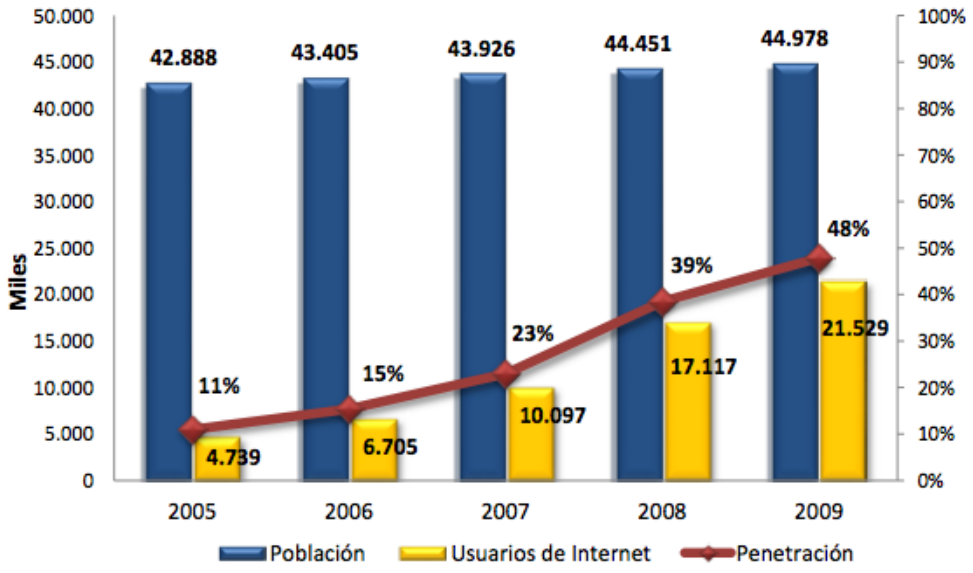
Software Engineering Institute
Carnegie Mellon University

COLUMBIA CSIRT CASE STUDY

The CSIRT Development and Training team has published this case study-part of a series of case studies-to assist CSIRTs in getting started and improving their performance.

Introduction

As in many other developing countries, Colombia's internet usage grew rapidly in the first decade of the century. Internet penetration, which started at just 3% in 2000, reached 45% of the population by 2009 and doubled between 2008 and 2010 (see the chart below) [Conp 2011]. Something clearly had to be done to confront the information security problems this rapid growth brought with it. This was especially true because the Colombian government was embarking on an important online government initiative *(Gobierno en Linea)* that would be severely compromised without a secure base from which to start.

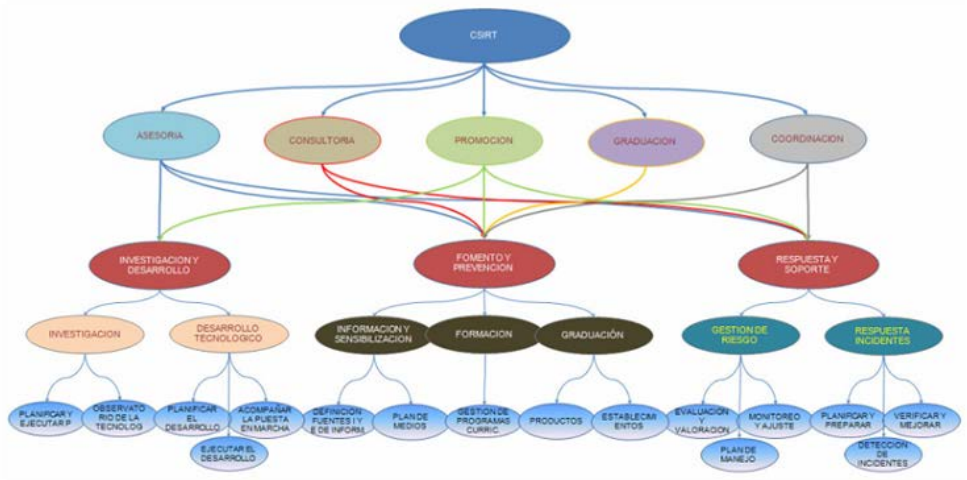


Early Initiatives

Between 2007 and 2010, the need for national action on cybercrime was becoming clear, resulting in several proposals and new initiatives.

