Continuity of business and operations during disasters in Latin America and the Caribbean: Balance and recommendations

Economic and Technical Cooperation

II Regional Seminar “Partnership between public and private sectors for disaster risk reduction: Continuity of government and continuity of business operations during disasters”
Cartagena de Indias, Colombia
01 and 02 August 2013
SP/II-SR-ASPPG RD/DT Nº 2-13
CONTENTS

FOREWORD

EXECUTIVE SUMMARY 3

I. INTRODUCTION 4

II. PRELIMINARY DEFINITIONS 5

III. WHY IS CONTINUITY OF BUSINESS AND OPERATIONS IMPORTANT FOR LATIN AMERICA AND THE CARIBBEAN? 6
   1. Natural threats 6
   2. Man-made threats 7
   3. Threats caused by technological failures for reasons not attributable to nature or man 8

IV. APPLICABLE METHODOLOGICAL STANDARDS AND REGULATIONS 8
   1. DRII (Disaster Recovery Institute International) 9
   2. BCI (Business Continuity Institute) 9
   3. ANSI/ASIS SPC.1 10
   4. NFPA 1600 11
   5. ISO 22301 11

V. METHODOLOGY APPLIED TO THE PUBLIC AND PRIVATE SECTORS 12
   1. Empowering and governing continuity of business and operations 12
   2. Identifying priority and urgent recovery activities 15
   3. Protecting most urgent activities 18
   4. Establishing strategies for continuity and recovery of activities 20
   5. Documenting action plans to be applied at the moment of the event 24
   6. Drilling and testing action plans 26
   7. Raising awareness and competences in the organization 28
   8. Maintaining continuity of business and operations 28
   9. Indicator of maturity and strategic planning on continuity of business and operations 29

VI. SUCCESSFUL CASES 31
   1. Implementation of professional practices for continuity of business and operations 31
   2. Integration of public and private sectors 34

VII. CONCLUSIONS AND RECOMMENDATIONS 35

BIBLIOGRAPHY 39
FOREWORD

This document was drafted in compliance with the Work Programme of the Permanent Secretariat of the Latin American and Caribbean Economic System (SELA) for 2013, Project II.1 “Strengthening economic and technical cooperation in Latin America and the Caribbean, in line with the mandates of CELAC”, which envisages Activity II.1.3, “Partnership between public and private sectors for disaster risk reduction in Latin America and the Caribbean. Promoting strategic alliances with the private sector.”

Along with the document on continuity of government and operations, this study is a contribution of the Permanent Secretariat to encourage the discussions and debates that will take place during the II Regional Seminar “Partnership between public and private sectors for disaster risk reduction: Continuity of government and continuity of business operations during disasters”, to be held in Cartagena, Colombia on 1 and 2 August.

The document comprises an introduction and six chapters dealing with the following issues: i) Some preliminary definitions of commonly used terms; ii) The most frequent natural, man-made and technological threats in Latin America and the Caribbean; iii) The most recent and recognized world-class standards and regulations to implement programmes for continuity of business and operations; iv) The recommended methodology that both public and private organizations may apply to implement and maintain their business and operations continuity programmes; v) Some examples of how some Latin American and Caribbean organizations are implementing best practices, both at company level and in coordination between the public and private sectors; and finally vi) Conclusions and recommendations.

This study was prepared by Consultant Yves Dávila Cainero, to whom the Permanent Secretariat wishes to express its gratitude and recognition.
EXECUTIVE SUMMARY

Latin America and the Caribbean is a region where major natural events have occurred, such as earthquakes, tsunamis, hurricanes, tropical storms, fires, floods, landslides, ash rains from volcanic eruptions and extreme cold, among others. Populations are affected by such events, but organizations also suffer their impacts which sometimes force them to paralyse operations.

The Latin American and Caribbean Economic System (SELA), the United Nations International Strategy for Disaster Reduction (UN/ISDR) and the Office of U.S. Foreign Disaster Assistance (USAID-OFDA) are working on initiatives that seek to promote the private sector’s participation in the response led by the public sector. The organizations in both sectors may be affected by disasters and they may cease to provide the key services that are the raison d’être of public and private organizations. The service systems for electrical power, water, telephone, gas, financial sector, companies in the area of consumer goods, among others, should continue to operate so that society continues normal life despite the disaster.

Continuity of business and operations is aimed at ensuring the survival of organizations during disasters. Survival means that organizations must have prioritized in advance which activities carried out on a daily basis should be recovered or continue to operate. Just as in the case of a person’s survival, in which vital organs are already defined, the same thing should happen for organisations: vital activities must be defined.

In addition to the security measures already existing in the organization, further protection measures should be taken in the case of vital activities so as to minimize the risk of stoppage due to disasters. But since there is no guarantee that the preventive measures are sufficient, because such undesirable event can occur, then alternative operating strategies must be already defined for vital activities, which should be re-located at another facility at a cautious distance from the affected site, so that the organization can continue to perform such vital activities as soon as possible.

There isn’t necessarily forewarning of severe incidents. Therefore, the organisation must have its continuity protocols or plans properly documented and updated to let staff know how to act and use alternate strategies during the incident. Such protocols could become dead letter if they are not drilled and practised. Drills will ensure a swift and efficient response of the organization to disaster.

However, such major events that may affect operations do not frequently occur to organizations. Therefore, it is necessary to constantly remind their authorities and staff in general that such events can actually happen and that it is important to be prepared.

Permanent preparedness involves defining and enforcing roles that will be assigned to authorities, designating a Coordinator of Continuity, headquarters, teams to recover vital activities and staff. Through the Coordinator of Continuity, the authorities of the organization must demand and monitor that such roles are being complied with and improved every year.

The remarks made above are based on best practices and international standards such as ISO 22301 on continuity of business and operations, as approved in 2012. For some years now, several organizations in our region have applied those standards to varying extents.
The publication Disaster Recovery Journal en Español (DRJ) has organized various events and forums publicizing several examples of public and private sector companies in Latin America and the Caribbean that are applying such best practices. Since they are regulated, the financial and insurance sectors have made great strides as regards the implementation of programmes on continuity of business and operations. The telecommunications, electricity and gas sectors have also progressed but to a lesser degree. Oil and extractive industries in general, due to their operational risks, have also implemented such practices. Other organizations have also followed suit because of corporate requirements.

These concepts are applicable to any organization, including society in general, which must be able to identify its key activities to protect itself against disruptive events, to ensure the lives of citizens, housing, basic services, health and financing, among others. Therefore, municipalities, local, regional and national governments should know and apply these practices.

Collaboration between the public and private sectors does not only occur through the voluntary collaboration of the private sector with the public sector, but also through the commitment to the recovery and continuity of operations of those private companies that provide vital public services to people, under the leadership of the public sector.

I. INTRODUCTION

The following document contains the results of a study carried out by the Permanent Secretariat of the Latin American and Caribbean Economic System (SELA) in order to make specific recommendations to private enterprises and public institutions on the decisions, policies, strategies and contingency plans that must be undertaken before, during and after the occurrence of a disaster, with the purpose of ensuring continuity of their business and operations.

Before going into further details, it is important to understand that any organization needs to design, implement and maintain a series of initiatives and procedures, and to create an entire organizational culture to face major events that might disrupt their operations. We live in a region where natural disasters are frequent. Natural disasters include earthquakes, tsunamis, floods, landslides, pandemics and fires, to name a few. In addition, there can be other types of events, not of a natural kind but man-made, which could also paralyze operations, such as: terrorist attacks, sabotages, explosion and theft of information. Moreover, some technology-related events can affect specific industrial sectors, such as: system failures and obsolescence of equipment, among others.

In addition to continuity of operations, there are many ways to protect an organization against the occurrence of a major event or disruptive incident that may paralyze its activities. One of the most common protection measures is to count on appropriate insurance for those goods that can be affected and in some sectors even an insurance for lost profits. Although they seem to be almost absolute measures, in the case of the private sector, they do not include the massive loss of key customers for failing to serve them; and in the case of public institutions they do not cover image deterioration or political costs. In this connection, continuity of business and operations goes a step beyond the mere protection of assets or revenues of an organization, seeking to achieve its survival despite the adverse situations that may arise.
It should be kept in mind that continuity of business and operations will be resorted to only in rare, extreme or infrequent cases. For this reason, we should ensure the smallest possible cost for deploying and maintaining a continuity plan for the organization, but without putting it at the risk of not being adequately protected. To better understand such balance between costs and risks, let’s use the following example: If a person is hurt during an incident, he or she will not be able to continue living if the injury occurs in any vital organ, but any other type of injury will allow for a longer life span, so that the person can receive help and eventually recover. In the case of an organization, the situation is similar. There are key activities that the organization cannot afford to be affected because they can compromise the life of the organization, while there are other activities that, in case they are affected, can wait until help arrives and operations are recovered back to normal. The investment made by a company in continuity plans should focus mainly on those critical activities, which are known as urgent.

II. PRELIMINARY DEFINITIONS

Continuity of business and operations is a recent discipline and its terminology is not completely uniform. Thus it is necessary to resort to international standards that allow for creating a common language.¹

Continuity of business and operations. Capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident.

Continuity plan. Documented procedures that guide organizations to respond, recover, resume, and restore to a pre-defined level of operation following disruption. There can be one or more documents and they can receive different names (including contingency plan) according to the size, sector or type of organization.

Continuity programme. Ongoing management and governance process supported by top management and appropriately resourced to implement and maintain business and operations continuity management.

