computers

MDPI

Article

Proposal for an Implementation Guide for a Computer Security Incident Response Team on a University Campus

William Villegas-Ch. [1,*], Ivan Ortiz-Garces [1] and Santiago Sánchez-Viteri [2]

[1] Escuela de Ingeniería en Tecnologías de la Información, FICA, Universidad de Las Américas, Quito 170125, Ecuador; ivan.ortiz@udla.edu.ec

[2] Departamento de Sistemas, Universidad Internacional del Ecuador, Quito 170411, Ecuador; ssanchez@uide.edu.ec

* Correspondence: william.villegas@udla.edu.ec; Tel.: +593-98-136-4068

Abstract: Currently, society is going through a health event with devastating results. In their desire to control the 2019 coronavirus disease, large organizations have turned over the execution of their activities to the use of information technology. These tools, adapted to the use of the Internet, have been presented as an effective solution to the measures implemented by the majority of nations where quarantines are generalized. However, the solution given by information technologies has several disadvantages that must be solved. The most important in this regard is with the serious security incidents that exist, where many organizations have been compromised and their data has been exposed. As a solution, this work proposes the design of a guide that allows for the implementation of a computer incident response team on a university campus. Universities are optimal environments for the generation of new technologies; they also serve as the ideal test bed for the generation of security policies and new treatments for incidents in an organization. In addition, with the implementation of the computer incident response team in a university, it is proposed to be part of a response group to any security incident at the national level.

Keywords: informatics security; cybersecurity; CSIRT

Citation: Villegas-Ch., W.; Ortiz-Garces, I.; Sánchez-Viteri, S. Proposal for an Implementation Guide for a Computer Security Incident Response Team on a University Campus. *Computers* **2021**, *10*, 102. https://doi.org/10.3390/computers10080102

Academic Editor: Grigorios E. Koulouras

Received: 22 April 2021
Accepted: 13 August 2021
Published: 19 August 2021

1. Introduction

The Internet has become a form of business in today's society, but this brings new challenges to protect our data and information from cyberattacks. According to experts, the only way to protect the web and avoid information theft is not to use the Internet at all. However, this measure is almost impossible nowadays due to the number of resources that are present on the web, as well as due to the number of activities that it allows us to carry out. A security event occurs due to the lack of security policies and techniques enjoyed by networks or applications, and the lack of security culture on the part of users. Preserving information in organizations in an interconnected computing environment is increasingly difficult. The implementation of new services and the increase in network intrusion methods put information security at risk. For this reason, the security of communication networks is a problem that affects the world's population.

Cyberattacks have become one of the main threats to countries and governments. They occur at any moment, regardless of the type of organization, be it large, medium, small or highly relevant. In 2004, the European security agency was created in order to guarantee a high level of knowledge of network and information security called "ENISA", which allowed the development of a culture of computer security in the European community [1]. In Latin America, response teams have been implemented, but the expected results have not been obtained. This is mainly due to the lack of information and importance towards this global issue, which causes great economic losses.

Several countries see it as a necessity to form computer security incident response teams (CSIRTs) that allow organizations to limit damage, tolerate attacks, and consolidate

the continuity of services [2]. Furthermore, it is a good future practice to maintain an adequate safety culture at the country level. Organizations such as educational institutions, and even more so, universities, are at constant risk due to the services they manage and provide to students. What greatly increases the means of unauthorized access to our information is that having a CSIRT helps to greatly mitigate computer attacks [3]. The scope of the response team depends on policies, requirements and high impact areas so that they can act in each field.

Several related works treat CSIRTs from one approach, where it can be structured and organized to provide a range of services in various ways. The type of services offered will be of importance in providing the type of expertise available and the type of incident handling capacity that already exists in an organization [4]. Other work focuses on environmental variables, such as constituency size and organization, available funding, and geographic distribution, and can also affect the range and level of services provided by a CSIRT. A small, centrally located organization will require a CSIRT that is different from that required by a large, geographically dispersed organization [5]. Some CSIRTs provide a full suite of services, including incident response and analysis, vulnerability management, intrusion detection, risk assessments, security consulting, and penetration testing. A variety of these full-service teams can be found in the commercial sector. Other papers look at CSIRTs that provide a smaller set of services. For example, the main service provided by some military organizations is intrusion detection, while some government organizations provide only a referral service, referring incidents to third-party equipment. Some teams act only as a central repository to collect activity from reported incidents. Others act as a central repository and disseminate any information about new vulnerabilities and intruder trends.

This work proposes a guide for the design of a CSIRT academic model that complies with international standards applied to a university. The model follows a guideline with guidelines approved and endorsed by ENISA. To do this, the initial phases established in the different models of creating a CSIRT team are developed. Considering the resources, requirements and policies are established in the university in order not to put the security of the institution at risk and preserve the integrity of the data, as well as to provide a general and practical vision of how it is executed and who coordinates the organizational part of the project. This article is organized as follows: Section 2 reviews the concepts used in this research; Section 3 describes the proposed method; Section 4 shows the results of the investigation and discusses the results obtained; and finally, Section 5 presents the conclusions.

2. Preliminary Concepts

For the development of this work, several concepts have been used that provide a guide to all the components that must be included for the design of the proposal. These concepts clarify the environment where the work is carried out; in addition, it shows the operation of each of the technologies and policies individually. In addition, it is the starting point that lays the foundation for the design of a CSIRT applied to a university.

2.1. Computer Security Threat

Threats arise from vulnerabilities, as these can be used to compromise information security [6]. Currently, the increase and new intrusion techniques in the network have exponentially increased the number of intentional attacks on an organization's network [7]. Threats are classified into two types:

- Intentional threats happen when you try to put the organization at risk. For example, the theft of information using techniques such as logical trashing that searches the garbage or trash for information that serves to cause fraud, theft and data disclosure.
- Unintentional threats are threats that do not seek to expose a vulnerability but put an organization's information at risk—for example, when natural disasters occur and the infrastructure is affected, as well as the computers that handle the data.

Information security vulnerability in companies has caused incidents and threats to increase exponentially. Therefore, the governments of the countries look for alternatives to mitigate the problems related to cybersecurity. Figure 1 shows the percentage of malware attacks by country with respect to Latin America. The data is taken from ESET, which annually produces a report in which the questions, incidents, controls, answers, and concerns of more than 2500 companies in Latin America are analyzed to determine the level of vulnerability of the countries.

Figure 1. Percentage of malware attacks by country with respect to Latin America [8].

2.2. Computer Security Vulnerabilities

A vulnerability is a weakness of a system or software, of which an attacker can take advantage of in order to violate the confidentiality, integrity, availability of information, and applications [9]. Flaws or the incorrect design of software produces vulnerabilities; however, it can also be produced by the limitations of the device or application, since, by not having an updated system, and it will be ready to suffer more attacks that are sophisticated.

2.3. Computer Security Incident Response Team

A CSIRT is a working group made up of experts in charge of computer security, through the creation of preventive, proactive, security policies. In such a way, that it manages to respond quickly and efficiently to an incident or threat, whether internal or external, reducing the impact on the organization. One of the most important functions of a CSIRT is to share the information collected from the incident with other CSIRTs; in this way it will be possible to analyze the way in which this vulnerability of the system was acted upon and how to proceed to eliminate it at its roots.

Among the functions of a CSIRT is to determine the importance of an incident, type of incident and the impact it will have on the organization. It allows for knowing the derivations of an incident while at the same time providing a more effective solution, as well as give preventive solutions, recommendations to avoid future incidents and investigate alternatives that allow solving a security requirement. It allows implementing security policies in different areas of the organization, so that they can act more efficiently in the event of an incident until they contact the information technology (IT) department. Further, it allows for communicating relevant information on security issues, security risks, alert mechanisms, threat mitigation strategies, malicious sites, etc. In this way, the user can slow down the scope of the incident and prevent it from spreading throughout the organization and create a repository with information on incidents that have occurred in the organization, to more efficiently solve the incident or threat. By relying on experience and lessons learned from past incidents, better incident management can also be employed. It allows working with external groups to solve large-scale incidents or high-risk incidents for the company, be it these providers, external CSIRTs, security groups, etc. It generates security policies, more configurations that are robust, protection measures for the network, training on security, security of critical information or incident prevention. In addition, it monitors networks, websites, email, technological equipment, social threats, political threats, and monitors technological advances to always have updated and cutting-edge technology.

Currently, CSIRTs fulfill different functions or areas in society or organizations, due to the constant growth of threats and ways of corrupting security, which is why it is necessary to know the standards, measures and functions that are applied in each sector [10]. Due to the size of the companies, it is not feasible to use an individual CSIRT, so private or public CSIRTs must be used to provide their information security services to the members that belong to their network [11]. In addition, there is a commercial CSIRT that focuses on providing its services to end customers who contract a service—for example, the Internet—and in this way it is possible to prevent abuse of rates or verify that the service offered is the one that is being received [12]. Commercial CSIRTs establish agreements for their services with their clients in exchange for financial compensation.