CIRTISI

In May 2007, a preliminary 11-page proposal [CIRT 2007] for a national team named CIRTISI-Colombia *(Centro De Información y Respuesta Técnica a Incidentes de Seguridad Informática de Colombia)* was issued by the Colombian Ministry of Communications. That proposal suggested forming a team that would act as a computer security incident response team (CSIRT) for the government, set up a malware lab for government use, and work with the police on cybercrime. The figure below shows the structure of this CSIRT.



Col-CSIRT

In the same time frame, the Francisco José de Caldas University created Col-CSIRT with the goal of helping the academic and governmental communities prevent, detect, and handle cybersecurity incidents. The website for Col-CSIRT still exists but appears to be dormant.

El CSIRT Colombiano

In December 2008, the Ministry of Communications followed up with a 183-page proposal for a national CSIRT. The document is an impressive piece of work: It surveys the history of national CSIRTs, their theory and practice, and previous initiatives within Colombia. It defines the proposed CSIRT's goals, organizational structure, concept of operations, mission, constituency, organizational home, services, staffing, and even proposed budget ($1,620,957.96 for the first year of operation). The proposal also appears to have laid the groundwork for the Colombian Defense Ministry's CSIRT.

CSIRT-CCIT

The *Camara Colombiana de Informática y Telecomunications*, or CCIT, is a consortium of internet service providers (ISPs) that works closely with the government on issues such as developing the IT

sector in Colombia, passing cybercrime legislation, and implementing educational and marketing initiatives. Around 2009, the CCIT created CSIRT-CCIT, a team that assumed nationwide responsibility for all of Colombia. It was a coordinating CSIRT whose constituency was the major ISPs of Colombia. It monitored international cybersecurity organizations for potential incidents and distributed information about those threats to its constituents. It focused especially on financial phishing attacks in collaboration with the banking industry in Bogotá. Unfortunately, as of 2012, CSIRT-CCIT appears to have ceased operations, although its logo still appears on the CCIT website (the homepage is shown below).

ColCERT, CCC, CCP, and CSIRT-PONAL

Introduction

On July 14th, 2011, the Colombian National Planning Department published Conpes document Number 3701, "Policy for Cybersecurity and Cyberdefense." This document was approved by the Ministries of Interior, Justice, Foreign Relations, National Defense, Information and Communications, by the Security Department, and by the Attorney General's office. The introduction to this document says that its goal is to develop "a national strategy for counteracting the rise of computer threats which are a significant problem" for Colombia:

Adopting a National Policy on cybersecurity and cyberdefense which involves all sectors of society, under the leadership of the Minister of National Defense coordinating with the other state entities, is an imperative which must be given the highest priority.

The authors cite the Estonian incident, the 2009 distributed denial of service (DDoS) attacks against the Whitehouse, and the Mariposa botnet, noting that Colombia was the fifth most affected country from that attack. To underscore the seriousness of the situation, the authors note a survey showing that 75% of private-sector enterprises reported having suffered an attack during the preceding 12 months and that 42% of them considered information security their highest priority.

The report further mentions that Colombia has been the victim of targeted attacks and cites the 2011 attack by Anonymous (which occurred in the first half of 2011) and the fact that, in 2010, the number of computer crimes reported to the "policia informatica"-a total of 995-shows an increase of 73% during that year alone.

The National Context

The report summarizes the history of cybersecurity legislation in Colombia as a way of putting the proposed national team in context. The relevant laws are

- Law 527 (1999): regulates the use of email, ecommerce, and digital signatures
- Law 999 (2000): updates the penal code, making it a crime to misuse an information system
- Law 962 (2005): streamlines government services through the use of computer technology

- Law 1150 (2007): expedites government publishing by allowing the use of electronic media
- Law 1273 (2009): updates the penal code to better protect information systems
- Law 1341 (2009): creates the National Spectrum Agency and defines some principles of the "information society"
- Regulation 2258 (2009): establishes regulation of ISPs
- Circular 052 (2007): establishes minimum security requirements for information management

The report also summarizes three initiatives within Colombia that were taken into account when ColCERT was being designed:

- the information security model developed by Government Online within the Ministry of Information and Communications Technology, with the twin goal of protecting citizens' personal information and preserving the credibility of Government Online
- the recommendations made by the Telecommunications Regulatory Commission to the national government, urging the creation of a national cybersecurity strategy
- CSIRT-CCIT, mentioned above

The International Context

The report mentions five international initiatives that it considered relevant to creating ColCERT:

- the Council of Europe's Convention on Cybercrime
- Resolution AG/RES 2004 (XXXXV-O/04) of the General Assembly of the Organization of American States, which establishes a complete strategy for combating cyber risks and stipulates three paths of action: creation of a hemisphere-wide network of CSIRTs; identification and adoption of technical standards to improve the security of the internet; and adoption of a legal framework to protect internet users from cyber attacks
- Decision 587 of the Andean Community, which embodies a regional policy on information security
- the International Telecommunication Union's consensus on cybersecurity adopted in Tunis in 2005 [TUNI 2005]
- Resolution 64/25 of the General Assembly of the United Nations, which urges member states to protect against threats while maintaining a free flow of information

The report also notes that 13 countries in the region (Argentina, Bahamas, Bolivia, Brazil, Canada, Chile, United States, Guatemala, Paraguay, Peru, Suriname, Uruguay, and Venezuela) have already established CSIRTs and that the total number worldwide, as listed on ColCERT's webpage, has now reached 55.

Creating ColCERT

ColCERT grew out of a 2008 workshop cosponsored by the National Government and the Organization of American States' Interamerican Committee against Terrorism (CICTE). The workshop raised

awareness of the information security problem and led to a national dialog on the subject in 2009. That dialog resulted in the government asking the Ministry of National Defense to provide leadership for policies to deal with cybersecurity, as well as providing mechanisms for managing incidents and prosecuting cybercrimes. This decision was based on "...a profound analysis of the particularities of national defense, the technical capabilities of the Ministry of Defense, and the international context." During 2010 and 2011, the Ministry of Defense worked to position cybersecurity within the national agenda. For example, cybersecurity is now included in the five-year national development plan as part of the "Live Digital" initiative.

In April 2012, ColCERT was accepted as a member by the Forum of Incident Response and Security Teams (FIRST), the first Colombian organization to be so accepted. During 2012, ColCERT conducted five seminars for private and government organizations and publicized the formation of the team. A budget of more than $3,000,000 was allocated to the team through 2014, and a security operations center (SOC) is being implemented to provide security monitoring, early warning, and other cybersecurity services.

ColCERT's Organization

Staffing and staff development have begun, and the teams have already had to assume operational responsibilities to deal with some serious DDoS incidents. Many of the personnel being hired for the Ministerio de Defensa Nacional CERT are graduates of the master's program in information security launched by the University of the Andes around 2006.

ColCERT's Concept of Operations

The ColCERT is a national team that provides technical assistance, incident coordination, operational capability development, strategic intelligence information, and assessments. It is divided into two branches: the *Comando Conjunto Cibernético (Joint Cybernetic Command)* or CCC, which defends the government, and the *Centro Cibernético Policial (Cybernetic Police Center)* or CCP, which ensures citizen safety in cyberspace. CSIRT-PONAL, the CSIRT within the CCP, has the ambitious goal of making the national police the primary point of contact in Colombia for U.S. and Latin American police forces. The goal is to have a single controlling organization for cyberspace in Colombia. To this end, CSIRT-PONAL has assembled a team dedicated to securing information and communication technology, and helping organizations mitigate and prevent serious information security incidents.

In a presentation titled *Evolución de la Ciberseguridad*, Alex Duran Santos, the head of CSIRT-PONAL, explains the mission and vision of his organization. CSIRT-PONAL, he says, understands that knowledge is the transformation of information, whereby it becomes critical strategic assets. The CSIRT's goal is to form a trained, qualified team to design, implement, measure, and monitor the Information Security Management System (ISMS). (The government chose ISO 27001 as its information security framework.) The team is aware of the need to invest in tools and training to form the ISMS team, to establish an information security policy supported by upper management, and to establish a mature business continuity and recovery model to deal with security incidents. To achieve

that mission, CSIRT-PONAL is using a fairly classic plan-do-check-act strategy, starting with the creation of an organizational culture favorable to improving security and then identifying the critical processes, analyzing risks, making management decisions based on that risk analysis, implementing the necessary controls, measuring their effectiveness, and adjusting the ISMS based on those measurements.