Continuity management system. Set of interrelated management systems of an organization to establish, implement, operate, monitor and maintain policies, as well as improve the continuity of business and operations.

Incident (continuity). Situation that might be, or could lead to, a disruption, loss, emergency or crisis. It is important to point out that this definition of incident must be understood from the perspective of continuity of business and operations, and may be different from the definition of incidents within the context of information technologies, risks or safety.

Crisis. Situation with a high level of uncertainty that disrupts key business activities and/or the credibility of the organization, and which requires immediate action.

¹ All definitions are based on the International standard ISO 22301-2012.
III. WHY IS CONTINUITY OF BUSINESS AND OPERATIONS IMPORTANT FOR LATIN AMERICA AND THE CARIBBEAN?

Studies conducted by different organizations on disaster risks in Latin America and the Caribbean show that our region is vulnerable to various threats.

As mentioned in the technical document prepared in 2012 by the United Nations Development Programme (UNDP) after the VI Summit of the Americas, a total of 98 major climatic and geophysical disasters occurred in Latin America and the Caribbean in 2010, with damage exceeding US$ 49.188 billion. This reveals a regional and global trend entailing a worrying five-fold increase in disastrous events from 1975 to 2005.”

Even though the studies on disaster risk reduction are focused on highlighting vulnerabilities for populations, the threats identified and studied can be taken as references that can be applied to public or private organizations.

A threat is defined as the potential cause of an unwanted incident, which in case it occurs may result in damage to persons, an organization or a system.\(^3\)

A company or organization may not have control over the threat, it exists by itself. What the organization can do is to establish protective measures so that the threat causes the minimum possible damage in case it materializes.

Continuity of business and operations is aimed at protecting critical or urgent activities and ensure their recovery. Even though activities could be interrupted due to the disruptive event, the organization should be able to continue carrying out such activities. Hence the importance of continuity.

1. Natural threats

Natural threats or hazards occur without human intervention and are attributable to a physical phenomenon of natural origin. The National Fire Protection Association (NFPA) lists these possible threats in their 1600 standard for the year 2010\(^4\) as follows:

a) Geological hazards: Earthquakes, seismic movements; tsunamis, volcano eruptions; landslides, mudslides, subsidence; glaciers and icebergs.

b) Meteorological hazards: Floods, flash floods; droughts, famines; fires; snow, ice, hailstorms and avalanches; hurricanes, tropical storms, tornados, sandstorms; extreme temperatures (hot or cold); rays; geomagnetic storms.

c) Biological hazards: Emerging diseases with impact on human beings or animals (plague, smallpox, anthrax, the West Nile virus, foot and mouth disease, severe acute respiratory syndrome, pandemic diseases, mad cow disease); infestation or damage by insects or animals (such as dengue).

For an organization, the likelihood of suffering any of the threats mentioned above depends on its geographic location. Southernmost in our region, in Argentina and Chile, there are many snowy and even icy areas where avalanches are very likely. A long desert...


\(^3\) Definition taken from ISO 22300:2012.

strip stretches from northern Chile to southern Peru, but torrential rains can cause severe
damage in other areas of those countries. The vast majority of the Latin American and
Caribbean countries have coasts where tsunamis can occur.

Central American and Caribbean countries are subject to cyclone seasons. The Andean
mountain range has active volcanoes. The extensive Amazon jungle in South America
and the tropical climate in many Central America and Caribbean countries make them
prone to suffer heavy rains, floods and landslides - not to mention climate phenomena
such as “El Niño” or “La Niña”. The region has also been hit by mass contagions by the
avian flu and the H1N1 flu, the latter of which led to a general quarantine in Mexico City.
Remote areas in the region are plagued by endemic diseases such as the dengue fever,
which is still an uncontrolled problem.

The shortcomings as regards disaster prevention are another factor that increases both
the occurrence of such threats and the vulnerability of organizations. According to the
technical document prepared by the UNDP for the VI Summit of the Americas, “the risks of
mortality and economic losses due to floods and hurricanes have decreased at the
global level, but in the Americas they continue to increase. The best strategy for disaster
risk reduction is to reduce vulnerability of people and economies vis-à-vis different threats.
For this purpose, it is necessary to address the factors causing risks, such as poorly
managed urban development, environmental degradation and poverty, which generate
vulnerability.”

There are many and quite different studies aimed at gaining knowledge about areas of
risk and potential disasters in the region, but it is complex to get reliable information. The
national institutions responsible for disaster risk prevention are good sources of information.
We also count on the Regional Disaster Information Centre (CRID), which was created to
join efforts and collect and disseminate reliable information on disasters in Latin America
and the Caribbean. National universities are another source of information.

2. Man-made threats

In its standard 1600 of year 2010, the National Fire Protection Association (NFPA)
classifies possible threats or hazards as follows:

a) Accidental hazards: spillages or leaks of hazardous materials; explosion, fire;
transportation accident; building or structure collapse; failure in public service
networks of electricity, gas, water or other similar; shortage of fuels or resources;
water or air contamination; levee or dam structural failure; economic depression,
inflation, financial crisis; disruption in communication systems (voice and data);
disinformation.

b) Intentional risks: terrorism (in its various forms: explosions, chemical, biological,
radiological, nuclear or cyber-terrorism); sabotage; social unrest, protests, hysteria,
riots; war; insurrection; misinformation or rumours; criminal activity (vandalism, theft,
fire, fraud, embezzlement, theft of data); electromagnetic pulses; violation of
physical security or information; violence in work places, universities or colleges;
pollution or defective product; harassment; discrimination.

In the case of accidental risks, these threats will be more likely depending on the type of
sector, industry or economic activity of the organization. There might be even new threats
to specific economic activities which are not listed yet. According to ECLAC’s Statistical

5 Regional Disaster Information Centre (CRID) - http://www.cridlac.org/.
Yearbook 2012,⁶ the economic activities considered for Latin America and the Caribbean are as follows: agriculture, livestock, hunting, forestry and fishing; mining and quarrying; manufacturing industries; supply of electricity, gas and water; construction; wholesale and retail trade, repair of goods, hotels and restaurants; transport, storage and communications; financial intermediation, real estate, business and rental activities; public administration, defence, compulsory social security, education, health and social services, and other community, social and personal services.

In many of the countries in the region there is contamination due to illegal extractive activities, pollution-related accidents in seas and rivers, interruptions in telephony and Internet public systems, frequent power outages, serious inflation problems, as well as rumours about bankruptcies of banks or financial institutions. However, while the study focuses on Latin America and the Caribbean, these threats should not be viewed only from the regional geographic context, but from a global standpoint of the sectors or economic activities the organizations operate, in order to identify other threats that might be emerging in other regions of the world or could have a local scope.

In the case of intentional risks, threats are more related to social problems, which are very frequent in our region. The Report on Citizen Security Statistics for the Americas of the OAS Hemispheric Security Observatory, by Alertamerica.org,⁷ provides statistics by country on the main social violence factors: killings and violent deaths, weapon trafficking, drug consumption and trafficking, sexual crimes and human trafficking. Many of these crimes are associated with increasingly growing organized crime networks.

3. Threats caused by technological failures for reasons not attributable to nature or man

The National Fire Protection Association (NFPA) classifies these possible threats in its standard 1600 for the year 2010 as follows: failures in central server computers, software or applications, failures in ancillary support equipment; damages in telecommunications, energy or electricity outages, or failures in public services.

Even though there are no official statistics about technological failures in enterprises in our region, we should look at statistics on the use of Internet in countries of the region. According to statistics of the International Telecommunication Union (ITU),⁸ in terms of Internet access in households in Latin America and the Caribbean Brazil holds the first place, followed by Chile, Argentina, Costa Rica, Uruguay, Colombia, Mexico and Panama, which are above the average in the region.

IV. APPLICABLE METHODOLOGICAL STANDARDS AND REGULATIONS

The continuity of the business and operations has been established as a discipline on the basis of the use of technology by organizations. When operations of companies were conducted manually, processes were slow and there wasn't a high demand for services. As companies began to incorporate information technology in their operations, productivity started to increase and processes accelerated. By the 1970s, such advances began to make it necessary for companies to “recover” quickly after any system failure.

---

⁶ Statistical Yearbook for Latin America and the Caribbean 2012, by the United Nations Economic Commission for Latin America and the Caribbean (ECLAC).
At present, this is still a very widespread notion since companies think that continuity of business and operations is strictly linked to information systems.

In the 1980s and 1990s, companies realized that the failure of information systems was not only cause for a disruption of operations, but that there were also other factors such as the lack of personnel, physical infrastructure or providers which could also disrupt operations. Therefore, other disciplines - such as physical security of staff, management of incidents, risk assessments and insurance - became necessary for continuity of business and operations.

In the 1990s, reputation was considered to be an important aspect that should be safeguarded, as it may also interrupt or seriously affect operations. Thus, the discipline of image management during crises started to form part of continuity of business and operations.

Over the years, the concept of continuity of business operations evolved and turned into an ongoing process. The term business continuity programme became more common to denote the need for something maintained on a permanent basis and updated through time. This led to awareness-raising and improvement of those skills considered to be key elements to ensure the success of continuity of business and operations.

During the second half of the 2000s, national and international standards on the subject were formalized. Continuity of business and operations started to be interpreted as a management system (similar to quality control systems) and organizations started to be granted certifications as regards compliance with such standards.