In military organizations, CSIRTs act in the IT area for defense purposes, thus allowing them to respond to incidents that affect the structure of the State, as are the Cyber Defense commands of each country. Government CSIRTs focus on ensuring ICT services that are provided to the population of a nation; for example, telecommunications services, in addition to caring for the well-being of citizens. This type of CSIRT is aimed at public managers and their workers. Government CSIRTs are sponsored by state organizations. According to state-run policies, it could be the case that a military CSIRT can be treated as a government CSIRT or each can be independent [13] in academic institutions, be they school, colleges, institutes, or universities. The requirements and the personnel will limit the number of services provided and will have to adjust to the policies and rules established in the Educational Unit; in this way the field on which the CSIRT will act can be determined.

3. Method

For the development of the method, several elements are considered that are established in Figure 2 and are detailed by means of a flow diagram. The diagram identifies the key points for the implementation of an academic CSIRT, and includes parameters integrated into the results in order to create a loop in each recorded event. The detail of each stage of the flow chart is detailed in the following subsections.

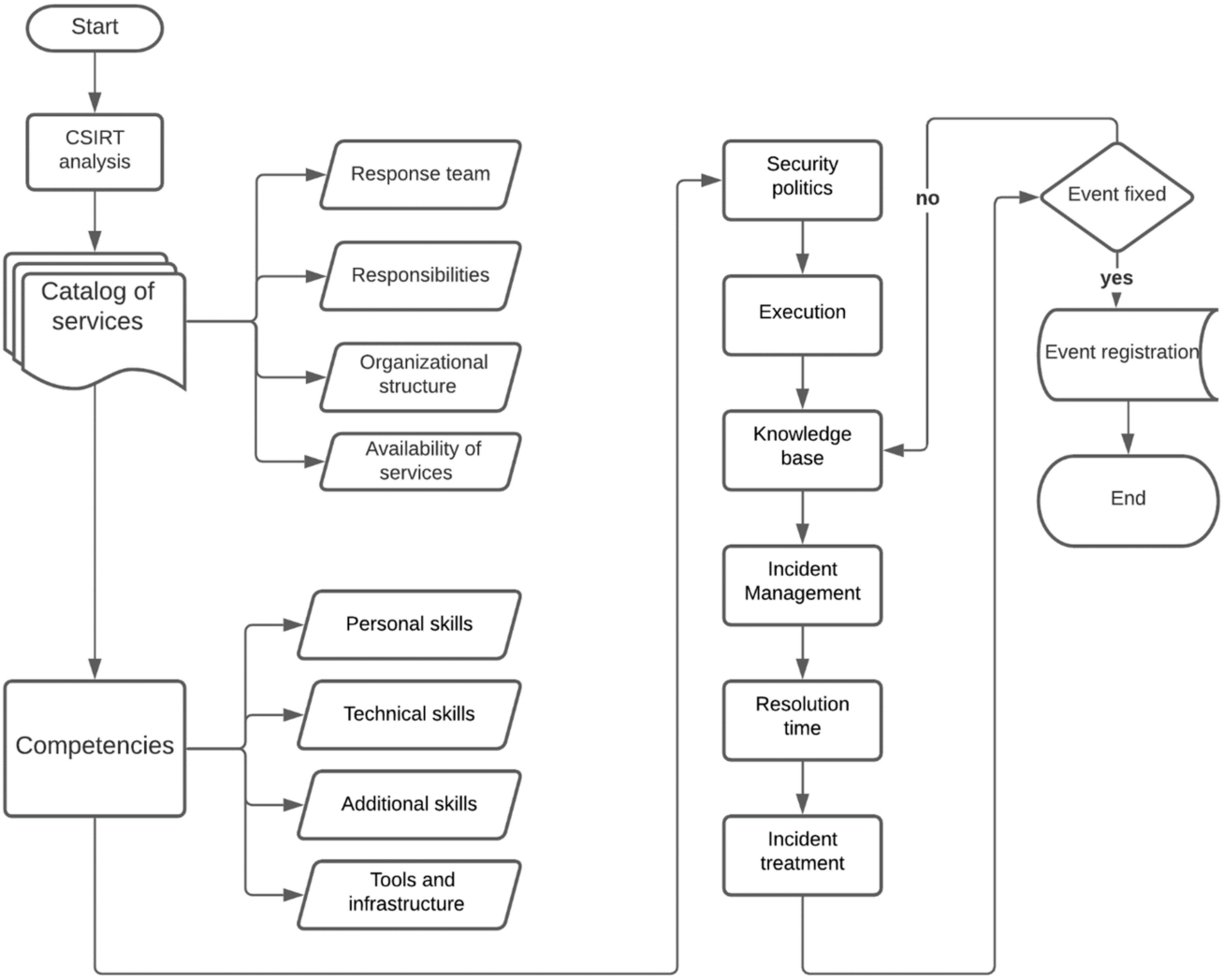

Figure 2. Flowchart of an academic CSIRT for the resolution of security events.

3.1. Analysis for the Creation of an Academic CSIRT

For the design of the guide, it is necessary to analyze the security procedures; the existing resources to mitigate an incident. In addition, the structural model that it uses is considered and the situation in which it finds itself, in addition to the university where the model is applied, is examined [14]. This analysis is used to determine positive impact areas when establishing an information incident response team. Generally, a university has a hierarchical organizational structure in which the highest academic body is the superior council or university council formed. They have a strategic management area, through which the development of the objectives and strategies proposed by the university is possible [15].

3.2. Academic Services Catalog

The high-level educational level is one of the factors that characterize universities; therefore, having a wide catalog of services helps to comply with the standards that it is desired to offer to students and staff that are part of the institution [16] in such a way that IT management and the use of updated technologies exponentially increases the risks and benefits within the institution. Table 1 shows the basic services available to universities, and they have been considered to generate the academic CSIRT. The catalog column shows the reference of the basic services that keep the different academic areas in operation. The next

column presents the final service to the user [2]. This information is relevant in the design of the CSIRT model due to the importance of establishing the implementation parameters.

Table 1. General services catalog of an IT department.

Catalogue	Service
Technical Support	
Equipment Support (Hardware)	Telephone Help
	Remote connection
	Preventive Maintenance
	Corrective maintenance
	Guarantee
	On-site support
Antivirus	Kaspersky antivirus
Utility Software	Matlab
	Office 2013
	Adobe
	Windows/MacOS/Linux/Android/iOS
	Matlab
Email	
Online services	Microsoft office 365
Technological services	
Print	Change printer toner
	Ink change
Parking	Parking ticket machine
Telephony	Telephone extensions
Connectivity	
Wifi	SSID
	Signal quality
Navigation	Blocking pages with spam, virus and insecure content
Accessibility	
Password	User lock
	Change of password
	User permits

3.3. Information Security Analysis

When designing an academic CSIRT, several obstacles must be overcome, due to the different institutional roles, among which are teachers, students, administrators, researchers, etc. who are an active part of a university [17]. In addition to having different areas or departments belonging to the campus such as cafeteria, library, classrooms, recreational areas, etc. and finally the services among which are, Office 365, Internet, telephony, etc. The use of these services and the environment where they are developed requires the use of the web, which generally causes problems that determine the total success of an IT team. In addition, they make it difficult to design methodologies, standards of use, and above all, they make it difficult to ensure the confidentiality and integrity of user information [18]. Risk assessment through technical and operational measures allows the area with a high security risk to act accurately and deeply, which leads to the management of good practices and the establishment of an excellent security policy.

3.4. Analysis of IT Requirements Oriented to Help Desk

Classrooms have become places where students can conduct discussions from any technological device that can access the network [19]. For this reason, the institutions have devoted their efforts to modernize and adapt to continuous changes in technology, and at the same time improve their management systems to offer a better service [20]. That is why the members who provide support services must seek the most practical and quick

solutions to provide an effective first level solution; these solutions are scaled to other departments.

3.5. Preparation of a CSIRT

This section describes all the tasks, activities, and services that will be necessary for a CSIRT to perform its functions. The best practices are followed for in the future, being a member of the different international CSIRTs, to share interests, as well as advice, security policies, technological contributions, and initiatives [13]. Generally, they share the same requirements to be part of or cooperate with each other; for this reason adopting these practices will make the process easier. When planning development and implementation in a university, coupling with the structure already established in the university is considered in such a way that the new proposal improves the processes, whether they are updated or simply terminated by new procedures, in order to reduce the IT security gap and offer an improved catalog of services according to the needs of the university. Within the elaboration it is necessary to establish the mission of the CSIRT; this must be punctual and clear, explaining the purpose, emphasizing the objectives and ambitions for the future [3]. A good practice is to do it in two or three lines, as the mission will not change until a few years have passed, since future goals are always established.

In addition, it is important to understand to whom the service provided is directed, to determine the needs of the organization, the critical assets that must be protected, and how they will interact with the CSIRT. These parameters are established in any report, service agreement, mission; documents that describe the function and purpose of the CSIRT for various recipients of service are presented in Table 2.

