



**Project Number:**

**Project Title:** Disseminating Cybersecurity Culture and Combating Cyber Threats in Latin America

**Estimated Start Date:** July 2012

**Estimated End Date:** June 2014

**Cooperation Agencies:** ASETA, CITEL, COMTELCA, REGULATEL

**Other Cooperating Partners:** UN Agencies and IMPACT

**Implementing Agency:** International Telecommunication Union (ITU)

**Beneficiary Countries:** Latin American countries of the Americas Region

**ITU Project Manager:** Regional Office for the Americas, Brazil

**SUMMARY OF CONTRIBUTIONS**

**A) Project Budget**

Description	USD
Personnel costs	
SSA Consulting	90,000
Missions (SSA and ITU)	79,000
External Services	36,000
Miscellaneous and Other Costs	36,875
<b>Total:</b>	<b>241,875</b>

**B) Cost Sharing:** USD 241,875

**C) Contributions from Beneficiary Countries:**

**In-kind:** all those specified in this PRODOC including availability of logistic facilities

**In-cash:** as to ensure the recruitment of experts in case no other funding partners are identified

**Brief Description:**

The overall Project objective is planning, developing and implementing capacity building programmes in the field of cybersecurity for government decision-makers of Latin American countries, including ministerial agencies and regulators mainly focused on the need of developing a sustainable and proactive culture of cybersecurity, awareness of legal aspects for future harmonization of cybersecurity laws, development of national strategies and security standards. This project aims at promoting and facilitating, through online/face-to-face training programmes, the implementation and deployment of cybersecurity capabilities towards the consolidation of the ITU Global Cybersecurity Agenda (GCA).

For the	Signature	Date	Name/Title
ITU:	_____	__/__/__	
Partner(s):	_____	__/__/__	
	_____	__/__/__	

# 1. BACKGROUND AND CONTEXT

## 1.1 BACKGROUND

Information and Communication Technologies (ICTs) are constantly transforming lifestyles since they have become an integral part of modern societies, propelling the end user to the forefront of communication. ICTs provide real time communication, borderless and almost unlimited access range of innovative services and entertainment. There is a common understanding among the members of the international community that ICTs provide unprecedented opportunities to accelerate social and economic development, at the same time, ICTs misuse and their vulnerabilities have also created new threats and ever-growing challenges across national borders for all countries.

All kind of information is available through Internet, in all different formats and of varying topics and points of view. Every person who is on the internet is vulnerable to cyber threats such as malware and attacks, which are becoming extremely sophisticated. ITU recognizes that information and technology security are critical priorities for the international community. Cybersecurity generally is in everyone's best interest and this can only be achieved through a collaborative effort.

In this sense, ITU launched in 2007 the **Global Cybersecurity Agenda (GCA)** that is a framework for international cooperation aimed at enhancing confidence and security in the information society. The GCA is designed for cooperation and efficiency, encouraging collaboration with and between all relevant partners and building on existing initiatives to avoid duplicating efforts. The GCA strives to engage all relevant stakeholders in a concerted effort to build confidence and security in the information society. The GCA is built upon five strategic pillars, also known as work areas, as follows: (a) Legal measures, (b) Technical and procedural measures, (b) Organizational structures, (d) Capacity building and (e) International Cooperation.

In addition, ITU collaborates with the **International Multilateral Partnership Against Cyber Threats (IMPACT)** -an international public-private initiative dedicated to enhancing the global community's capacity to prevent, defend and respond to Cyber threats. IMPACT's new state-of-the-art global headquarters in Cyberjaya, Malaysia, has become the physical home of the GCA. This landmark collaboration provides ITU's 193 Member States with the expertise, facilities and resources to effectively address the world's most serious cyber threats. The close synergies between the five work areas of the GCA and the services and infrastructure provided by IMPACT made this partnership a logical step in the global fight against cyber threats, cybercrime and other misuses of ICTs.