1. DRII (Disaster Recovery Institute International)
The DRII was founded in 1988 in the United States. It provides best practices, training and certification for professionals specialized in business continuity. Initially, it provided eight best practices but later on they were expanded to ten. According to its latest update in May 2013, they can be summarized as follows:

   a) Programme start-up and management
   b) Risk evaluation and control
   c) Business impact analysis
   d) Business continuity strategies
   e) Response and emergency operations
   f) Business continuity plans
   g) Awareness raising and training programmes
   h) Drilling, auditing and maintaining the business continuity plan
   i) Communications during crises
   j) Coordination with external public agencies

2. BCI (Business Continuity Institute)
The BCI was established in 1994 in England. It provides best practices, training and certification for professionals specialized in business continuity. It has six best practice guides. According to its latest update in May 2013, they can be summarized as follows:

   a) Business continuity plan development
   b) Business continuity plan training and exercise
   c) Business continuity plan management
   d) Business continuity plan audit
   e) Business continuity plan update
   f) Business continuity plan coordination with external agencies

---

10  http://www.thebci.org/.
PP1: Programme policy and management
PP2: Incorporating continuity of business (culture)
PP3: Analysis
- Business impact analysis
- Threat analysis
PP4: Design
- Strategies and tactics for continuity and recovery
- Measures for threat mitigation
- Structure for response to incidents
PP5: Implementation
- Business Continuity Plan
- Development and management of plans
PP6: Validation
- Development of a Drilling Programme
- Maintenance
- Revision

3. ANSI/ASIS SPC.1

ASIS International\textsuperscript{11} was founded in 1955. It has over 230 Chapters around the world. It is made up by professionals specialized in security, specifically protection of assets, including people, properties and/or information. In 2009, it published standard SPC.1, recognized by ANSI to certify organizations in business continuity. The most important sections can be summarized as follows:

Section 1: Scope of the standard
Section 2: Regulation references
Section 3: Terms and definitions
Section 4: Requirements for organizational resilience or system management
- Planning
  - Evaluation of risks and analysis of impact
- Implementation and operation
  - Resources, roles, responsibilities and authorities
  - Competence, training and awareness
  - Documents and control
  - Prevention, preparedness and response to incidents
- Evaluation
  - Evaluation, measurement and monitoring
  - Drilling and testing
  - Non-conformity, and corrective and preventive actions
  - Control of registers
  - Internal audits
- Management revision
  - Revision inputs and outputs
  - Maintenance
  - Permanent improvement

4. **NFPA 1600**

NFPA \(^{12}\) was founded in 1896. Its main objective is to prevent fires and other risks that may affect security and quality of life. The Association has developed, published and distributed over 300 codes and standards. Since 1995, it has published six editions of its standard 1600, with the latest one being the 2013 review: “Standard on disaster / Emergency Management and Business Continuity Programs.”

Following is a summary of the most important sections of that standard:

- **Chapter 1: Management (scope, purpose and implementation)**
- **Chapter 2: Reference publications**
- **Chapter 3: Definitions**
- **Chapter 4: Programme Management**
  - Leadership and commitment, important roles, register management
- **Chapter 5: Planning**
  - Risk evaluation
  - Business impact analysis
- **Chapter 6: Implementation**
  - Communications during crises and public information
  - Alert and notification communications
  - Response to incidents
  - Emergency response and operations
  - Business continuity and recovery
  - Support and assistance to employees
- **Chapter 7: Training and Education**
- **Chapter 8: Drilling and testing**
- **Chapter 9: Programme improvement and maintenance**

5. **ISO 22301**

ISO (the International Organization for Standardization) is a global federation of national organizations for standardization (ISO members). The ISO technical committees are in charge of preparing the international standards. Standard ISO 22301, Societal security - Business continuity management systems, was issued in May 2012. Following is a summary of the standard:

- **0. Introduction**
- **1. Scope**
- **2. Reference to norms**
- **3. Terms and definitions**
- **4. Context of the organization**
  - Interested parties
  - Scope of business continuity
- **5. Leadership**
  - Top management commitment
  - Business continuity policy
  - Roles and responsibilities in business continuity
- **6. Planning**

• Objectives of business continuity and plans to accomplish them

7. Support
• Resources
• Competences
• Awareness raising
• Communications
• Documents

8. Operation
• Planning and operational control
• Business impact analysis (BIA) and risk evaluation
• Business continuity strategy
• Establishing and implementing business continuity procedures
• Drilling and testing

9. Evaluation of performance
• Monitoring, measurement, analysis and evaluation
• Internal audit
• Management revision

10. Permanent improvement
• Non-conformity and corrective actions
• Permanent improvement

V. METHODOLOGY APPLIED TO THE PUBLIC AND PRIVATE SECTORS

Taking into consideration the aforementioned standards and the experiences in applying them in various private and public organizations, the following guidelines for adopting the methodology to implement and maintain programmes for continuity of business and operations are presented below. Many of them are currently being implemented by organizations in our region.

1. Empowering and governing continuity of business and operations

Continuity of business and operations is a great challenge for both private and public organizations in our region. Authorities\(^\text{13}\) are usually concerned about the pressure to perform daily activities and comply with the objectives of the organization. Even though authorities are aware of the importance of implementing continuity of operations, sometimes little is done in this regard or initiatives are poor.

In addition, continuity of business and operations is often confused with just having a document outlining a contingency plan, which another very common mistake of authorities. The contingency or continuity plan should be another component of a permanent ongoing process in the organization called business continuity and operations management.

Achieving appropriate empowerment according to the hierarchy level (Board of Directors, authority, headquarters and experts in the activities of the organization, among others) is one of the first objectives for the purpose of governing the permanent process of continuity of business and operations. Chart 1 outlines such roles.

\(^\text{13}\) In this context, the term “authorities” applies to both the public and the private sectors. In the latter sector, “authorities” can also be referred to as “Direction” or “Senior or High-Level Management.”
Roles of instances participating in continuity of business

**Board of Directors.** It is responsible for continuity of business and operations of the organization. It entrusts this task to the highest-ranking authority within the organization - e.g. a general manager - and demands accountability as regards this issue at the end of the time period it deems convenient. The Board of Directors is also responsible for approving the investments in resources to implement continuity of business and operations, as deemed necessary. The Board should also make sure that continuity of business and operations actually ensures the continuity and survival of the strategic objectives of the organization, by checking the scope of its application within the organization.

**General Management (or equivalent authority).** It is responsible for implementing continuity of business and operations in the organization. For this purpose, it must implement and review on a permanent basis a management process for continuity of business and operations by assigning it to one single person with the proper hierarchy and the necessary skills to carry out such work. The General Management is also responsible for approving the investments in resources to implement continuity of business and operations, as deemed necessary.

The organization’s authorities under the leadership of the general management should establish, maintain and practice a system to respond to the incidents and crises that may arise at the operational level, which might cause emergencies or damage reputation. For this purpose, they must designate a response team and assign roles to manage the incidents and crises, and provide it with the necessary resources to create skills.

**General coordinator of continuity of business and operations.** He/she is responsible for implementing and maintaining the continuity of business and operations programme and report on the progress to the General Management (or equivalent authority). According to the size of the organization, this function could be shared (for small or medium-sized organizations) or exclusive (for large organizations). The implementation of the continuity programme should follow a methodological order in accordance with one or several of...
the aforementioned international standards and must involve the Heads of area departments or process leaders.

The general coordinator of continuity of operations must have the necessary skills and competences, credentials on specialised training, and will participate in forums and conferences on business continuity at the local, regional and international levels.

**Heads of area departments or process leaders.** They are responsible for implementing and maintaining continuity of business and operations in its scope and responsibility for operations. For this purpose, they shall designate a head of operational continuity of his area or process, with the necessary authority to coordinate internal efforts in conjunction with and under the leadership of the general coordinator of continuity of business and operations.

In the case of the departments supporting operations, such as Security, Human Resources, General Services, Information Technologies or others, they should lead responses to the most common incidents and events within their scope of action (pandemics, fires, earthquakes, and computer failures, among others) and support response to those incidents that might disrupt critical activities of the organization.

The Heads of areas and process leaders must have the required skills and competences, credentials on specialised training in leadership, continuity of business and operations.

**Members of planning and/or response teams.** They are usually operational staff at the command of the Heads of area, who provide expertise and knowledge on recovery needs and priorities during the process of implementation and maintenance of the continuity of business and operations. During a drilling or an actual incident they participate in response to the incident by applying continuity strategies and plans outlined during the planning stage.

The members of the planning and/or response teams must have the required skills and competences, credentials on specialised training in issues related to continuity of business and operations, knowledge of their plans as well as experience in responding to incidents by applying their plans.

**General staff.** Operational staff at the command of the Heads of area during the process of implementation and maintenance of continuity of business and operations. They provide expert knowledge about the priorities and needs for recovery, and during a drilling or an actual incident they participate in response to incidents by applying continuity strategies and plans outlines during the planning stage.

In addition to the responsibilities described in the organizational structure, organizations also need to define a policy of continuity of business and operations. Such policy makes reference to the reach at the level of services, areas or localities that are considered to be within the scope of the continuity programme. Therefore, all those activities not foreseen within this scope are not deemed to be urgent in terms of recovery. Thus, there can be enough time to restore such non-urgent activities when an incident occurs without the need to plan something in advance.

Governance is also executed through the monitoring and review meetings held by the authority, which are recommended to be carried out every two or three months. If such meetings are not so regular, the problems that may arise during the implementation or maintenance stages of the continuity programme are not likely to be solved.
Internal audit also plays an important role in governance of continuity of business and operations. The audit must ensure that the continuity process is executed in accordance with the instructions given by the Board of Directors and the best professional practices in this regard. The auditor must be independent from the organisation and must have appropriate skills and competences to propose improvements in line with the objectives of the continuity, without derailing from such objectives.