Table 2. Work sectors of a CSIRT.

Target	Area	Recipients
Academic CSIRT	Institutions, universities, educational units, etc.	Students, researchers, visitors, teachers, administrators and the university community.
Commercial CSIRT	Service provider, Internet service providers, access provider, independent providers.	Clients and organizations.
Internal CSIRT	Institutions, organizations and public or private companies.	ICT area, users and administrators.
National CSIRT	Government or state, which processes incidents outside the border limits.	The government CSIRT is sometimes referred to as the national CSIRT.
CSIRT SMEs	Small and medium businesses.	They represent the largest % of companies.

Among the services provided by a CSIRT are reactive services, among which are early warning systems, incident management, help desk, vulnerability analysis, incident response, vulnerability response, incident analysis, vulnerability management, and level 1 support [12]. Proactive services include communications, security policies, computer audits, systems maintenance, implementation of security tools, development of security tools, transmission of information, training and security consulting, and risk analysis.

3.6. Power of a Response Team to Computer Security Incidents

The power refers to the level of action of a CSIRT; that is, the limits on which it may act. This is variable, depending on the service agreement, either solely as an Incident Advisor or with the power to modify, create, and remove vulnerable or corrupted services. It is recommended that a CSIRT is only in charge of the technical aspects, and there should also be a supervisor or department head in charge of announcing the repercussions [21], as well as preventive mitigation measures to avoid similar incidents from occurring again. Users who do not fully understand the technical part will not be able to determine the level of severity of the incident; for this reason it is essential to have a good socialization with users, because they could stop reporting incidents for fear of reprisals or punishment [22].

3.7. Responsibilities

The activities that a CSIRT must carry out are defined, and they commonly carry out tasks or monitor specific services and in turn may carry out additional functions such as consultancies or interact with security forces [23]. By allowing him to act in functions outside the organization, it must be considered that there are no conflicts of interest in activities where information management can play a critical role. For national and governmental CSIRTs, these regulations are handled as policies or laws.

3.8. Organizational Structure

The classification of a CSIRT allows determining the area over which incidents are managed to generate a possible solution, for which there are five types of classifications that are presented in Figure 3. Depending on the selected organizational model, it is possible to provide different services, taking into account that the quality and level will be different from each other to determine the corresponding area; the maturity and experience of the CSIRT are taken into account [24,25].

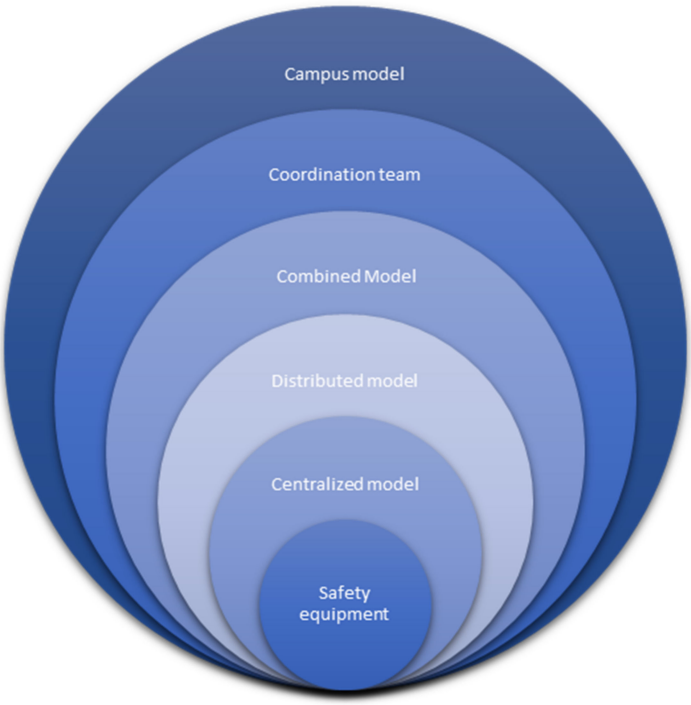

Figure 3. Models of a CSIRT.

- For a security team, formed by the absence of a formal CSIRT in the organization, the responsibilities for security incidents are assumed by the IT department and resolved as a daily activity or task. For this, it is necessary that two fundamental teams are included in the management of computer security and data protection; the Red Teams and the Blue Teams. To these teams must be added a third—the Purple Team. Red Teams and Blue Teams carry out complementary work to detect vulnerabilities, prevent cyberattacks and emulate threat scenarios. Red Teams emulate attackers, using tools to exploit security vulnerabilities in systems or applications, pivoting techniques, and organization objectives [26]. The Red Team carries out a process of emulating threat scenarios that an organization can face, analyzing security from the attackers' point of view and giving the security team (Blue Team) the possibility of defending itself in a controlled and constructive way of attacks. While the pen testers perform an intrusion process with pivoting techniques, social engineering and other hacking tests, which then ends with a report in which vulnerabilities are identified. Therefore, the Red Team is a training tool for the Blue Team, where the real

capacity is that an organization has to protect its critical assets, and its detection and response capabilities are evaluated considering both the technological, process, and human levels [27]. The main objective of the Blue Team is to carry out evaluations of the different threats that may affect organizations, monitor and recommend action plans to mitigate risks. In addition, in cases of incidents, they perform response tasks, including forensic analysis of the affected machines, traceability of attack vectors, proposing solutions and establishing detection measures for future cases. The Purple Teams exist to ensure and maximize the effectiveness of the Red and Blue Teams [28]. They do so by integrating the defensive tactics and controls of the Blue Team with the threats and vulnerabilities found by the Red Team. Ideally, it should not be a team, but rather a dynamic of cooperation between the red and blue teams. The objective of a purple team is to manage the security of the organization's assets, perform tests to verify the effectiveness of security mechanisms and procedures, and define or develop additional security controls to reduce the risk of the organization. The purple team as such makes sense in small organizations where due to constraints such as insufficient budget; they cannot support the existence of an independent Red Team and Blue Team.

- The centralized model is made up of a full-time CSIRT within the organization, which assumes all incidents related to computer security within the organization.
- Distributed model; this model must consist of at least one security manager or department head who supervises and coordinates the members who are part of it. Generally, they are members of the organization who are assigned a partial or total incident depending on the difficulty or critical level. This model is suitable for large companies in which a centralized CSIRT will not be sufficient.
- The combined model is a hybrid model between the centralized and distributed model, which has a team manager and trained members who will perform designated tasks.
- Coordination model: made up of external organizations that facilitate and coordinate the resolution of security incidents, generally assisting specific communities or organizations.
- Campus model; this model is focused on academic and research CSIRTs. Made up of several universities from different locations, making it possible for this service to spread throughout a nation. One of the main characteristics of this model is that a mother or central CSIRT coordinates it. This is in charge of communicating with the other academic CSIRTs, as well as providing information to all members that make up or use the campus model, allowing collaboration between them and in the same way reducing costs by only using the service.

In Figure 4, the structure of a CSIRT applied to a campus is presented, where several of these pass to a basic team. This, in turn, is made up of different resources—several technicians who respond to a manager [29]. These align with the media, legal advisers, a bureau chief, and an ISP abuse team.

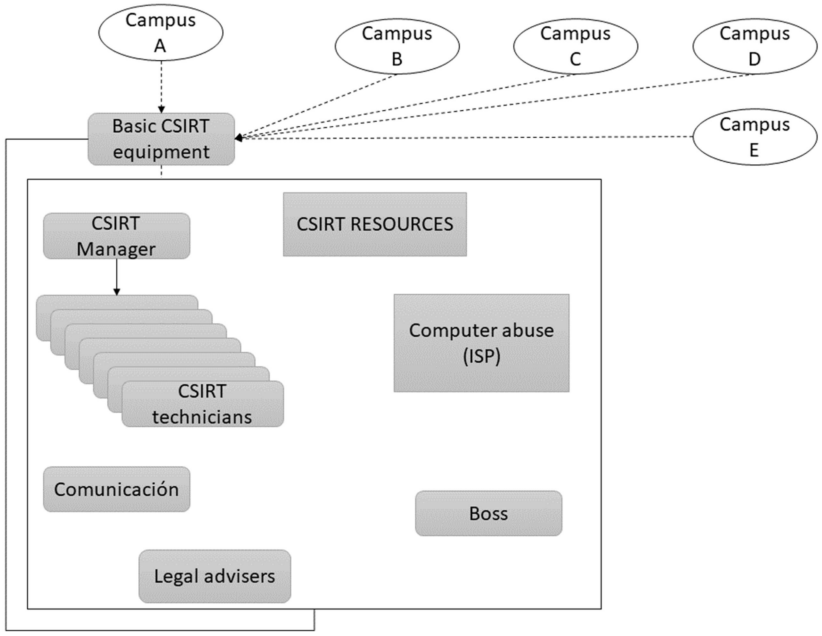

Figure 4. Campus model of a CSIRT.