The ITU-IMPACT Collaboration seeks to build on synergies to provide a number of services and activities. These include: real-time analysis, aggregation and dissemination of global cyber threat information; Early warning system and emergency response to global cyber threats; and training and skills development on the technical, legal and policy aspects of cybersecurity. Several ITU Member States globally, including twenty-one (21) from the Americas Region<sup>1</sup> are receiving cybersecurity services from IMPACT and enabling them to have access to its Global Response Centre (GRC), intellectual property, consulting services, reports and more.

IMPACT initiatives, such as the GRC, as well as training and skills development, security assurance, research, and international cooperation will be conducted under the auspices of the GCA.

The GRC plays a pivotal role in realizing the GCA objective of putting technical measures in place to combat new and evolving cyber threats. The two prime highlights of the GRC are NEWS (Network Early Warning System) and ESCAPE (Electronically Secure Collaboration Application Platform for

---

<sup>1</sup> Antigua and Barbuda, Belize, Brazil, Costa Rica, Cuba, Dominican Republic, Ecuador, Grenada, Guatemala, Guyana, Honduras, Panama, Paraguay, Peru, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and The Grenadines, Suriname, Trinidad and Tobago, Uruguay and Venezuela.

Experts). The GRC is designed to be the foremost cyber threat resource centre in the world. Working with leading partners including academia and governments, the Centre will provide the global community with a real-time aggregated early warning system. NEWS will help countries identify cyber threats early on and provide critical guidance on what measures to take to mitigate them.

The GRC also aims at providing ITU Member States with access to specialized tools and systems, including the above-mentioned ESCAPE platform, which is an electronic tool that enables authorized cyber-experts across different countries to pool resources and collaborate with each other remotely, yet within a secure and trusted environment. By pooling resources and expertise from many different countries on short notice, ESCAPE will enable individual nations and the global community to respond immediately to cyber threats, especially during crisis situations.

IMPACT is poised to help its partner countries track and overcome looming cyber threats, through the GRC. Through IMPACT and its GRC, partner countries<sup>2</sup> can enhance their knowledge and awareness of the cyber threat landscape that affects them, while learning about possible solutions to overcome these malicious attacks. With IMPACT operationalizing ITU's GCA, current Member States of the ITU are eligible to become IMPACT's partner countries.

Within the framework of the GCA and in line with ITU's mandate to assist Member States in developing cybersecurity capacity, among other things, the ITU works to facilitate the deployment of cybersecurity capabilities necessary to combat cyber threats. As such, the ITU Telecommunication Development Bureau (BDT) is playing a key role in implementing the main goals of GCA, and responding to the needs of Member States.

## 1.2 CONTEXT

With the important role that ICTs play today in providing services in sectors as varied as health, education, finance and commerce, awareness of the opportunities offered by a secure cyber environment and of the threats inherent to cyber space are vital. Since threats can originate anywhere around the globe, the challenges are inherently international in scope and require international cooperation, investigative assistance, and common substantive and procedural provisions.

The Internet and ICTs have enabled interconnection between countries and they can neither easily close their borders to incoming cyber threats nor contain those coming from within. Cybersecurity is as global and far-reaching as the Internet and solutions need to be harmonized across all borders. This necessarily entails international cooperation, not only at government level, but also with industry, non-governmental and international organizations. Cybersecurity concerns all types of measures. For this reason, the GCA seeks to harness the power of multi-stakeholder collaboration in order to arrive at global strategies to enhance cybersecurity.

Since its launch, the GCA has attracted the support and recognition of leaders and cybersecurity experts around the world<sup>3</sup>. The GCA has fostered initiatives such as the Child Online Protection (COP) and through its partnership with IMPACT and with the support of leading global players is currently deploying cybersecurity solutions to countries around the world.

Programmes aimed at creating a level playing-field in raising basic awareness and building capacity at all levels are important, and these also need to be undertaken within the international arena.