2. Identifying priority and urgent recovery activities

Identifying priority activities is aimed at establishing the scope of preparedness for a disruptive incident; identifying the order and time frames for recovery activities and their connections; identifying the minimum resources needed at the time of the disruptive incident; and providing the basis to propose cost-effective strategic options for continuity or recovery.

The scope of continuity of business and operations is important in order to restrict the focus of the organization’s efforts on those activities that must be really be urgently recovered. A severe disruptive incident does not occur frequently and many organizations are not very likely to suffer it.

This does not mean that no actions will be taken to protect those activities outside the scope of continuity. Comprehensive risk management, whose scope goes beyond great impact events, does identify and implement appropriate security and protection measures for the organization’s activities. This reinforces the notion that continuity is an additional control to those foreseen in risk management to protect the organization. However, from the standpoint of continuity, not all activities should be considered to be within its scope; and for those organizations implementing continuity of business or operations it is very important to remain within the scope of continuity.

There are several ways to determine the scope of business continuity, depending on the type of organization, industry or sector. The most recommended way is to establish the scope according to the services provided by the organization. Thus, in case of a disruptive incident, the main question is: Which minimum services should continue to be provided and which are not likely to continue?

Once the scope of services has been established, it is easier to identify the geographical scope to be considered, in case the organization has various offices or facilities offering the services within the scope. It is also easier to establish the scope for processes or activities to provide priority services, and therefore the scope at the level of departments or functional units within the organization.

A common mistake among officials responsible for implementing continuity of business and operations is to establish a very broad scope for continuity of business. This forces the organization to make huge efforts in terms of trained personnel, time and costly investments in alternate operational options in case of disruptive incidents, which might be frequent but rarely affect the organization.

In order to determine time frames for recovery of activities, it is necessary to first establish non-tolerance thresholds for the organization. This means the level of damage that the organization could not bear in each of the categories that can potentially suffer impacts: economic or financial (how much money committed is intolerable for the organization?), involvement of users or customers (number of customers or users that the organization

14 Either services or products.
cannot tolerate to be affected?), legal or regulatory (which level of sanctions or legal proceedings for non-compliance is intolerable for the organization?), environmental (which level of environmental damage is intolerable for the organization?), personal security (which level of damage to people is intolerable for the organization?)

The authorities should provide the answers to these questions, considering the vision and perception that they would have during a disruptive event as stakeholders of the organization. Stakeholders of an organization include: users or clients, owners or shareholders, public authorities and regulatory agencies, business partners, organization staff, and community or town where the organization operates, among others. The answers should help define non-tolerable thresholds\(^{15}\) for the organization.

The next step is to estimate the Maximum Tolerable Period of Disruption (MTPD), which should respond to the following question: in case of failure of service / locality / department / process / activity (it can be any of them, depending on priorities), how long will it take before non-tolerable thresholds are reached? Responses can vary: does not apply, minutes, hours, days, weeks or months.

To answer that question, it is also necessary to consider the most stressing scenario for the element under analysis and the most stressing moment. This is aimed at determining whether the most urgent response was given when the disruptive incident affected only the organization or massively affected other organizations; and at determining whether the greatest involvement occurs on any specific date of the week, month or year.

The Maximum Tolerable Period of Disruption (MTPD) must be defined by the shortest time for response given to the different types of impact of non-tolerable thresholds and must always will be estimated by considering the worst-case scenario which is really the most stressful for the organization, and not necessarily causing the greatest damage to the community. Continuity is aimed at protecting the organization from the worst-case scenario, not against the most likely one.

**CHART 2**

Matrix to estimate MTPDs

<table>
<thead>
<tr>
<th>Service or Activity</th>
<th>How long will it take to reach non-tolerable thresholds?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Critical seasonality</td>
</tr>
<tr>
<td>Service 1</td>
<td>...</td>
</tr>
<tr>
<td>Activity 1</td>
<td>...</td>
</tr>
</tbody>
</table>

After the MTPD has been defined, a Recovery Time Objective (RTO) must be estimated. RTO is a value expressed in time, between zero and the MTPD. The closer to zero it is, the costlier the strategic option to continue operating will be. On the other hand, the closer to

\(^{15}\) Non-tolerable thresholds are not necessarily unique values. They can be established in different ways: Is it intolerable not to offer the service to a thousand clients, not to provide the service to a certain company, or not to provide the service to ten strategic clients?
the MTPD it is, the riskier it will be. The best balance between cost and risk will be the most appropriate RTO.

The dependence relations between services/facilities/business units/process/activities should also be analyzed in order to identify or correct MTPDs and RTOs of depending parties.

This process of estimating MTPDs and RTOs can function at different levels: at the strategic level or by services (plants or functional units) and at an operational level, by activity (or process). Estimating MTPDs and RTOs must be a permanent job in the organization because of the changes that they may have. The emergence of new services (or new facilities or plants, and new functional units) and new activities (or processes) will make it necessary to reevaluate emergency recovery priorities. A similar situation could occur if a service (or plant or functional unit) gains more relevance than another. If recovery priorities are not updated in a timely manner, a disruptive incident could occur in which decisions will be incorrect because the information available is outdated.

Once RTOs have been defined, services (plants or functional units) or activities (or processes) are grouped according to RTOs, creating windows for recovery in time, i.e. services or activities that are recovered in zero time (if any), in hours (if any), in days (can be one, two or three days, or just days), those which are recovered within weeks (can be one or two weeks, or just weeks), and those which take one month or longer to be recovered.

Once the recovery time windows are established, it is necessary to identify the minimum resources needed during the disruptive incident. Such resources can be as follows: 16 people: staff, transportation and communications; infrastructure: buildings, public services; equipment: labour environments, equipment, supplies or consumables; information technology: computer services, information and data; finance: financial viability, regulation: regulatory aspects to comply; vendors: partners and suppliers; stakeholders: customers to be contacted, authorities to be contacted and community in general to be contacted.

- Staff resources are identified by taking into account the necessary minimum profiles to continue operating services/activities for each recovery window, even if organization staff complies with the profiles properly.

- Transport resources are identified by considering the mobile facilities that the organization can provide to staff during the disruptive incident.

- Communications resources are identified by considering communication capabilities among the organization staff, which may be available during the disruptive incident.

- Facility resources or buildings are identified by considering the alternatives for labour places or other offices or plants from which operations could continue during the disruptive incident.

- Public services resources are identified by considering alternatives for the provision of electricity, water and drainage, gas and phone service, which may be used during the disruptive incident.

16 According to ISO 22301.
- Labour environments and equipment resources are determined by considering the alternatives for operation in other labour environments or with alternative equipment located elsewhere, which could be used during the disruptive incident.

- Inputs and consumables resources are identified by considering the alternative materials (or raw material), inputs or other perishable or durable consumables, which need to be considered at the time of the disruptive incident and the locations where they are.

- Information technology resources (systems, information, and data) are identified by considering IT services to be used at the time of the disruptive incident, as well as the information or other necessary data for the service or activity analyzed.

- Financial viability resources are identified by considering the needs for available financial resources in cash or some other type to deal with the disruptive incident.

- Regulation resources are identified by considering the legal or regulatory obligations that should continue to be complied with during the disruptive incident, and if there are alternatives in case they cannot be met.

- Providers and business partners are identified by considering those who support critical services, contacts and other alternate suppliers in case they are also affected by the disruptive incident.

Other stakeholders such as customers, public authorities and community are identified by considering the contacts that need to be made in case of a disruptive event.

This information obtained at the level of resources is the basis for identifying optional strategies for continuity and recovery, as well as the corresponding budget estimation for implementation.

3. Protecting most urgent activities

Continuity of operations of the most urgent activities must be ensured not only by identifying optional strategies after the disruptive incident, but also by adopting preventive options before the disruptive incident. Thus, continuity seeks to assess whether protection and security measures existing in the facilities where the urgent activities of the organization are carried out are sufficient or if they need to be improved, or even if new safety and security measures are required.

To assess if protection measures are sufficient, different methods can be used. The most recommended one is the risk analysis proposed in ISO 31000, which assesses risk as a combination of probability and impact of a risk event.

To determine the risk events that may be of interest for continuity, it is necessary to focus on the consequences of the threats that could create a disruptive event due to lack of the resources needed to operate. Examples of risk events to be considered for continuity could be: impact on staff in case of an earthquake; impact on building in case of an earthquake; impact on suppliers in case of pandemics.

It is also necessary to define the threats that the organization may be exposed to and are likely to occur, which are called dangers. These hazards should be identified on the basis of the most global threats as compared to the more specific threats applicable to the
organization. For example, if the organization is headquartered in the Caribbean, the hurricane season is an applicable threat, i.e. a danger, but in the case of South America, hurricanes would not be an applicable threat. Nevertheless, a pandemic, even though it starts in China, due to its global expansion, is a threat applicable both to the Caribbean and South America. If we limit the scope of threats to more local issues, crime, civil protests, and other examples of threats are likely to be considered hazards in some cities in our region more than in others.

Risk analysis in continuity of business and operations aims to identify new prevention options or improve already existing security measures for each of the risk events taken into consideration. The first step is to identify existing prevention and safety measures in the organization. Security measures will be related to staff safety, physical infrastructure, labour environments, inputs and consumables, information systems, suppliers, and each one of the other resources associated with continuity that are relevant for the organization.