3.9. Availability of Services

The availability of the services provided by a team is subject to the organization's working hours, unless a CSIRT is established 24 h, 7 days a week (24/7). It all depends on the handling of incidents; incidents reported outside office hours are generally carried out the next working day [30]. For this, a member is assigned to monitor the incident or is on duty during extraordinary hours. According to the severity (low, medium, high), measures will be taken to solve instantly, and in some cases an incident can be left on hold until the resolution of critical incidents. Having a full-time team could be beneficial, but on the contrary, it would involve an additional cost to perform these tasks.

3.10. Proposed Services When Starting

When creating a CSIRT, it is appropriate to offer one or two services while the team's capabilities are strengthened to later add more services, depending on the organization's needs. Services are specifically selected to meet the organization's needs in an optimal way [31], and adding a new service implies an additional budget with a direct impact on the available resources. In this way, it is better to offer a smaller, but high-quality catalog of services.

Reactive services allow you to respond to requests, reports and incidents that are within the jurisdiction of a CSIRT. Reactive services can also be reported by third parties, or during monitoring or alerts. Alerts and threats are focused on the dissemination of information that helps determine a malicious attack, virus, spoofing, spam, etc. Alerts are sent by systems as a means of warning or notification that something abnormal is happening on the network [32]. When an alert is detected, the CSIRTs must support mitigation or provide information to protect systems, information or recover from a system crash. Incident management allows the recovery, evaluation, solution and response to an incident of a system. It allows its correct operation and mitigation of the impact on the organization. Among the most representative activities in effective incident, management establishes mitigation strategies or ways of acting in the face of an alert or threat in order to reduce the impact of an incident. By constantly monitoring the network, a possible threat is identified early [33], filtering network traffic, executing updates and maintenance periodically. Have alternative mitigation strategies and the creation of security policies. Incident analysis refers to the description of all the information, evidence, and devices

used in mitigating a computer security request, incident, or problem. Carrying out this task helps to identify the scope of the incident, as well as the nature of the incident and the damages caused to the organization, whether financial or material. A CSIRT uses this collection of information to carry out mitigation strategies and a complete report of what happened during the computer attack, in addition to making comparisons that allow determining trends, patterns and guidelines to limit and avoid similar attacks [32], sharing information with other CSIRTs and thereby generate greater understanding of these threats. In an immediate local response, you must act on an incident by analyzing the affected systems in person, so that if a recovery of the information or the system is necessary, it is carried out as quickly as possible. If a CISRT is at another location or carrying out another activity, they must immediately go to the site and respond to the incident. In most cases, the CSIRTs are at the location and proceed to provide the corresponding support, assuming these incidents are normal functions of their work. For incident response, a CSIRT assists in recovery from an attack via telephone, remotely, email, or through documentation that helps resolve an incident. To do this, it interprets the information collected by the user and provides a simple and effective solution [34]. The response to incidents does not refer to a local response as mentioned above; in this case, remote solutions must be provided so that the user or personnel who are on the site can solve the problem.

Proactive services are designed to provide information or support in a preventive way, mostly improving the infrastructure and incident management. One of the main objectives is to reduce the number of incidents and their severity. Components such as advertisements are presented in proactive services [35]. These are notifications that allow increasing incident mitigation mechanisms, by providing the possibility of sending warnings and notices of system vulnerabilities. In such, a way that users are aware of new security incidents applied by intruders or hackers. In addition to the impact, they cause and how it allows you to prevent problems in your systems before they occur. The audits and evolution of the systems allow a detailed analysis of a security infrastructure, and determine compliance with the standards and policies of an organization [36]. There are different types of information systems audits; among these are web page audits, review of equipment configurations or updates to operating systems. In addition, the review of security policies, tests of attacks in order to determine the vulnerability of the systems, auditing of the coding of the applications, forensic analysis and configuration and maintenance of the systems. By implementing proactive services, the configuration of a system is properly applied, providing the user with the necessary tools, applications, services and the IT infrastructure. This service is used as part of their daily functions. A CSIRT is in the ability to scale the service up to incident management to avoid the vulnerability of a system. Some configuration and maintenance services include network monitoring, firewall, authentication mechanisms, server maintenance and configuration, hardware, telephony, VPNs, and security tools [37]. It includes the requirements and requests of a CSIRT; this may include the development of patches that allow avoiding a vulnerability in a system, tools that facilitate network-monitoring, installation of antivirus, attack detection devices, etc. In this way, an incident is identified early, or determined if it is possible to eliminate it before its level of danger increases.

3.11. Personnel Requirements

There are no clear studies of a recommended minimum of people to form a CSIRT because each team works in different environments, as well as their policies and standards. However, taking the expert community in the area as a reference, when offering at least two services, a minimum of four full-time trained people must be available [32]. CSIRTs that work full-time and offer the entire catalog of services must have a minimum of six to eight full-time members. If you want to provide a 24/7 service, you must have a staff of twelve workers performing three daily shifts divided into groups; these statistics include vacations and sick leave.

3.12. Competencies

For the development and implementation of a CSIRT, it is necessary to establish the necessary competencies for its proper functioning; the competencies to be considered are described in this section [5].

3.12.1. Personal Skills

The minimum expected competencies are:

- Ability to express a technical problem in simple words for the understanding of the user.
- Be analytical.
- Be trustworthy.
- Fast learning.
- Have labor flexibility.
- Sociable.
- To be organized.
- Be communicative.

3.12.2. Technical Skills

Technical skills include:

- Technological knowledge.
- Knowledge of different operating systems.
- Have extensive knowledge of networks, as well as their components.
- Have a high knowledge of computer security.
- Knowledge about risk assessment.
- Application knowledge.

3.12.3. Additional Skills

- Level of education according to the functions to be performed.
- Experience dealing with computer security issues.
- Having the time to make trips, sometimes face-to-face support will be necessary to solve an incident.

3.13. Training

The training can be carried out internally for new members in the organization in order to know the functioning and mode of operation of the CSIRT applied in the company [38]. In the same way, external training can be carried out periodically to learn about new technologies, and in this way increase the catalog of services, learn new mechanisms for resolving incidents, improving skills, making decisions, etc. Listed below are certain organizations that periodically offer training in the area:

- FIRST
- CERT/CC
- SANS institute
- TRANSITS

3.14. Tools and Infrastructure

Infrastructure refers to all software and hardware on which the organization's services run. Great care must be taken when designing and implementing the networks, telecommunications and facilities over which a CSIRT will operate, due to the confidential information of the company that is managed [39]. In addition, safety must be protected by providing a work environment according to the functions to be carried out.

- Physical structure

It is necessary to implement a security room in which any server that stores information or collects information will be placed. Security operations centers (SoCs) are also often established [40]. In addition, it is necessary to use soundproof rooms, avoiding the leakage of information in the discussions and activities of the CSIRTs, as well as tools that allow the total elimination of information, which is no longer necessary. Also, secure areas to store non-digitized information. In addition, dedicated areas only for operations must have some additional security [41].

- Specific include:
    - Ticket systems to enter an incident digitally.
    - Tools for forensic analysis.
    - Security tools (antivirus).
    - Secure communication mechanisms.
    - Alarm system.
    - Surveillance systems.
    - Information backup systems, to bring a system online as soon as possible.
    - Network intended for CSIRT operations.

3.15. Analysis of Security Procedures

The analysis of the security procedure is aligned with the handling of incidents, for which a flow diagram has been designed in Figure 5. Each stage of the analysis seeks to respond to the security events recorded in a SCIRT. The process begins with the incident report, which is carried out by means of reports that come from various sources such as web forms, e-mail, social networks or observations of those in charge of the SCIRT. In the notification of incidents, it is necessary to implement a notification backup system, avoiding points of failure in the incident report.

Notifications are registered in a ticket; each ticket has a unique number that is used during the communication of the entire incident [42]. In addition, this allows all incidents to be managed from one place in the CSIRT, even if the actual resolution of the incident is elsewhere. This prevents additional notifications from being related to an existing ticket. Once the incident is registered, it goes to triage, which is one of the most important steps in the incident handling process, since this is the point where critical decisions are made, for which verification of the incident is needed, where it is possible to ask several questions that identify the veracity of the incident; for example, "Is this really an incident?" and "How reliable is the source from which the report came?" Once it has been established that an incident is indeed occurring, we proceed with questions such as, "Is this incident within the scope of the CSIRT? Does it belong to the target community, and is the CSIRT responsible for this type of incident? What is the impact? Is there possible collateral damage?" Once the incident is identified, a response is given to the notifier where the receipt of the report is confirmed, it is explained how the processing will be carried out and what to expect, and it is suggested what to do in the meantime, until the incident is resolved.