Together with legal measures, international cooperation and other areas of work, capacity building is one important pillar for the establishment of harmonized laws, systems and develops a sustainable and proactive culture of cybersecurity. The international community identified several challenges in the field of cybersecurity and some of them concern on how effectively educating the

---

<sup>2</sup> <http://www.impact-alliance.org/countries/alphabetical-list.html>

<sup>3</sup> H.E. Dr. Óscar Arias Sánchez, President of the Republic of Costa Rica and Nobel Peace Laureate, and H.E. Blaise Compaoré, President of Burkina Faso, are both Patrons of the GCA.

end user since understanding and awareness of the potential dangers are critical. In addition, it is also important to understand the legal aspects of cyber-security in order to move towards harmonizing legal frameworks. Threats can originate anywhere around the globe and it is important that countries harmonize their legal frameworks to combat cybercrime and facilitate international cooperation. Countries also need to develop their national strategies by examining their existing capacities for addressing challenges to cybersecurity, identifying their requirements and outlining a national response plan. All those issues concern all stakeholders from governments.

The World Telecommunication Development Conference 2010 (WTDC-10) designed and adopted the Hyderabad Action Plan (HAP) to enable developing countries to promote the equitable and sustainable development of information and communication technology (ICT) networks and services. The HAP is a four-year comprehensive package of activities, which include five Programmes. Among these programmes, Programme 2<sup>4</sup> was designed to focus on Cybersecurity as one of the priority areas. In this framework, the objective of the ITU/BDT is to support ITU Member States in the development of their national and /or regional cybersecurity strategies, as an essential step towards building national capabilities for dealing with cyberthreats. In consonance with World Summit on the Information Society (WSIS) Action Line C5, "Building confidence and security in the use of ICTs", ITU is working to address the emerging challenges of the Information Society.

This Project is directly related to **Americas Regional Initiatives 3 and 5** based on the need to disseminate awareness of cybersecurity as to support secure/safe promotion of ICTs and broadband access in urban/rural areas (Regional Initiative 3), developing, at the same time, human capacity building on ICTs for the decision-makers (Regional Initiative 5). Knowledge and culture of cybersecurity should be widely disseminated by governments by fostering digital inclusion in a security and safe electronic environment, promoting telecommunication/ICT accessibility and the use of telecommunications/ICTs for the social and economic development including people with special needs. Also as indicated in the Regional Initiative 5, it is expected to promote technical cooperation between telecommunication/ICT training institutions for sustainable delivery of special programmes.

Considering that personal computers, mobile phones, and other devices are becoming ever more powerful, that technologies are converging, that the use of ICTs is becoming more and more widespread, and that connections across national borders are increasing, all participants who develop, own, provide, manage, service and maintain information networks must understand cybersecurity issues and take action appropriate to their roles to protect networks. Governments play a key role taking the leadership in promoting a culture of cybersecurity and facing their challenges.

## **2. PROJECT DESCRIPTION**

The overall Project objective is planning, developing and implementing capacity building programmes in the field of cybersecurity for government decision-makers of Latin American countries, including ministerial agencies and regulators mainly focused on the need of developing a sustainable and proactive culture of cybersecurity, awareness of legal aspects for future harmonization of cybersecurity laws, development of national strategies and security standards. This project aims at promoting and facilitating, through online/face-to-face training programmes, the implementation and deployment of cybersecurity capabilities towards the consolidation of the GCA.

---

<sup>4</sup> Programme 2: Cybersecurity, ICT Applications and IP-based network-related issues

### **3. EXPECTED OUTPUTS**

The following outputs are envisaged:

**3.1** Development of a consultancy service on “Cybersecurity Challenges and Perspectives in the Latin America”.

**3.2** Planning, development and implementation of online and/or face-to-face training activities based on the ITU Legal Resources, namely the “ITU Toolkit for Cybercrime Legislation” and the “Understanding cybercrime: a guide for developing countries”. This activity will also take into account existing international instruments, and will be undertaken within the overall framework of collaboration between ITU and the United Nations Office on Drugs and Crime (UNODC), where the two UN bodies agreed to cooperate globally on providing technical assistance. Therefore some specific activities will be jointly undertaken by ITU and UNODC.

**3.3** Planning, development and implementation of online and/or face-to-face training activities based on “ITU National Cybersecurity Strategy Guide”.

**3.4** Organization of face-to-face regional/sub-regional assessment workshops on the establishment of sound organizational structures with national responsibilities, namely National Computer Incident Response Team (CIRT), tailored to the ITU IMPACT deployment of the Global Response Centre.

The training programmes will be implemented with the support of the ITU Centre of Excellence for the Americas Region.