As noted earlier, the risk is estimated by combining probability and impact through qualitative or quantitative methods. The problem of quantitative methods is that they need historical data as well as complex statistical formulas for making projections on the occurrence of disruptive incidents stemming from threats. Moreover, in many cases, confusion emerges that continuity aims at proposing preventive measures instead of making accurate mathematic estimations of the probabilities and therefore risks. Because of this, some organizations decide to estimate the level of qualitative risks, as follows:

- The risk matrix is defined by identifying probability and impact scales. If there is a Risk Management Department in the organization, it is most advisable to adopt the scale already in use, although the meaning of scales may be different in the case of continuity (an issue that will be addressed later on). If the organization does not have a risk matrix, it should define one.

**CHART 3**

**Risk matrix, five by five scale**

<table>
<thead>
<tr>
<th>Impact Probability</th>
<th>Very low</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
<th>Very high</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very high</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Extreme</td>
</tr>
<tr>
<td>High</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>High</td>
</tr>
<tr>
<td>Medium</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Medium</td>
</tr>
<tr>
<td>Low</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>Very low</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The scale of the risk matrix may be three by three, four by four, or five by five, or a different combination depending on the best way for the organization to assess risks.

The risk level is estimated by combining probability and impact. Chart 3 shows four risk levels: extreme (represented in red background, and its treatment must be immediate), high (orange background, and treatment should in the short term or medium term), medium (yellow background, and treatment should be in the long term), and low (green background, and it is not necessary to treat the risk).

The scale of probability is defined on the basis of the incidence of the risk event through time, considering the context applicable to the organization. Examples of scales of probability are: very high (the incident has occurred at least once a year in the past five years), high (it has occurred at least once every five years in the past 25 years), average (it has occurred at least once every 10 years in the past 50 years), low (it occurs at least once every 25 years) and very low (it occurs in periods of over 25 years).

The scale of impact is defined on the basis of the level of damage that the incident could cause to the organization. In terms of continuity, this refers to damage as per the time for which the incident produces unavailability or interruption. Where the most urgent activities are carried out the highest impact will take a matter of hours; where less urgent activities are conducted the highest impact will be a matter of days or weeks.

Having defined the risk event, the risk matrix with its corresponding scales of probability, impact and risk, as well as existing controls, the organization should proceed to estimate the probability of occurrence of the risk event and its impact, calling on those experts within the organization who know about the threats and the effectiveness of implemented controls, so as to determine the resulting risk level on the basis of their expert opinion.

Wherever they determine that there are extreme, high or medium risks, it is necessary to implement new preventive measures or controls, or in any case improve existing ones, in order to help reduce risk levels based on the suggestions of the experts. The priorities in implementing new measures or improving current ones will depend on the risk level, i.e. first of all extreme risks should be prevented, secondly high risks should be addressed, and finally medium risks should be dealt with.

4. Establishing strategies for continuity and recovery of activities

Strategies may be preventive or reactive. The preventive options were identified by using the risk analysis carried out as regards the risk events that the organization has assessed. Its main objective is to mitigate or reduce vulnerability of services and/or most urgent activities of the organization. The reactive options will be identified from the results of the priorities attached to services and/or activities in accordance with the MTTRs and RTOs and, above all, taking into account the minimum necessary resources identified.

The strategic options should also consider the cost of their implementation and must comply with the established RTOs. If it is necessary to adjust the value of the RTO for the sake of technical feasibility or due to very high costs, then it should be done, previously checking the dependencies of such activity and redefining their new RTOs with such dependencies.
The options can range from the most demanding and costly to the less demanding and more economic, thereby defining how “hot” or “cold” the chosen alternative should be. The “hottest” alternatives include dividing operations into two or more parts and locate those parts safely, outside the scope of greatest geographical risks, and having an empty facility that can be occupied immediately in case of an event. “Warm” options include having portable systems that can be moved to the places of operation where a service has been affected or a space in use that can be emptied for use to conduct the most urgent activities. The “coldest” alternatives include not having almost anything pre-assembled, doing nothing at the moment of the event, waiting for it to finish and reacting afterwards.

All the options can be implemented, maintained and operated by the organization itself or by a third party who provides such options.

The importance of selecting the right strategy or set of strategies is not to risk the recovery of the business, i.e. to comply with the established RTOs, and not to risk the MTPD in an attempt to save money. The organization could use a combination of options. For example, for services or activities that can never stop even when a disruptive incident occurs, the option of splitting operations will be adequate, despite the cost. For those activities that can wait for some hours to be restored, the option of having a facility ready to transport the staff will be adequate. If the activity can wait for some days to be restored a movable system may be appropriate. However, if time for recovery extends for some hours, the strategy of immediate delivery should not be used.
### CHART 4
**Cost-benefit options for continuity strategies**

<table>
<thead>
<tr>
<th>Max</th>
<th><strong>Option of duplicating or replicating the primary operation while maintaining primary and alternate operations in function at the same time</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Option of maintaining an unused alternate operation and waiting to be used in case the disruptive incident occurs</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Option of maintaining an alternate operation ready to operate, which will be moved to the scene of the incident to replace affected infrastructure</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Option of maintaining an immediate delivery mechanism with a provider that will replace the affected operation</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Option of maintaining a reciprocal agreement with another related organization</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Option of having an alternate operation ready to set up in case of an incident</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Option of repairing damages more quickly</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Not doing anything for the time being</strong></td>
</tr>
</tbody>
</table>

### Level of investment in the recovery strategy in anticipation of the disruptive incident

- Some examples of staff recovery options include: defining a plan of succession establishing primary and alternate officials; policies to prohibit travel of primary and alternate staff at the same time and using the same medium; prohibition to take vacation at the same time; implementation of health programmes and emotional control of the personnel identified as critical.

- Examples of physical infrastructure recovery options include: defining alternate places for operations with guaranteed supply of public services from different
Examples of recovery options for materials, supplies or consumables include: creating small inventories at strategic locations; establishing inventories provision agreements with several suppliers; establish reciprocal agreements with similar organizations to provide mutual assistance in case of a disruptive event.

- Examples of equipment recovery options include: renewing equipment and keeping old ones for spare parts, maintaining operating obsolete facilities at a minimum level of operation; having transportable machinery (if possible) to take to the affected site; or having identified less critical service equipment that can be removed and taken to the affected site and assemble it there.

- Examples of computer systems recovery options include: replicating the computer centre in an alternate place either completely or partly in accordance with what has been identified as the most critical systems; outsourcing computer service and upload it to the “cloud”; perform backups and restore them whenever necessary.

- Examples of financial feasibility recovery options include: maintaining contingent credit lines to meet needs at the time of the incident; keeping cash available for access and meeting needs for cash during the incident; establishing procedures for registration and control of damages and expenses associated with the incident for later claims to the insurer; having deferred payment agreements with providers in case of major incidents.

- Examples of suppliers recovery options include: having more than one supplier for the provision of goods or services, and if it is not possible, establishing joint procedures to respond to disruptive incidents; measure the level of maturity in accordance with the BCMM\textsuperscript{17} of the supplier to require the adequate level of preparedness vis-à-vis disruptive events through time. Another example of options for recovery of customer relations includes having procedures for communications during crises, considering possible scenarios which could harm the organization’s image and attaching priority to affected audiences.

- Examples of options for recovery of internal and external communications includes: purchasing, setting up and maintaining a system for mass notifications and a collaboration platform to be used during disruptive incidents; purchase mobile phones from different suppliers; acquire satellite phones; and having pre-established agreements with broadcasters and media to disseminate key messages in case no other means are available.

- Finally, an example of an option for recovery of relations with regulators and public authorities includes establishing in advance channels for notifications and mutual help each other as soon as the disruptive incident occurs.

\textsuperscript{17} BCMM (Business Continuity Maturity Model) is a model developed by Virtual Corporation to classify the maturity of an organization’s continuity programme, which can also be used to assess the maturity of a corporation and its respective affiliates as well as that of a provider. It can be used as an evaluation tool or as a guideline to determine audit compliance.
5. Documenting action plans to be applied at the moment of the event

Continuity plans formalize strategies in a document that should be consulted and put into practice during disruptive incidents. Therefore, it is important for it to be easy to read and to be drafted as an aide-mémoire to remember what to do. It is not a procedure thoroughly detailing every step to be followed by anyone who is around at the moment of the disruptive incident, even less so if that person has no experience in the service or activity to be recovered.

Before drafting the action protocol it is important to create a model or document template, which does not necessarily has to follow the same guidelines applied to procedures for consultation, guidance or training on the daily activities of the organization which are used in normal situations. Thus, it is necessary to create a space for dialogue do as to explain the differences between a continuity procedure and a procedure for daily operations. A continuity procedure is not intended to document new operating procedures invented for the contingency. As a matter of fact, the premise is to continue performing the same daily processes but according to different priorities. Moreover, any non-urgent activity could remain suspended even for months. Nor is it intended to document manual procedures to be used when systems are not available. Manual procedures are one more way to operate daily activities without computer systems, and at present manual processing is very likely to be discarded as an option in view of the need to process large volumes of transactions or orders, and because of the security and fraud risks to which the organization might be exposed.

The general structure of any continuity plan should be as follows: a) objectives and scope; recovery priorities according to MTPDs and RTOs; b) response, continuity or recovery team; c) team activities, preferably by role; d) strategy to be followed at staff level, i.e., personnel assigned to specific roles (more than one person per role); e) strategy to be followed at the level of physical infrastructure, namely alternative operation sites; f) strategy to be followed as regards materials, consumables and supplies, namely locations of the necessary resources. By the same token, the same criteria should be applied to each one of the resources considered in the recovery strategies. The plan may be complemented by annexes including contacts data, location maps and templates to be used at the time of the incident.