The problem that CSIRT-PONAL is confronting is serious and involves ever-increasing numbers of reported events, the evolution of malware technology, rising monetary losses, increasing numbers of web defacements in both the governmental and private sectors (375 cases in 2011), increasing numbers of DDoS attacks (30 in 2011), and an increasing number of cases of cybercrime (over 1000 in 2011, including unauthorized access to information systems, theft of intellectual property, sabotage, use of malware, and unauthorized modifications to websites).

To address this problem, CSIRT-PONAL's set these objectives: strengthen the ability of the state to protect against threats to its cybersecurity; create the environment necessary to provide protection in cyberspace; create guidelines for developing and promoting cybersecurity; put capabilities and mechanisms in place to identify and establish the roles and responsibilities needed to protect, prepare, manage, respond, and recover from any cybersecurity threat; and raise citizens' awareness of cybersecurity issues.

The scope of the problem is daunting. The Ministry of Defense is the largest organization in Colombia, distributed over 8,368 sites in the country. It has over 166,000 employees and hires 4,700 more every year. In addition, there is a floating population of 27,000 reservists. This large organization has many different information sources, including 25,000 computer groups and 50 information systems. One interesting aspect of the situation is that there are 50,000 communication radios tied into the computer systems.

CSIRT-PONAL is organized into three teams. The first is dedicated to prevention through officer training; outreach through email and bulletins; and conferences and workshops. The second responds to incidents by identifying activities that generate risks or threats to constituents' information systems; developing mitigation and response strategies; and publishing early warning of possible malicious

activity. The third team is the forensics team, which is dedicated to supporting legal prosecution of cybercriminals.

Lessons Learned

In his overview of CSIRT-PONAL, Duran Santos reproduces a slide from the CERT Program's courses that shows the expected five-stage evolution of a newly formed CSIRT, from Education through Planning, Implementation, Operation, and Collaboration. The fact that this diagram became part of the overview is telling because it reflects the process that the National Police went through forming CSIRT-PONAL. They began by sending potential CSIRT members to CERT classes and other training, and making contacts with the local universities. The early initiatives described in Section 2 constituted the Planning phase, with much thought given to how the CSIRT model could be tailored to the Colombian context. Implementation began in 2010 and culminated in an international conference, the " *Seminario Internacional de Seguridad de la Información*," held in Bogotá in October 2011.

The primary lesson learned is that with a clear vision and mission, and strong governmental support, success is possible by following the tried and true processes learned from past experience of other teams. The Colombian experience also illustrates the need for flexibility and pragmatism when setting up a national team. Multiple proposals from government, academia, the military, and the private sector competed with each other before crystalizing in the CSIRT PONAL.

References

[CONP 2011]
"Lineamientos de política para ciberdefensa." Consejo Nacional de Política Económica y Social, República de Colombia, Departamento Nacional de Planeación, document Conpes 3701, 2011.

[DURA 2011]
Duran Santos, Alex. "Policia Nacional: Evolución de la Ciberseguridad CSIRT-PONAL." ARADI-PONAL, BogotÃ¡, 2011.

[MINI 2008]
Ministerio de Comunicaciones, República de Colombia, "Diseño e un CSIRT de Colombia para la estrategia Gobierno en Línea" Bogotá, December 2008.

[NOTI 2010]
Noticias de Colombia, " Ministerio de Defensa implementa centro contra ataques cibernéicos," 2010.

[SALA 2011]
Salas, F. C. "El Gobierno en línea la seguridad de la información. Presentation at the International Seminar on Information Security "Nuevos Retos," Bogotá Colombia, October 2011.

[TUNI 2005]
"Tunis Agenda for the Information Society". International Telecommunications Union Document WSIS-05/TUNIS/DOC/6(Rev. 1)-E, Tunis, November, 2005.

Contact Us

Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

Phone: 412/268.5800 | 888.201.4479
Web: www.sei.cmu.edu | www.cert.org
Email: info@sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM-0004352