productivity and competitiveness: the way out of the crisis," in *Proc. of Principles for Transforming Management in Western Companies*, 1st ed. Madrid, Spain: Editions Diaz de Santos S.A, pp. 62-68, 1989.
[16] *Security incident management*, IGTC-ISO/IEC 27035:2012, ICONTEC, Colombia, 2012.
[17] I*nformation technology. Security techniques. Information security management systems requirements*, NTC/ISO/IEC 27001:2013, INCOTEC, Colombia, 2013.
[18] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer security incident handling guide," National Institute of Standards and Technologies, USA, 2012. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
[19] MISP Threat Sharing, "MISP malware information sharing platform and threat sharing," MISP, 2021. [Online]. Available: https://misp.github.io/misp-website/index.html
[20] The Hive Project, "The hive and cortex," 2020. [Online]. Available: https://thehive-project.org
[21] National Cryptologic Center – CERT, "Guide to creating a CERT/CSIRT - CCN-STIC-810," CERT, 2011. [Online]. Available: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/520-ccn-stic-810-guia-de-creacion-de-cert-s.html
[22] ISACA, "COBIT 2019 Design guide and toolkit: designing an information and technology governance," ISACA, 2019. [Online]. Available: https://www.isaca.org/bookstore/bookstore-cobit_19-digital/wcb19dgd
[23] Y. Pan, J. White, D. C. Schmidt, A. Elhabashy, L. Sturm, J. Camelio, and C. Willians, "Taxonomies for reasoning about cyber-physical attacks in IoT-based manufacturing systems," *Int. J. Interact. Multimed. Artif. Intell.*, vol. 4, no. 3, pp. 45-54, 2017. Article (CrossRef Link)

Alejandro Enciso Bernal, Telecommunications Engineer from Universidad Santo Tomas de Aquino, Specialist in Industrial Cybersecurity from UNIR, Specialist in Systems Management and Information Technology from Universidad EAN and Universidad Politécnica de Madrid, Candidate to Master in Computer Security from Universidad Internacional de la Rioja. Consultant and commercial director for Latam of the consulting firm Krav Maga Hacking with experience in Cybersecurity. He has developed Honeypots and OSINT projects along with ISO 27001 projects and Ethical Hacking consultancies and CSIRTs implementation strategies based on MISP. Communication skills with executives and experience in delivering trainings in government, defense and private high-level environments. He has experience in the development of secure development methodologies and in the generation of cybersecurity strategies.

Sergio M. Martínez-Monterrubio was born in Mexico City. He received the degree in computer science and the master's degree in international business administration from the Universidad Nacional Autonoma de Mexico (UNAM), in 1998 and 2003, respectively, and the Ph.D. degree in computer science from the Instituto Tecnologico y de Estudios Superiores de Monterrey (ITESM), Mexico, in 2016. He received the Mexico's First National Prize for his thesis in computer science from ANFECA, in 1999, the Doctoral Scholarship from Conacyt, the Postdoctoral Scholarship from SECTEI, and the Doctorate Medal for his doctoral studies from ITESM Since 2017, he has been an Investigator making a Postdoctoral Research with the Department of Software Engineering and Artificial Intelligence, Universidad Complutense de Madrid (UCM), and with the Group of Artificial Intelligence Applications (GAIA), Computer Sciences Faculty and Engineering, UCM. His professional experience includes working in companies as McAfee antivirus, Oracle, Entrust Technologies, Colgate Palmolive, ABC Medical Center, and Continental Automotive Systems. He is currently the coordinator of the master's degree in computer security at the Universidad Internacional de La Rioja. His research interests include artificial intelligence, data mining, big data, computer science applied to medicine, and machine learning and its applications in cyber security.

Javier Parra Fuente is a full-time professor at the Universidad Internacional de La Rioja (UNIR). His current research interests are in software and web engineering, artificial intelligence and public administration services. He is deputy director of the international academic development department at UNIR. In addition, he is information and communications technology officer of the government of Spain. He has been professor in several universities during more than 20 years: Universidad Autónoma de Madrid, Marconi International University, Universidad Pontificia de Salamanca. He was a postdoctoral researcher at the Oxford University during 2 years and visiting professor at seven universities in Argentina, Colombia, the Dominican Republic, Mexico and Peru. Director of several university master's degrees and professor in different university doctoral, master and degree programs.

Dr. Rubén González Crespo has a PhD in Computer Science Engineering. Currently he is Vice Chancellor of Academic Affairs and Faculty from UNIR and Global Director of Engineering Schools from PROEDUCA Group. He is advisory board member for the Ministry of Education at Colombia and evaluator from the National Agency for Quality Evaluation and Accreditation of Spain (ANECA). He is member from different committees at ISO Organization. Finally, He has published more than 200 papers in indexed journals and congresses.

Elena Verdú received her master's and Ph.D. degrees in telecommunications engineering from the University of Valladolid, Spain, in 1999 and 2010, respectively. She is currently an Associate Professor at Universidad Internacional de La Rioja (UNIR) and member of the Research Group "Data Driven Science" of UNIR. For more than 15 years, she has worked on research projects at both national and European levels. She is co-author of articles published in relevant journals as "Computers & Education", "PLOS ONE", "Expert Systems with Applications", "Applied Soft Computing", "IEEE Access" or "Image and Vision Computing".