**CHART 5**
Types of plans according to objectives

Generally speaking, continuity plans can be classified into five categories according to their objectives: a) continuity plans to respond to incidents compromising staff security and the organization’s physical assets; b) continuity plans to respond to incidents affecting the organization’s image; c) continuity plans to respond to incidents disrupting operations.
Continuity of business and operations during disasters in LAC: SP/II-SR-ASPPGRD/DT Nº 2-13

Balance and recommendations

computer systems; d) continuity plans to respond to incidents disrupting operations; and e) continuity plan governing management of any of the incidents through the Crisis Committee.

1. In the case of continuity plans to respond to incidents compromising staff security and the organization’s physical assets, the main objective is to safeguard operation of services or activities at the affected physical place vis-à-vis specific scenarios, for example: What to do to minimize involvement of staff in case of pandemics? What to do to minimize impact on staff and assets of the organization in the event of a fire or an earthquake? What to do to minimize damage to the organization’s staff and assets in case of a hazardous spill? Do the incidents correspond to the assessment of most likely risk or threats, or those with greatest impact?

In such case, teams should be oriented to first-response brigades, which include: evacuation and fires, among others. They will attach priority to protecting physical assets, depending on the level of urgency of the processes. Such information should be provided with the MTPDs and RTOs.

2. In the case of continuity plans to respond to incidents affecting the image of the organization, the main objective is to safeguard the reputation of the organization, while determining possible risks to the image, audiences affected, extent to which they are affected, which communication means are appropriate to reach such audiences and spokesmen to communicate messages. In this case, the team will be led by the official in charge of corporate image, his support staff and his spokesmen.

3. For continuity plans to respond to incidents causing failures in computer systems, the main objective is to continue providing information and communications technology services, as well as the data on the organization. Recovery priorities will be set in accordance with the RTOs defined for the information technology services and the services or activities that they support. This means that the RTO for an information technology service should comprise the basics of all RTOs of the services or activities using that information technology service. The recovery team of the information technology service will be comprised by the authorities in charge of information technology, will participate in the most important decisions as regards recovery, and will report to the authorities of the organization. The recovery team will also include the technical staff working with servers, databases, telecommunications and applications for recovery of information technology services at the operational level.

4. In the case of continuity plans to respond to incidents disrupting operations, the main objective is that the organization continues to provide services and conduct its activities. Recovery priorities will be set in accordance with the RTOs defined for such services or activities. The recovery team in charge of continuity of operations will be led by the Heads of areas or process leaders (depending on how the organization is structured to respond to a disruptive incident, with the leaders playing a key role during the incident). The recovery team will also include the staff holding key positions to carry out minimum activities, according to the established RTOs.

5. In the case of continuity plans governing the management of any incident, the main objective is to make decisions regarding any of the aforementioned plans, by creating a Committee on Incident or Crisis Management. This Committee will
be made up by the authorities of the organization. It will be convened to support decisions of the teams in charge of responding to incidents affecting staff security, image, information technology services or functional business units.

Since the disruptive incident could occur at any time when the organization has not finished implementing its options for recovery (for instance, an alternative site not been determined yet), the Committee on Incident or Crisis Management should manage to outline and implement such missing strategy so that the other teams working on continuity and recovery that depend on such strategic option can respond to the disruptive incident.

6. Drilling and testing action plans

Action plans could become dead letter if they are not drilled and practised. Actually, in case of a disruptive event, the success of the action plan does not depend on how well documented it is, but on how well practised and internalized it has been. Therefore, the main objective of drills is to put the plan in practise and gradually expose it to the greatest possible stress so as to improve it and determine the additional skills that participating staff should have to carry it out. Thus, the objective of drilling is not to prove whether the plan works or not, but to identify weaknesses in the plan and the staff so as to achieve a better response. After successfully overcoming the initial drill scenario, it should be changed to make it more complex, in accordance with degree of maturity of continuity in the organization.

A real-life example that helps understand the above is jogging. One can aim at simply jogging “round the block” once a week or to train during the whole week “for a forty-two kilometre marathon” trying to obtain a qualifying time for the next Olympics. What makes us choose between a low stress or a full stress scenario? It all depends on the level of preparedness of the person.

It would be unwise to force an amateur person who has never trained to run as a professional to participate in a marathon or for the Olympic Games because he might suffer great health damage. On the other hand, it is not reasonable to ask a person who runs four kilometres every day to simply jog “round the block” because it would prevent him from improving his running technique. The ideal situation would be to determine the level of preparedness of the person so as to choose the target scenario. If the person has never practised jogging, it would appropriate for him to just run round the block. But once the person has achieved such objective, he should progressively pursue higher goals, by setting a schedule to run longer distances through time.

Thus, an organization that has just started its business continuity programme cannot be out to a very complex test such as shutting down its operations and working with the alternative options defined in the strategies and in less time than that required in the RTOs. Possibly, the organization should start with a simple fire drill, desktop exercises, checking certain critical equipment, and emphasizing staff evacuation. Later on, the fire scenario could include hurt people, and more difficult desktop exercises, thus gradually increasing complexity. Of course, it is not necessary to wait for ten years for the alternative information technology infrastructure to function properly. Most probably, the first few drills will ensure that the alternative information technology platform will be ready and operating in two or three years.

The organization must also plan its test objectives through time, restablishing the goals to be accomplished in one, two, three, and maybe up to five years. The organization sets it own goals will confirm them every year. It should be borne in mind that the organization will not conduct continuity drills on a daily basis. The frequency of the drills must be
cautiously set so as to give the organization a chance to comply with its operation objectives. The levels of complexity as regards business continuity should be progressively set at the organization’s own pace, but they should not be spaced out for too long time periods, so as to prevent the staff from forgetting the changes in the organization’s plans.

**CHART 6**
**Drills according to complexity**

The drills range from less to more complex and costly. The least complex ones are review drills, desktop drills and game drills, whose objective is mainly to disseminate and raise awareness in the use of the plan and strategy options available in the organization. The second type of drills include infrastructure and equipment performance tests to ensure that they are operational and functioning and to make sure that the personnel operating the equipment knows how to do it and makes it fast within established time frames. The third type of drills include displacement drills which seek to provide knowledge about the places where to move, what transportation means should be used and how to move within established time frames. The fourth type of drills include exercises on coordination, command and integration in which more than one response or continuity or recovery team act jointly under the coordination of the committee on incident or crisis management. The fifth type of drills involve more complex simulations, which can include a combination of the aforementioned drills and are usually the target exercise of the year, for which, the organization has been preparing itself through previous exercises without affecting or paralyzing any critical service. Finally, we have the full-scale drill, which in addition to the simulation seeks to disrupt a critical service and recover it within the expected time frame. This drill takes into account the risks that it represents but it is conducted within a controlled environment to the largest possible extent.

Performing an unwarned drill is not intended to “check whether the plan works”. It is rather aimed at creating the necessary skills and competences among the staff for managing stressful situations while keeping suitable alert levels in case of a disruptive event. Even though the drill is unwarned for participants, it should always be notified to the appropriate authority so that it can envisage any risk that might disrupt services. Unwarned drills can be conducted for any of the types of exercises described above. For example, an unwarned desktop drill could be carried out to assess the staff’s level of commitment to continuity of business and operations.
7. Raising awareness and competences in the organization

The staff of the organization is responsible for conducting the activities assigned to it. Even though the issue of continuity could be recognized as important, daily activities might tend to lower the importance of the issue of continuity through time. For this reason, creating a culture of continuity of business and operations within the organization should be a permanent task.

If continuity plans have not been implemented in the organization yet, the type of awareness-raising will be different and should seek to sell or justify the need for establishing a business continuity programme, either in view of past incidents, incidents that have affected other organizations, regulatory obligations or legal or audit requirements. If continuity plans are already in place, then the purpose is to remind staff that it is important to be prepared to face any possible incident.

It is necessary to work with the area of internal communications of the organization in order to outline the best ways to transmit this message to the staff and the appropriate means to do so. For this purpose, the organization can resort to newsletters, web sites, posters, lectures, games and even conduct yearly events such as the day or week of continuity.

Awareness-raising should be in accordance with type of target audience and should always count on indicators to measure whether the desired results are being achieved, otherwise there is no way to determine if the method used is still effective and it is not possible to enter the cycle of continuous improvement.

The creation of skills and competences has a different objective from that of awareness-raising. It is mainly aimed at generating knowledge and experiences on different topics or disciplines concerning continuity. The subjects could include: concepts of continuity of business and operations considering specializations, response to incidents affecting the security of staff and critical assets, response to incidents affecting the image, response to incidents disrupting information technology, response to incidents disrupting operations, or governance and handling of incidents or crises in the use and implementation of alternative strategies for recovery and continuity plans, in which the drills will be very successful as tool for creating knowledge and experiences and for the alternates to carry out daily activities as if they were the primary officials.

Training should also be conducted in accordance with the type of personnel and capabilities that need to be created. Just as awareness-raising, the results must be measured to determine whether it is effective and is complying with the objectives of capacity-building.

8. Maintaining continuity of business and operations

Organizations are always changing: people change, responsibilities change, services change, buildings and facilities change, systems change, suppliers change, and other parts of the organization also change. Therefore, one of the most important challenges of continuity is to prevent continuity from becoming out-of-date despite the changes in the organization.