For the resolution of incidents, the process begins with data analysis that seeks to obtain the greatest amount of information to have a more complete view of the incident. For this, the data of the reports and the environment of the affected system are considered. Several repositories must be integrated as data sources, among which are the logs of the routers, proxies, DHCP and the services available in the organization. These sources store data related to incidents; however, third-party sources can be added to the analysis in order to provide an effective response to all incidents. The next phase investigates similar solutions; this consists of finding the best solution from a set of possible solutions, based on the information gathered from the previous phase. It can be achieved by thinking or talking about the observations and conclusions obtained, or by comparing the configuration characteristics of already-known systems or installations. In the action proposal phase, dependence on the complexity of the incident is sought [1], for which one or more actions may be required to mitigate the incident. To this end, it is necessary to keep the audience as the main element when proposing actions. For example, technicians will understand

technical solutions, but if the acquisition of additional services or a financially costly measure is required, it is suggested to adjust the language so that management or financier can understand it.

The next stage verifies the action taken, for which it is necessary to answer several questions such as, "Is the target of the attack achievable, as it is supposed to be? Did the action really solve the problem?" If the target of the attack is still vulnerable, the proposed solution does not fully resolve the incident. Therefore, the system repeats the previous steps to find other solutions. Once the incident has been resolved, the system is cleaned up and returns to production. Some actions may require more time after the incident has been resolved. For example, a criminal investigation could proceed. Also, if other departments have been involved in the incident, make sure they have the information to update their communications. To close the incident, there must be a very clear policy of how and when it can go into a closed state [43]. The length of time an incident remains open can be used as a performance metric; some teams choose to never close incidents, while others decide that an incident can be closed when it is technically resolved, and various teams will close the incident only after action has been taken in follow-up.

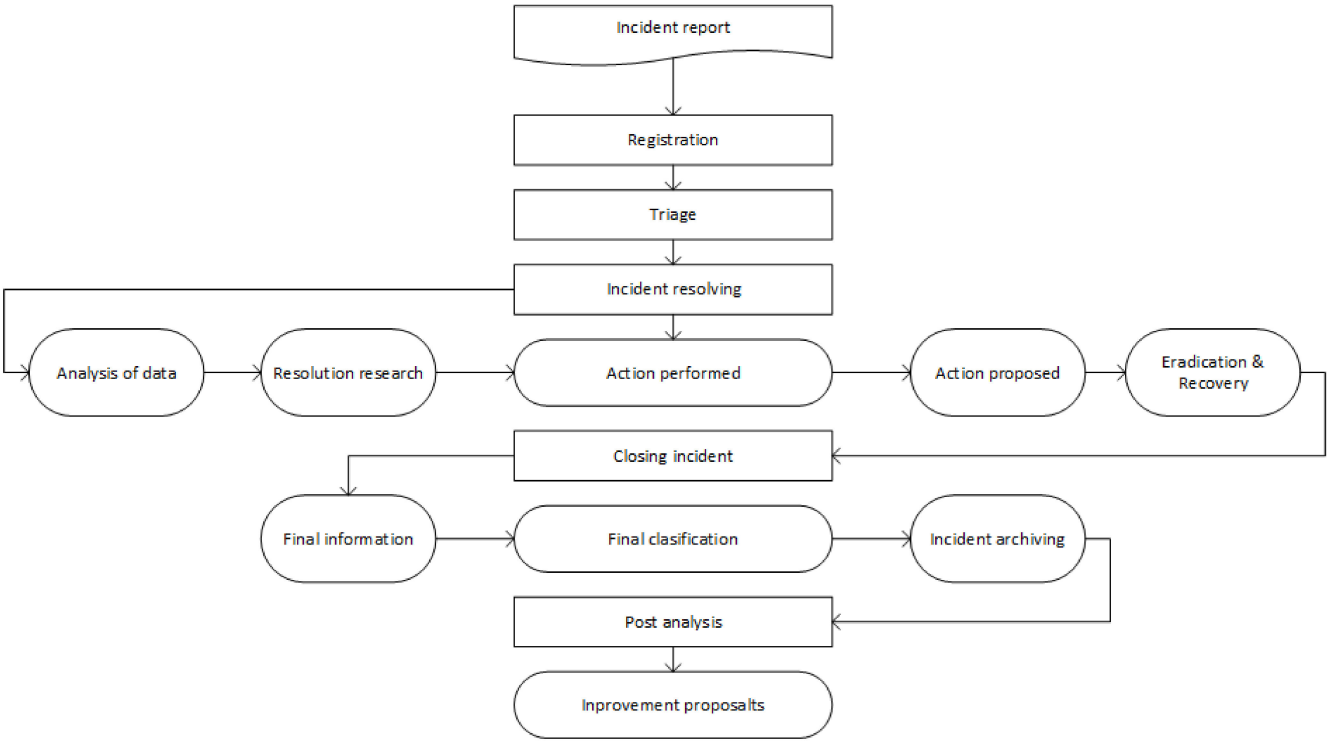

Figure 5. Workflow for Safety Procedures Analysis [44].

In the final information stage, it is important to ensure that all supporting documentation is included in the ticket. At this stage, stakeholders are informed about the status of the incident. It should contain a brief description of what happened, the outcome of the mitigation work, findings, and recommendations. In the final classification, all the information about the incident is available; for this, it is a good practice to verify, correct and classify the information. If the original classification was very different from what we currently know, the triage function can benefit from additional information to improve the classification [5]. Once the information is classified, the incident can be closed and filed. It is suggested that closed tickets remain accessible to the team through a searchable system. Similar incidents can happen again and being able to review the steps taken in similar incidents can save an enormous amount of time. In post-analysis, several things can be

learned from an incident, in order to prevent them from happening again in the future or to mitigate them quickly.

4. Results

The results analyze the information security procedures used by the University participating in this study, as well as the existing resources to mitigate an incident. In addition, the structural model used, and the current situation of the university are studied to determine the areas with the greatest impact by establishing a response team for information incidents. The guide is adjusted to the resources and the structural organization of the university participating in this study, taking as a reference each detailed section of the method [43]. This guide was applied at the university participating in the study, with the aim of offering a better service to users, as well as being part of the CSIRT community in Ecuador.

4.1. Planification

When planning the development and implementation of an academic CSIRT, there are parameters to consider such as the coupling of this on the structure of the university, in such a way that the proposal improves the processes, whether they are updated or new, in order to reduce the IT security gap and offer an improved catalog of services according to the needs of the university.

4.2. Application of the ISO/IEC 27002 Standard

Through the application of the different standards, it is possible to recommend the best information security practices preserving the confidentiality and integrity of the data in any university, for which the ISO / IEC 27002 security standard is taken as a reference, and where a series of guidelines is defined to apply and manage controls, taking into account the risk analysis within the university [45]. Table 3 shows the domains and their characteristics that are considered in the university's risk analysis, aligned to ISO 27002.

Table 3. Definitions and abbreviations ISO 27002.

Domain	Domain Characteristic
Control objectives	Number of control targets
Controls	Number of controls per objective
Description	Defining the target grouped in a domain
ID	Importance of the domain
CC	Control compliance
IC	Importance of control
Scale	Control compliance scale

4.3. Concerned Parties

The catalog of services provided by the academic-CSIRT is intended for the entire university community, which includes students, teachers, administrative staff, researchers and visitors [2]. In addition, it covers all the headquarters if there are branches, and in this way be part of the academic CSIRT community in Ecuador.

4.4. Services Provided

From the data obtained during the analysis of incidents of the university participating in this study, an average of incidents oriented to the help desk was determined as shown in Figure 6. When considering the degree of difficulty of some incidents, a diagram was developed flow that allows analyzing the process by which an incident must be dealt with from its initial stage or incident recording, until its closure. Good incident management must be in place to determine the area, over which the incident will be resolved in the optimal and efficient way.

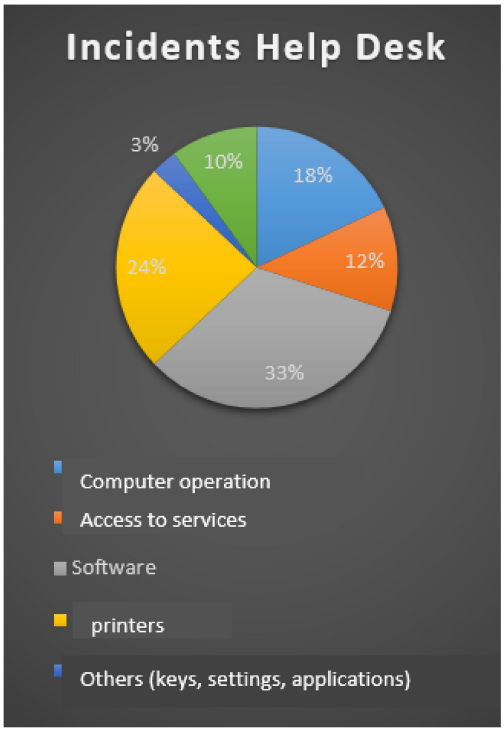

Figure 6. Incidents reported in the period 2020.

In Figure 7, the procedure for closing an incident is presented, in which the initial phase is the user's request, who, in turn, records the incident manually or digitally. The level one support team determines the area to which the incident will be assigned; at this point, the level one member must verify similarities with previous incidents using tools such as the knowledge base. This database collects information from past incidents, and if there is a similar case, the solution is applied and the incident is closed. If the solution is not effective, the resolution of the incident or requirement is reassigned with a ticket to level two personnel successively until the incident is finished and closed.