### **4. INDICATORS**

The following indicators will be used to measure the success of the Project:

**4.1** Elaboration of 1 (one) Report/Assessment on “Cybersecurity Challenges and Perspectives in the Latin America”.

**4.2** At least one (1) online and/or face-to-face training activity on facilitating the establishment and harmonization of cybercrime legislations, using the ITU and other existing tools, and within the framework of the ITU/UNODC collaboration.

**4.3** At least one (1) online and/or face-to-face training activity on the “ITU National Cybersecurity Strategy Guide”.

**4.5** At least one (1) face-to-face regional/sub-regional workshop on facilitating the establishment of Computer Incident Response Teams (CIRT).

**4.7** At least 70% of the target audience for the training activities/workshops being decision-makers and specialists from government’s institutions.

**4.8** At least 10% of the target audience for the training activities/workshops being representative of academic and research institutions.

## 5. MAIN ACTIVITIES

In accordance with the GCA, the following activities are planned to be carried out in the framework of this project:

**3.1** Development of consultancy service for an assessment on Cybersecurity Challenges and Perspectives in the Latin America.

**3.2** Planning, development and implementation of online and/or face-to-face training activities based on the **ITU Legal Resources**:

The ITU cybercrime legislation resources<sup>5</sup> currently consist of two main deliverables: 1) the ITU publication titled “**Understanding Cybercrime: A Guide for Developing Countries**” that aims at helping developing countries better understand the national and international implications of growing cyber-threats, assess the requirements of existing national regional and international instruments, and assist countries in establishing a sound legal foundation; 2) **The ITU Toolkit for Cybercrime Legislation** that is a practical instrument that countries can use for the elaboration of a cyber-security legal framework and related laws. It is intended to serve as a guide for countries desiring to develop, draft, or modify their own cybercrime laws and to advance the global harmonization of cybercrime laws by serving as a central resource to help legislators, attorneys, government officials, policy experts, and industry representatives around the globe move their countries toward a consistent legal framework that protects against the misuse of ICTs. This activity will be undertaken within the broader collaboration framework between ITU and UNODC.

**3.3** Organization of face-to-face regional/sub-regional assessment workshops, on the establishment of sound organizational structures with national responsibilities, namely National Computer Incident Response Team (CIRT), tailored to the ITU IMPACT deployment of the Global Response Centre:

The primary objective of this activity is to assist the identified Member States in the assessment of their readiness to implement a National CIRT. The National CIRT would provide a capability to identify, respond and manage cyber threats and at the same time will enhance the cybersecurity posture of the country. The establishment of National CIRT, integrated with the ITU IMPACT capabilities already deployed, namely GRC, and taking into account international best practices (e.g. from FIRST) can play a key role in maintaining round-the-clock vigilance to defend critical national infrastructure/assets against cyberattacks, and also serve as a critical cyber-nerve centre in analyzing threat information. Specific activities may include:

- a. Study the readiness assessment of current needs of the countries.
- b. Study and suggest institutional and organizational requirements, and arrangements for setting-up National CIRTs.
- c. Capacity building program for the CIRTs.
- d. Conduct trainings for human capacity building to impart knowledge and skills for operation, maintenance and coordination of CIRTs with relevant agencies, both local and international.
- e. Design specifications for hardware and software for the CIRTs.

---

<sup>5</sup> The ITU Legal Resources are available at: <http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html>

### 3.4 Planning, development and implementation of online and/or face-to-face training activities based on the **ITU National Cybersecurity Strategy Guide**:

**ITU National Cybersecurity Strategy Guide** focuses on the issues that countries should consider when elaborating or reviewing national cybersecurity strategies. As national capabilities, needs and threats vary, countries use national values as the basis for strategies for two main reasons. Firstly, culture and national interests influence the perception of risk and the relative success of defenses against cyber threats. Secondly, a strategy rooted in national values is likely to gain support of stakeholders such as the judiciary and private sector. Since cybersecurity is a national policy issue, the guide adopts the Ends-Ways-Means strategy paradigm due to its popularity with national policy-makers. The activity will have the main objective of assisting Member States on building a plan for the establishment of a national cybersecurity strategy, and build the necessary capacity to implement it.