The success in managing change consists of identifying the change, and for this purpose it is necessary to know who can report on it and determine how frequently the source of the change must be consulted. For example, the source regarding personnel changes can be the Department of Human Resources, the frequency in consulting it can be every fifteen days and the means for consultation can be through a format specifying personnel changes that can be sent by e-mail. In another example, for changes in
computer systems, the source is the Department of Information Technologies, specifically the Committee of IT Changes, the frequency for consultations can be once a month by participating in meetings convened by the Committee.

As organizations can undergo many changes, the most important ones should be those that have a direct impact on continuity, namely: changes in services, processes or activities; people, transport and communications; physical infrastructure, public services and labour environments; equipment, materials and supplies; information technology services; suppliers; and financial viability; among others.

Once a change of interest for the continuity of business is identified, it should be registered in a change log and its impact on the obsolescence of the continuity of business and operations programme should be analyzed. If it has a low or moderate impact, the organization can wait until the following yearly update cycle. If it has a high or very high impact, the operational work plan of the current year (continuity) must be modified at once and the necessary continuity components must be updated.

Once the change is made in one or more documents of the continuity programme, a registry must be made to record what has changed, who made the change, who approved the change and what is the new version of the modified document. In case the document (for example a plan) needs to be distributed again, it will be necessary to collect the old versions of the document and store or destroy them, deliver the new versions, and even request officials to sign a form acknowledging receipt of the new copies.

The plan document is a controlled document. Its contents are the responsibility of the head of the Department or process plan, and the Coordinator of Continuity is responsible for access to the document and for distributing it only to those officials to whom the plan needs to be delivered.

9. Indicator of maturity and strategic planning on continuity of business and operations

An organization without indicators to measure progress or without a strategic plan will not have a means to measure strides. The same goes for the continuity of business and operations programme. If maturity is not measured and strategic objectives through time are not identified, it is not possible to prove to authorities whether progress is being made or not. Successful continuity of business and operations is not only measured by the continuity plans generated, but also by other factors that should occur to determine if the continuity of business and operations programme is on the right track.

The Business Continuity Maturity Model (BCMM) is the oldest and most widespread model in this area. It allows for determining how mature the programme on continuity of business and operations is within the organization. It includes eight objectives: 1) authorities' leadership; 2) awareness and interest of the staff in general; 3) structure, roles and responsibilities; 4) internalization and integration with internal and external parties; 5) measuring finest continuity indicators; 6) having competent resources and making investments in accordance with desired outcomes to be protected; 7) ensuring supply chains and handling third-party expectations; and 8) methodological order according to best practices.
The BCMM evaluates each corporate competence on a six-level scale, namely: Level one, the lowest level in which no continuity efforts are made. Level two, where at least one functional Department is making some efforts on its own initiative. Level three, where various functional departments try to coordinate efforts through any working Commission. Level four, where the organization is implementing a best practice and a continuity of business and operations plan has been established. Level five, where the organization has gone from theory to practice in implementing best practices as well as a continuity programme throughout the organization (within the scope of continuity) albeit not successfully in some departments. Level six, where the organization conducts a regular and constant practice aimed at excellence and all functional departments within the scope of continuity are highly committed. At this level, the organization counts on strategy options and implements plans frequently.

If the result from the maturity evaluation is one or two the model indicates that the organization is at risk. If it is three or four the organization is being competent. And if it is five or six it means that the organization is achieving excellence.

Based on the result of the BCMM model, progressive objectives can be estimated in time, for example: to reach level three the first year, to maintain that the second year, and then achieve level four the third year. Another example could be: to reach level four in leadership and awareness competences and at least level three for the departments with less than four-hour RTOs the first year, and in the second year to reach level four in all competences for the departments with zero RTO and level three for 24-hour RTO departments in the leadership and awareness competences.

Similarly, three, four or five years objectives could also be set as in the examples described above, and to review compliance on an annual basis, comparing them with the previous
year. If the objectives are not met, it will be necessary to periodically reassess the strategic continuity goals to adapt them to the maturity level of the organization.

VI. SUCCESSFUL CASES

Many private and public organizations are making efforts for continuity of business and operations. The following information corresponds to cases that have been disseminated in conferences and events organized by the publication *DRJ en Español,* specialized in continuity of business and recovery in cases of disaster.

1. Implementation of professional practices for continuity of business and operations

The types of organizations in Latin America and the Caribbean that are implementing practices for continuity of business include: regulated companies, mainly banking and, although to a lesser extent, the insurance sector; companies that have a big environmental impact, such as those of the oil and mining industries; public utilities, such as telecommunications, electricity and gas; large consumer and manufactured products companies; and large technology or third-party service providers, which at the request of their customers are implementing these best practices.

- An example of recovery priority for commercial banks is to enable users to continue withdrawing their money when they need it and making their financial transactions using the available channels, such as debit and credit cards, ATMs and electronic banking; these priority activities generate other related ones, such as back-office processes, liquidity in all channels, blocking of credit or debit cards, and of course the information technology that supports all the above-mentioned activities.

- An example of recovery priority for insurers is to deal with an incident, even more if it affects the health or life of the insured person. In this case, the emergency call centre and the issuance of guarantees, so that the insured person receives emergency care in an affiliated clinic or hospital, will be of the highest urgency. Of lower priority will be the attention of other types of incidents.

- An example of recovery priority for oil and mining companies is to respond to incidents affecting operations. In these industries, using alternate buildings or facilities to continue operations is not an option, and therefore the priority is to protect and contain the damage and call as soon as possible the insurer to start repairing the damaged structure.

- An example of recovery priority for public utility companies is to identify nodes, stations (or any other technical term to refer to them) that are more urgent than others and to create alternatives for ensuring the continuity of such nodes. Priority is also given to redundancy of networks, which can be of ring or mesh type to form alternate pathways. If a single link or a node were to fail, connectivity would be preserved in the other nodes.

---

18 Disaster Recovery Journal en Español - DRJ en Español is the most important publication that disseminates information on issues related to continuity of operations and recovery in cases of disasters in the region. It organizes virtual seminars once a month; face-to-face one-day events in Spanish-speaking countries; and an annual three-day international conference. The information presented in this section has been taken from those events.
In addition to these examples, there are others that are specific to certain sectors. However, different companies in a single sector do not necessarily have the same recovery priorities.

Banco Supervielle is one of the leading banks in Argentina, with a continuity programme in place for many years. As most organizations, it started with an information technology approach, called DRP (Disaster Recovery Plan); then, it incorporated aspects of business continuity, and finally it established a permanent management mechanism for continuity of business and operations. The management process to ensure continuity is led by the bank’s general manager and managed by the risk management department; it implemented multimedia sensitization and awareness campaigns. It is interesting to see the close collaboration between the information technology department and the risk management department to support and look for the approval of a budget to optimize the technological infrastructure of the bank, not only in terms of the technical aspects of the systems area, but also of disruption risk.

Grupo Bancolombia is one of the leading organizations in the financial sector with a presence in Colombia and Central America with more than eight million customers. Its business continuity programme is based on strategies designed and implemented on four fronts: people, infrastructure, processes, and technology. The continuity process is led by a Business Continuity Management Strategy, which coordinates with the Human Resources Management, Information Technology, Administration and Customer Services departments to maintain the programme.

Bank of Costa Rica has 250 offices throughout the country and is part of the BCR Financial Conglomerate, which is made up of the Bank, a stock exchange post, an investment fund management company, a pension operator and an insurance broker. The Bank has a business continuity programme in place led by the Board of Directors and the General Manager. There is a business continuity office responsible for managing a Business Continuity System, which integrates the efforts by the authorities responsible for operations, systems and risks in the Bank.

Banco Popular Dominicano is one of the largest banks in Dominican Republic. It was founded in 1963 and currently has 1.16 million customers; it has received national and international awards from prestigious rating institutions. The Bank has a continuity programme that, as in most organizations, was initially focused on the information technology or DRP. At present, all bank processes are taken into account and considered critical in their impact assessment.

Toyota Financial Services of Mexico provides financing, insurance and services in the automotive branch. Its programme for continuity of business and operations consider several scenarios, which account for no access to facilities, no access to information technology infrastructure, both scenarios together, and unavailability of critical staff. With the support of a consultancy company specialized in the subject, it managed to improve its continuity programme, increasing the culture of continuity, with a phased programme of tests and exercises, as well as the use of an alternate world-class centre.

Pacífico Seguros is one of the most important companies in the field of insurance in Peru. Given both its corporate nature and regulatory requirements, it implemented its business continuity programme, which includes a business continuity policy, maturity indicators, prioritized business functions and processes, risk assessment, plans and protocols for crisis management, crisis communication plans, response to emergency, recovery of computer systems and recovery of business processes, a testing and drilling programme and practical exercises.
Zurich is one of the most important insurance companies in our region. It has a business continuity programme in place at its various subsidiaries and has implemented its technological continuity and recovery plans in different events, such as the pandemic that mainly affected Mexico and the last earthquake in Chile.

Sistema Nacional de Comunicaciones Financieras de Chile (SINACOFI) is a company that offers services of credit bureau, clearing house and electronic messaging for the entire financial sector in Chile: banks, regulators, leasing companies, cooperatives and factoring companies. They have implemented a business continuity programme which takes as its main pillars: select the appropriate emergency plan for the recovery of the organization; integrate operation processes and information systems; define roles, assign responsibilities, gain skills and be part of the performance evaluations; and recognize the importance of integrating critical suppliers in the capacity for resilience of the organization.