4.5. Organizational Structure

In this work, the coordinating team structural model is used because generally the universities of Ecuador have several headquarters. In this case, the university that participates in the study has three campuses distributed throughout the city of Quito. This model allows having a coordinator in charge of the incident response centers, who interacts directly with the departments distributed in each headquarters. The main function of this model is to coordinate the optimal resolution of incidents, as well as the interaction with the other areas, to obtain an analysis by sectors and a global one. When choosing a model, you should consider the services to be provided, since certain structural models do not allow fully meeting certain requirements. In this work, being developed in a large organization and with a high rate of requirements, it is possible to implement this model without problems. Figure 8 shows the distribution of each area and element of the organizational structure.

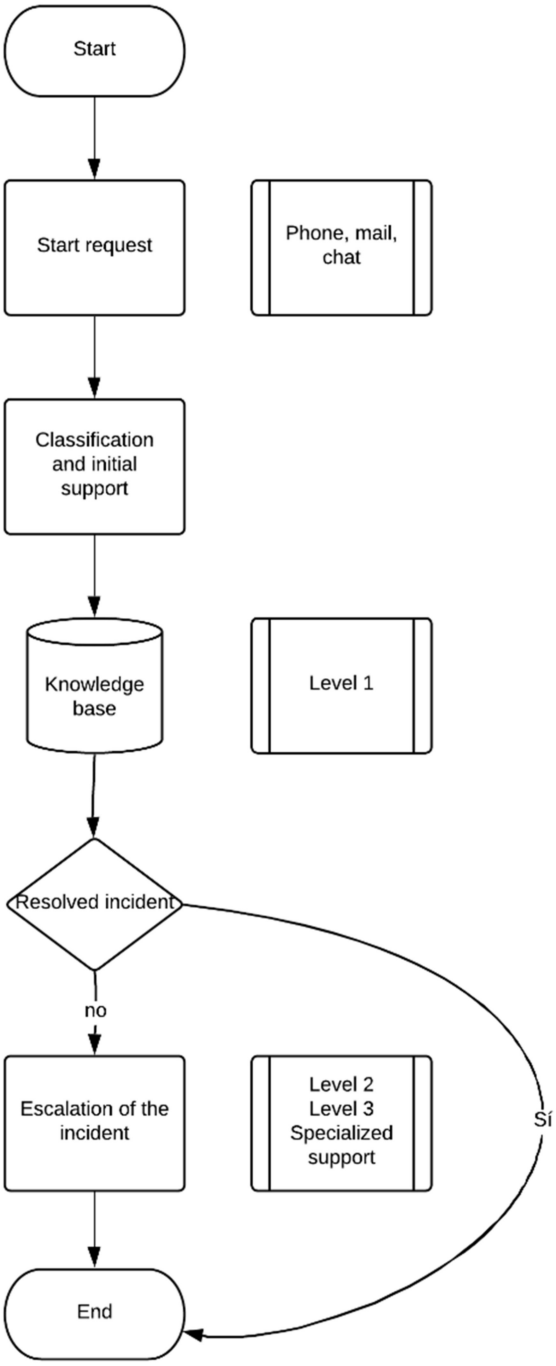

Figure 7. Process for handling an incident.

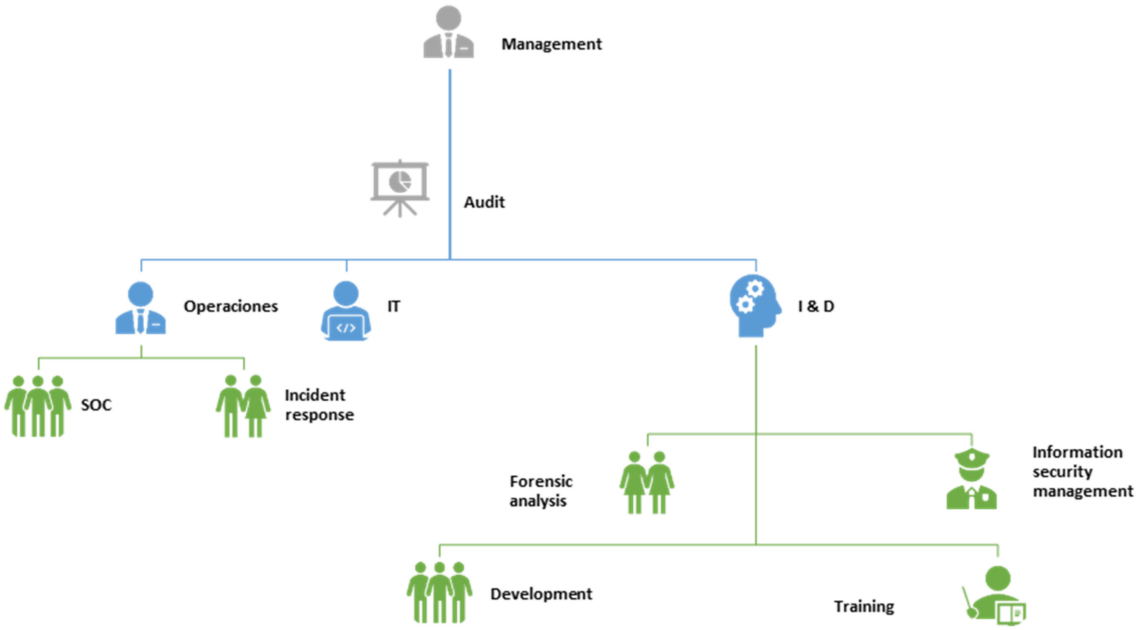

Figure 8. Process for handling an incident.

4.6. Security Politics

4.6.1. IT Responsibilities in Hardware Infrastructure

Responsibilities of the IT department, when acquiring, installing, maintaining and operating the organization's equipment, as well as:

- Check the specifications of the equipment purchased with those established in the purchase contract. If you do not meet this condition, the device must be returned immediately.
- Manage preventive technical maintenance of the devices used in the organization, together with the supplier.
- Conduct training on the correct use of installed devices and programs.
- In charge of installing the devices and programs, as well as verifying the correct location of the device in the workplace.
- Verify the physical area where the device will be installed is optimal and has electrical power, structured wiring, temperature, etc.

4.6.2. Policies for Hardware Infrastructure Users

The rules that users must comply with when using devices provided by the organization are, the equipment provided by the organization will only be used to perform tasks within the company and not for personal purposes. Requests for equipment repair that are not provided by the organization will not be received.

4.6.3. IT Responsibilities in Software Infrastructure

The IT department is in charge of monitoring applications and systems, in order to keep them updated to their latest version. In addition, certain IT-specific functions are disclosed.

- Inventory of applications and programs installed on devices, making sure that they all have valid licenses.
- Determine if the device is active or in operation and in the same way those that are not active.
- Responsible for the storage of computer programs.

4.6.4. Responsibilities of Software Infrastructure Users

Users must specifically comply with the following rules:

- Prohibition of downloading and installing software that poses a threat to the organization.
- Denied the entry of storage devices that were not provided by the organization.
- It is forbidden to alter the antivirus functions, as well as to deactivate or uninstall it.

4.7. Execution

Building relationships with other academic CSIRTs will allow the university to become part of a community of response teams nationwide. In order to seek support in new policies, treatment of new incidents and in the same way support in the resolution of more complex incidents that have a higher level of impact on organizations. By joining a security group, it is possible to exchange information, training, technological contributions, recommendations, security policies, etc.

For this, it is necessary to reach a high level of maturity with respect to information security, as well as incident and infrastructure management. When communicating between CSIRTs, a mechanism or service should be considered that allows ensuring the privacy of communications, so it is recommended to use tools such as privacy such as pretty good privacy (PGP) or GNU privacy guard (abbreviated as GnuPG or GPG), which basically perform the same function of encrypting Internet traffic through public key cryptography [46].

4.8. Knowledge Base

A knowledge base must be developed and used, in which the resolved incidents are recorded, as well as the method that was used to solve them, so that CSIRT members can access and discuss best practices and effective solutions to similar incidents [47]. The knowledge bases are also intended to house information such as user manuals, articles, and advertisements, among others. It is important to use this tool because the information can be shared with the community.

4.9. Incident Management

Incidents are classified according to the ISO 27001 standard, which establishes the impact and urgency of a requirement. By making a relationship between these parameters, it is possible to determine the priority of each incident. In this way, it is possible to resolve an incident properly, considering the current and future impact that postponing or immediately resolving the requirement will have. Table 4 shows incidents with a high critical level are marked in red, while the medium level indicates incidents that are not urgent but require attention and are marked in yellow. The low value of incidents is marked in green and are those that may be within normally operable parameters.

Table 4. Classification of incidents within a university campus.