## 6. INPUTS

### 6.1 International Telecommunication Union (ITU)

ITU will be the executing agency. ITU will undertake to manage the staff resources that will be funded and hired through this project. Information on the access and use of ICTs related issues, access to ITU existing materials, including training courses and relevant publications will be provided. ITU will exercise all reasonable skill, care and diligence to ensure the success of the project. ITU will also indicate a Project Coordinator to monitor and evaluate its implementation, will identify and recruit the specialists to implement the training programmes.

### 6.2 Partners

It is necessary to identify partners interested in provide funding support for the implementation of the Project. The Project foresees the recruitment of experts to delivery the training activities, as well the coordinate the workshops at an estimated cost of **USD 241.875**. The cost of the activities foreseen to be carried out in the framework of this Project can be covered by programs and/or initiatives of the organizations working for the combat of cyber treats.

### 6.3 Beneficiaries

The regional organizations and respective countries are expected to provide support for the organization of the training activities and workshops, through staff resources and local facilities. The beneficiary countries are also expected to provide information/data necessary to carry out the work, secured premises to host the training activities and workshops, logistics arrangements and support and any other assistance to the project that may be required by the project staff.

## 7. RISK ASSESSMENT

**7.1** Regional organizations, multiple national government institutions and local partners committed with the Project will work in close coordination since the lack of coordination/collaboration among the stakeholders involved may represent a risk.

**7.2** The collaboration of the relevant Government partners to the development of the project is essential to reduce any implementation risk at this level.

**7.3** Primary risk is that activities may suffer delays due to unforeseen events and/or circumstances. In this sense, the Project Coordinator will ensure the preparation of each activities in due time.

## **8. PROJECT MANAGEMENT**

**8.1** The roles and responsibilities of the different stakeholders will be clearly defined in a stakeholder meeting at the beginning of the Project. ITU is the Executing Agency. After the identification of the primary funding agency and in order to facilitate the implementation of this project, a project team funded by the project, will be constituted by ITU, including a Project Coordinator.

**8.2** The Project Coordinator will be responsible for the implementation of the Project under the supervision of the Regional Director of the ITU Americas Regional Office, in close coordination with the Area Offices, as well as with the corresponding Departments at ITU Headquarters.

**8.3** The Project Coordinator will work in close coordination with the corresponding Services at Headquarters for the management and follow-up of all administrative and financial aspects involved in the Project and will regularly provide the corresponding Progress Reports.

**8.4** The Project Coordinator will provide to the funding partners the Financial Situation of the Project to be updated by the corresponding service at ITU Headquarters.

## **9. MONITORING AND EVALUATION**

**9.1** The progress of the project will be monitored through periodic reports to be prepared by the Project Coordinator.

**9.2** A final evaluation report will be prepared at the end of the Project.

**9.3** Special reports may be required and they will be provided in accordance to the situation.

**9.4** Field visits will be arranged to those training face-to-face activities that may require a direct evaluation of their progress.

**9.5** Coordination meetings of evaluation may be arranged as per decided by the Parties involved.

**9.6** A Project Closure Report will be prepared by the Project Coordinator in close coordination with the Parties.

## 10. WORK PLAN

Activities	2012		2013				2014	
	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q
Identification of primary funding Partner								
Report/Assessment on “Cybersecurity Challenges and Perspectives in the Latin America”								
<b>Progress Report</b>								
Implementation of online training activity on the “ITU legal resources”								
Implementation of online training activity on the “ITU National Cybersecurity Guide”								
<b>Progress Report</b>								
Implementation of a face-to-face regional/sub-regional workshop on the establishment of Computer Incident Response Team (CIRT)								
<b>Progress Report</b>								
Final Report								
<b>Project closure</b>								

## 11. BUDGET

The estimated budget for the project is the following:

Sponsor Classes	Description	Budget in US\$
3000	STAFF COST	90.000
3100	MISSION EXPENSES	79.000
3300	EXTERNAL SERVICES	36.000
	Miscellaneous other costs	36.875
<b>TOTAL BUDGET:</b>		<b>241.875</b>