Urgency \ Impact	High	Half	Low
High	1	2	3
Half	2	3	4
Low	3	4	5

4.10. Resolution Time

Response times must be established according to the level of urgency and impact of the incident. Table 5 shows the maximum response times in which a member of the IT must solve a requirement in this implementation. In this way, it is guaranteed that the quality of the service offered by the IT area is optimal. Good incident management is important

to properly handle each incident. In this way, an incident is directed to the most trained personnel or those who have the tools to solve the requirement.

Table 5. Maximum time to resolve an incident.

Risk Classification	Response Time
High	30 min. or immediately
Half	1 to 2 h
Low	2 h onwards

4.11. Incident Treatment

The user will establish the incident treatment process through the management diagram of a requirement from its entry or request until the closure and entry of information in the knowledge base, as can be seen in Figure 9. Similarly, it will be decisive to establish an initial service catalog according to the personnel, infrastructure and tools that are in possession.

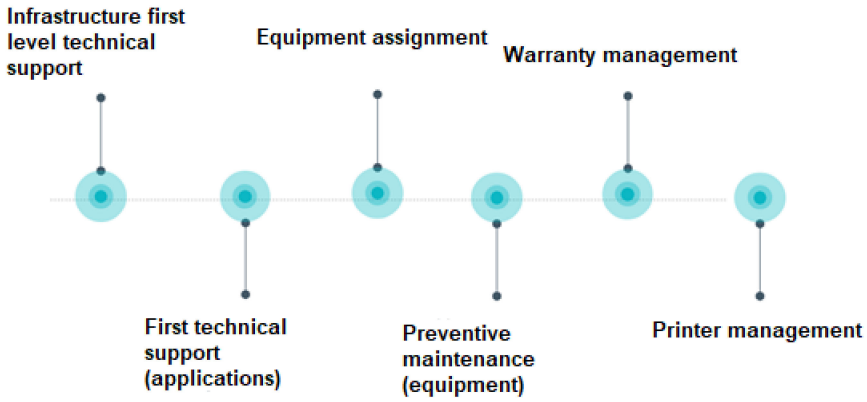

Figure 9. Incident handling with an initial service catalog.

5. Discussion

Currently, organizations have found it necessary to give continuity to their businesses using ICT. When moving all activities to a remote work or telework model, the security problems facing the infrastructures must be considered [19]. Universities, due to the large number of users that exist within their organizations and the services that they must deploy to provide continuity to education, have been compromised with respect to information security [18,42]. In 2020, attacks on university infrastructures have increased considerably. However, it is not enough to establish policies for and techniques for the detection and prevention of attacks and intruders [48]. It is necessary to establish response centers that have the capacity to respond to any incident and that all attacks are analyzed and detailed [9]. This knowledge must necessarily be shared between universities and organizations to promote immediate control policies that respond to the greatest number of attacks that are generated in a specific area.

The CSIRT have the ability to coordinate activities for a quick and efficient recovery of the activities that have been affected, in conjunction with the IT teams in such a way that organizations can operate normally in the shortest possible time and with the least tolerable impact [49]. In addition, they make it possible to prevent similar events from occurring in the future in such a way that the root causes of the incident can be eradicated. This is possible by maintaining a knowledge base that allows the lessons learned from these events to be recorded, with the aim that they are not repeated and if this happens, and a precedent of the possible solution or solutions can be counted on.

In work that includes models and techniques of defense against a security incident, policies and techniques for responding to attacks are generally established [25]. However,

this work includes activities to share information related to security incidents with other CSIRT, for dissemination purposes, and trying to mitigate the impact of new threats, vulnerabilities or attacks. Although at first glance, having an incident response team within the universities can be seen as an unnecessary expense, since there is no return on investment [38]. All actions aimed at protecting assets, mainly information, serve a specific purpose. In this sense, CSIRT activities can be seen as services offered by incident response teams in organizations, from a reactive and proactive perspective. With this analysis, it is proposed as future work to create test environments where it is possible to simulate defense attack models and how this information is aligned with the implemented CSIRT. Another line in which you want to work is on a data analysis model that takes the information generated from all the events stored in the CSIRT, through data mining models and algorithms, identify existing patterns, and classify them to improve the model's defense in the field of cybersecurity.

6. Conclusions

Today, it is necessary for organizations to work together to establish security policies to respond effectively to computer incidents. This work provides a complete guide on the implementation of a CSIRT, applied to an educational environment. Universities are very complete environments that serve as ideal training models for future professionals who will contribute to better standards and security policies in companies. However, this guide can be applied to all organizations and is a starting point for joint work at the national and international level in order to improve computer security at all levels.

The increase in incidents, as well as their degree of difficulty, makes it impossible for traditional security mechanisms or methods to be sufficient to deal with them. Therefore, mitigation strategies must be established that cover the entire organization. The protection of the assets of an organization depends largely on the security employed by the IT department. To do this, it is necessary to have more sophisticated security methods than those used for other areas of the company. Currently, it is important to have mechanisms for detecting threats, alerts, incidents, problems and computer attacks. For this, the development and implementation of a specialized team will achieve a robust security level in the company.

The increase in incidents, as well as their degree of difficulty, makes it impossible for traditional security mechanisms or methods to be sufficient to deal with them. Therefore, mitigation strategies must be established that cover the entire organization. The protection of the assets of an organization depends largely on the security employed by the IT department. To do this, it is necessary to have more sophisticated security methods than those used for other areas of the company. Currently, it is important to have mechanisms for detecting threats, alerts, incidents, problems and computer attacks. For this, the development and implementation of a specialized team will achieve a robust security level in the company.

The tools used in the field of information security, such as the implementation of an antivirus, firewall, traffic control, audits, vpn, etc., are not enough to mitigate the increase in attacks, so having a team specialized for an organization is indispensable. For this reason, it is advisable to create tools that allow incidents to be entered digitally, since in this way reports and statistics can be obtained and subsequently monitored.

Author Contributions: Conceptualization, W.V.-C.; formal analysis, I.O.-G.; investigation, W.V.-C., I.O.-G. and S.S.-V.; methodology, W.V.-C. and I.O.-G.,; project administration, S.S.-V.; visualization, S.S.-V.; writing—original draft, I.O.-G.; writing—review & editing, S.S.-V. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Skopik, F.; Settanni, G.; Fiedler, R. A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Comput. Secur.* **2016**, *60*, 154–176. [CrossRef]
2. Martins, R.D.J.; Knob, L.A.D.; Da Silva, E.G.; Wickboldt, J.A.; Schaeffer-Filho, A.; Granville, L.Z. Specialized CSIRT for Incident Response Management in Smart Grids. *J. Netw. Syst. Manag.* **2018**, *27*, 269–285. [CrossRef]
3. Tanczer, L.M.; Brass, I.; Carr, M. CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy. *Glob. Policy* **2018**, *9*, 60–66. [CrossRef]
4. Espín, F.V. Guidelines and Their Challenges in Implementing CSIRT in Ecuador. In *Advances in Intelligent Systems and Computing*; Springer Science and Business Media, LLC: Riobamba, Ecuador, 2021; pp. 239–251.
5. Van Der Kleij, R.; Kleinhuis, G.; Young, H. Computer Security Incident Response Team Effectiveness: A Needs Assessment. *Front. Psychol.* **2017**, *8*, 1–8. [CrossRef] [PubMed]
6. Zamzuri, Z.F.; Manaf, M.; Ahmad, A.; Yunus, Y. Computer Security Threats towards the E-Learning System Assets. In Proceedings of the Communications in Computer and Information Science, Pahang, Malaysia, 27–29 June 2011; pp. 335–345.
7. Graham, J.H.; Yu, Y. Computer System Security Threat Evaluation Based Upon Artificial Immunity Model and Fuzzy Logic. In Proceedings of the 2005 IEEE International Conference on Systems, Man and Cybernetics, Waikoloa, HI, USA, 10–12 October 2005; Volume 2, pp. 1297–1302.
8. ESET. Security Security Report. *Security* **2020**, *7*, 1–15.
9. Mulwad, V.; Li, W.; Joshi, A.; Finin, T.; Viswanathan, K. Extracting Information about Security Vulnerabilities from Web Text. In Proceedings of the 2011 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology, Lyon, France, 22 August 2011; Volume 3, pp. 257–260.
10. Rao, D.; Stupans, I. Exploring the potential of role play in higher education: Development of a typology and teacher guidelines. *Innov. Educ. Teach. Int.* **2012**, *49*, 427–436. [CrossRef]
11. Narasimhan, R.; Kim, S.W.; Tan, K.C. An empirical investigation of supply chain strategy typologies and relationships to performance. *Int. J. Prod. Res.* **2008**, *46*, 5231–5259. [CrossRef]
12. Panko, R.R. Computer Security Incident Response Teams (CSIRTs). *Handb. Comput. Netw.* **2012**, *3*, 632–638.
13. Bhaskar, R.A. Proposed Integrated Framework for Coordinating Computer Security Incident Response Team. *J. Inf. Priv. Secur.* **2005**, *1*, 3–17. [CrossRef]
14. Fuertes, W.; Reyes, F.; Valladares, P.; Tapia, F.; Toulkeridis, T.; Pérez, E. An Integral Model to Provide Reactive and Proactive Services in an Academic CSIRT Based on Business Intelligence. *Systems* **2017**, *5*, 52. [CrossRef]
15. Tchoubar, T.; Sexton, T.R.; Scarlatos, L.L. Role of Digital Fluency and Spatial Ability in Student Experience of Online Learning Environments. *Adv. Intell. Syst. Comput.* **2019**, *1*, 251–264. [CrossRef]
16. Silva, A.; Silva, K.; Rocha, A.; Queiroz, F. Calculating the trust of providers through the construction weighted Sec-SLA. *Futur. Gener. Comput. Syst.* **2019**, *97*, 873–886. [CrossRef]
17. Wang, A.J.A. Information security models and metrics. In Proceedings of the 43rd Annual Southeast Regional Conference on-ACM-SE 43, New York, NY, USA; 2005; Volume 2, pp. 2178–2184.
18. Stanton, J.M.; Stam, K.R.; Mastrangelo, P.; Jolton, J. Analysis of end user security behaviors. *Comput. Secur.* **2005**, *24*, 124–133. [CrossRef]
19. Henning, R.R. Security service level agreements: Quantifiable security for the enterprise? In Proceedings of the New Security Paradigm Workshop, New York, NY, USA, 1 September 1999; pp. 54–60.
20. Lichtenstein, S.; Nguyen, L.; Hunter, A. Issues in IT Service-Oriented Requirements Engineering. *Australas. J. Inf. Syst.* **2005**, *13*, 176–191. [CrossRef]
21. Wiant, T.L. Information security policy's impact on reporting security incidents. *Comput. Secur.* **2005**, *24*, 448–459. [CrossRef]
22. Kjaerland, M. A classification of computer security incidents based on reported attack data. *J. Investig. Psychol. Offender Profiling* **2005**, *2*, 105–120. [CrossRef]
23. Wiik, J.; Gonzalez, J.J. Chronic Workload Problems in CSIRTs. In Proceedings of the 27th International Conference of the System Dynamics Society, Albuquerque, NM, USA, 26–30 July 2009; pp. 1–19.
24. Skierka, I.; Morgus, R.; Hohmann, M.; Maurer, T. CSIRT Basics for Policy-Makers. *Researchgate* **2015**, 1–28. Available online: https://www.researchgate.net/publication/323358187_CSIRT_Basics_for_Policy-Makers (accessed on 15 August 2021).
25. Grobler, M.; Bryk, H. Common challenges faced during the establishment of a CSIRT. *2010 Inf. Secur. South Afr.* **2010**, *1*, 1–6. [CrossRef]
26. De Cusatis, C.; Bavaro, J.; Cannistraci, T.; Griffin, B.; Jenkins, J.; Ronan, M. Red-blue team exercises for cybersecurity training during a pandemic. In Proceedings of the 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 27–30 January 2021; pp. 1055–1060.
27. Bresch, C.; Michelet, A.; Amato, L.; Meyer, T.; Hely, D. A red team blue team approach towards a secure processor design with hardware shadow stack. In Proceedings of the 2017 IEEE 2nd International Verification and Security Workshop (IVSW), Thessaloniki, Greece, 3–5 July 2017; pp. 57–62.

28. Meszaros, T.; Despinasse, F. Innovation in defense for crisis management: Red teams and blue teams. *Rev. Def. Natl.* **2020**, *1*, 101–105.
29. Naseri, A.; Azmoon, O. Proposition of Model for CSIRT: Case Study of Telecommunication Company in a Province of Iran. *Int. J. Comput. Sci. Issues* **2012**, *9*, 156–160.
30. Wiik, J.; Gonzalez, J.J. Persistent Instabilities in the High-Priority Incident Workload of CSIRTs. In Proceedings of the 27th International Conference of the System Dynamics Society, Albuquerque, NM, USA, 26–30 July 2009; pp. 1–15.
31. Bieker, F.; Friedewald, M.; Hansen, M.; Obersteller, H.; Rost, M. Privacy Technologies and Policy. In *Proceedings of the Proceedings of the 4th Annual Privacy Forum, (APF 2016)*; Frankfurt, Germany, 7–8 September 2017, Volume 10518, pp. 21–37.
32. Wiik, J.; Gonzalez, J.J. Limits to Effectiveness in Computer Security Incident Response Teams. In Proceedings of the 23rd International Conference of the System Dynamics Society, Boston, MA, USA, 1 August 2005; pp. 152–153.
33. Khan, R.; Khan, S.U.; Zaheer, R.; Khan, S. Future internet: The internet of things architecture, possible applications and key challenges. In Proceedings of the 10th International Conference on Frontiers of Information Technology, Islamabad, Pakistan, 17–19 December 2012; pp. 257–260.
34. Mahmoodi, Y.; Reiter, S.; Viehl, A.; Bringmann, O.; Rosenstiel, W. Attack Surface Modeling and Assessment for Penetration Testing of IoT System Designs. In Proceedings of the 2018 21st Euromicro Conference on Digital System Design (DSD), Prague, Czech Republic, 29–31 August 2018; pp. 177–181.
35. Ruefle, R.; Dorofee, A.; Mundie, D.; Householder, A.D.; Murray, M.; Perl, S.J. Computer Security Incident Response Team Development and Evolution. *IEEE Secur. Priv. Mag.* **2014**, *12*, 16–26. [CrossRef]
36. Search, H.; Journals, C.; Contact, A.; Iopscience, M.; Address, I.P. Improving the Effectiveness of CSIRTs. *Glob. Cyber Secur. Capacit. Cent.* **2015**, *158*, 211–235.
37. Elhissi, Y.; Haqiq, A. Information system at the Moroccan University: A business intelligence tool for management and communication of scientific research. In Proceedings of the 2016 International Conference on Information Technology for Organizations Development (IT4OD), Fez, Morocco, 30 March–1 April 2016; pp. 1–5. [CrossRef]
38. Chen, T.R.; Shore, D.B.; Zaccaro, S.J.; Dalal, R.S.; Tetrick, L.E.; Gorab, A.K. An Organizational Psychology Perspective to Examining Computer Security Incident Response Teams. *IEEE Secur. Priv. Mag.* **2014**, *12*, 61–67. [CrossRef]
39. Oh, S.-R.; Kim, Y.-G. Security Requirements Analysis for the IoT. In Proceedings of the 2017 International Conference on Platform Technology and Service (PlatCon), Busan, Korea, 13–15 February 2017; pp. 1–6.
40. Kowtha, S.; Nolan, L.A.; Daley, R.A. Cyber security operations center characterization model and analysis. In Proceedings of the 2012 IEEE Conference on Technologies for Homeland Security (HST), Waltham, MA, USA, 13–15 November 2012; pp. 470–475.
41. Janos, F.D.; Dai, N.H.P. Security Concerns towards Security Operations Centers. In Proceedings of the 2018 IEEE 12th International Symposium on Applied Computational Intelligence and Informatics (SACI), Timisoara, Romania, 17–19 May 2018; pp. 273–278. [CrossRef]
42. Schmitz, C.; Pape, S. LiSRA: Lightweight Security Risk Assessment for decision support in information security. *Comput. Secur.* **2020**, *90*, 101656. [CrossRef]
43. Valladares, P.; Fuertes, W.; Tapia, F.; Toulkeridis, T.; Perez, E. Dimensional data model for early alerts of malicious activities in a CSIRT. In Proceedings of the 2017 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS), Seattle, WA, USA, 9–12 July 2017; Volume 49, pp. 74–81. [CrossRef]
44. Marinos, L. Risk management and risk assessment at ENISA: Issues and challenges. In Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06), Vienna, Austria, 20–22 April 2006; Volume 2006, pp. 2–3.
45. Disterer, G. ISO/IEC 27000, 27001 and 27002 for Information Security Management. *J. Inf. Secur.* **2013**, *04*, 92–100. [CrossRef]
46. Kamarudin, S.; Mohammad, M.I. File Security based on Pretty Good Privacy (PGP) Concept. *Comput. Inf. Sci.* **2011**, *4*, 10–28. [CrossRef]
47. Uyana, M.; Escobar, M. Respuestas Ante Incidentes De Seguridad Informáticos (Csirt). 2013, p. 1. Available online: http://repositorio.espe.edu.ec/bitstream/21000/8123/1/AC-GSR-ESPE-047639.pdf (accessed on 15 August 2021).
48. Hssina, B.; Bouikhalene, B.; Merbouha, A. *Europe and MENA Cooperation Advances in Information and Communication Technologie*; Rocha, A., Mohammed, S., Felgueiras, C., Eds.; Springer: Berlin, Germany, 2016; Volume 520, ISBN 978-3-319-46567-8.
49. Wiik, J.; Gonzalez, J.J.; Kossakowski, K.-P. Effectiveness of Proactive CSIRT Services. Available online: https://www.researchgate.net/publication/221002694_Effectiveness_of_Proactive_CSIRT_Services (accessed on 15 August 2021).