Unipago is a company that processes the database of the Dominican Social Security System, whose shareholders include the Pension Fund Administrators (AFP) and the Health Risk Administrators (ARS). It is in charge of the management of the single registration system, as well as the processing of information. Unipago has a business continuity programme in place based on its information security management system, which includes business continuity and technological recovery plans, emergency response and establishment of a crisis committee.

Telefónica Movistar Colombia is one of the country's telecommunications service providers and operates in most countries of our region. Telefónica Movistar Colombia is implementing a business continuity programme, considering the prioritization of processes that are urgent to recover, a risk assessment of the main offices of the country, the implementation of recovery strategies, establishment of the crisis management and operational continuity plans, conduction of tests and exercises and awareness campaigns. Telefónica Movistar Colombia implemented business continuity plans as a result of disruptive incidents caused by the winter wave affecting Colombia in recent years.

The Instituto Costarricense de Electricidad (ICE) is responsible for providing power and telecommunications services in the country. As for telecommunications, the ICE has implemented a business continuity programme focused on the country's networks and telecommunications infrastructure. It has prioritized urgent nodes in the network; has carried out risk assessments on all nodes and stations that are critical to the country; has designed and implemented recovery strategies; has documented its crisis management and business continuity plans and has tested them progressively. And it has activated its continuity mechanisms in certain incidents, such as the earthquake in Costa Rica in the year 2012, a fire in the station of El Limon (on the Atlantic coast of the country) in 2010, and emergencies arising from the impact of storm Thomas.

Grupo Nutresa is one of the largest Latin American organizations in the field of mass consumption. Its business covers cookies, pastas, chocolates, ice cream, coffee and meat and has a regional scope, with production plants in the United States, Mexico, Costa Rica, Venezuela, Ecuador, Peru, Colombia, Panama and Dominican Republic. Nutresa is implementing a business continuity programme within the framework of the comprehensive risk management, and is conducting risk and crisis management plans; an incident response plan; a disaster recovery plan at the level of information systems, emergency plan, succession plan, a plan for business recovery and continuity of operations, a plan for continuity support, a TI contingency plan and coordination plan with public authorities.
There are many other examples of companies in Latin America and the Caribbean that are implementing best practices in business continuity in other sectors, such as Ecopetrol of Colombia, Minera Xstrata of Chile, Explosivos SA in Peru, Grupo ISA from Colombia with presence in other countries of the region, among other organizations.

2. Integration of public and private sectors

The integration between the public and private sectors takes place in our region in two different manners: the first is through volunteerism in the private sector, which collaborates with the public sector to respond to catastrophic events of great geographical extent; and the second is through comprehensive, almost regulated or forced, collaboration among authority, regulator and companies of the sector in order to ensure the continuity of the service they provide. It usually refers to public services, such as telecommunications, electricity and banking.

DHL Panama is an example of the first type. DHL Global established a Disaster Response Team (DRT), which provides free logistical support to the country where the natural disaster occurs, but in cooperation with the United Nations and/or governmental agreements with organizations in the area.

DHL has a strategic alliance with the United Nations Office for the Coordination of Humanitarian Affairs (UN/OCHA) since 2005 and has signed agreements with Governments or State entities in Panama, Guatemala, El Salvador, Honduras, Nicaragua, Costa Rica, Peru and Chile.

The DHL DRT Americas is based in Panama, where it coordinates the movement of staff to provide logistical support at the affected site; examples of its activities in our region are: Hurricane Wilma in October 2005, in Cancun, Mexico; the earthquake of Pisco, Peru, in August 2007; floods in Honduras and Panama in October and November 2008; the earthquake in Haiti in January 2010; the earthquake in Chile in March 2010; floods in Guatemala in June 2010.

The central banks of each country are an example of the second type of integration between public and private sectors, since there are initiatives in some countries of the region that enable banks, in case of a large-scale event, to continue providing their services and that make it possible for central banks to articulate common and coordinated responses.

Something similar happens in the telecommunications sector, where the supervisory body, usually the Ministry of Telecommunications (or its equivalent depending on the country), requires that some kind of coordination is established among all service providers to coordinate comprehensive responses to major events, e.g. an earthquake.

In the electricity sector, efforts are coordinated, also under the leadership of the corresponding Ministry or of the national centre for control and dispatch of the interconnected system (or its equivalent depending on the country), to restore the service in the areas affected by a major incident that caused the massive service outage.

In the case of Costa Rica, where the Instituto Costarricense de Electricidad (ICE) is the main telecommunications operator and the only electricity system operator, this institute is part of the National Emergency Commission. The centres responsible for monitoring networks and dealing with emergencies are interconnected with the national incident response systems to coordinate the response to a severe incident affecting the country.
VII. CONCLUSIONS AND RECOMMENDATIONS

Latin America and the Caribbean is a region prone to natural disasters, but also to other incidents that could disrupt the operations of public or private companies, such as social unrest, insecurity and organized crime, among others.

Regardless of the cause or origin of threats, their impact could disrupt the activities and services of organizations, and for this reason they should implement the necessary measures to ensure continuity of operations despite the incident.

Although incidents do occur, the same organization will not be frequently affected, therefore officials in charge of continuity of business and operations should be very cautious as regards its scope and the investment that the organization should make in order to be protected vis-à-vis a major event that might never happen.

In order to define which activities of the organization should be protected and which not, it is necessary to determine first which activities are crucial for the survival of the organization. Like in the case of a human being, whose vital organs are defined, an organization must also define its vital activities.

The first step to identify vital activities is to identify what “intolerable” means for the organization when it comes down to surviving. The organization can determine intolerance levels as regards economic aspects, image, or regulatory, contractual, environmental or social aspects (for instance: it is intolerable to affect service for thousands of clients or users). The urgency of the activities is determined by considering how much time it takes for reaching an intolerable impact due to the interruption of each activity of the organization. Those activities showing an intolerable impact in a matter of hours or a few days will be the vital ones.

Vital activities should receive additional protection as compared to others activities of the organization, in line with existing security mechanisms (physical security, computer security, labour security, operational risk, market risk, among others). The risk management guidelines set forth in ISO 31000 can be followed to identify the additional security measures needed.

In addition to the preventive measures – which could fail in case of an event never thought of before – for those vital activities it is necessary to have alternate operation mechanisms at safe distances, which can be quickly activated so as to continue providing key services through the vital activities.

In view of the needs for coordination and having organized personnel, it is necessary to document the protocols of action during the disruptive incident. These continuity and incident management plans should be easy to obtain and use at the time of the incident. Plans should be set up for managing incidents and crises, for decision-making at the time of the incident, response to emergencies to protect personnel, response to impacts on the image, recovery of computer services and recovery of key activities.

The written paper is not a guarantee of continuity at the time of the incident, so practice is necessary. Drills must create the skills, experience and confidence among the personnel participating in them and the organization in order to implement the plans during the incident. Drillings must gradually become more complex to ensure continuous improvement in preparedness.
Since getting prepared to face disruptive incidents does not form part of daily operations, and such events are not very frequent, it is necessary to establish a permanent program for awareness-raising and training to maintain a state of alert in the organization. Authorities must be the first ones to demonstrate such state of alert, awareness and training so that the rest of the organization follows their example.

In order to maintain continuity of business and operations through time it is necessary to institutionalize it within the organization through a policy, integration of roles as regards preparedness and response in the functions manual of the organization, and follow-up by authorities, either through meetings every two or three months or through internal (or external) audit reports on its proper implementation and maintenance.

To implement continuity of business and operations, an organization should take as guidelines the best practices and international standards on the subject: BCI, DRII, ISO 22301, NFPA 1600 and ASIS SPC. Many organizations in our region implement those concepts according to their own understanding and experience, thereby confusing the objectives of continuity, delaying proper methodological application and putting their own organizations at risk.

An organization that has recently started with continuity plans or wants to improve them can review the experiences of other organizations that are already implementing these best practices in our region. A good source of information is DRJ en Español, where many enterprises have shared their experiences in implementing continuity of business and operation programmes, including Banco Supervielle of Argentina, Grupo Bancolombia, Banco Popular Dominicano, Banco de Costa Rica, Toyota Financial Services of Mexico, Pacífico Seguros of Peru, Zürich at the regional level, SINCOFI of Chile, Telefónica Movistar of Colombia, the Cost Rican Institute of Electricity (ICE), and Nutresa of Colombia, among others.

The integration of the public and private sectors does not only occur through private sector’s voluntary collaboration led by the public sector, but also when an industry sector which is vital to society – most of the times with a private share – should recover under the leadership of the public sector in order to continue serving society. The vital sectors for society which should not be disrupted are: power supply, telecommunications, gas, water and sewer, banking and financial services, mass consumption and basic products, and insurance.

The challenge for society, national, regional and local governments and regional institutions working to respond to natural disasters is to redouble their efforts to not only focus on improving response and protection for the population and their houses – which is clearly a priority – but also to protect other industrial and business aspects that society and the population demand in order to continue with their lives.

It is also necessary to make a call to both public and private institutions which have made little or nothing to protect themselves against disruptive incidents despite having the economic means to do so. This reveals the carelessness and little diligence of their authorities with respect to the viability of their organizations.

Finally, this concept of continuity of business and operations can also be applied to “continuity of society”, which central, regional or local governments may implement. Comparatively, a population is equivalent to an organization that has key services or vital activities such as housing, basic services, health services, power supply, transport and finance, among others, which should be recovered in case of a disruptive incident. Municipalities must have options to be implemented in order to provide alternative
housing, alternative basic services, such as alternative power generation plants, alternative drinking water tanks; alternative centres for collection and distribution of food and preparation of meals, alternative temporary health centres, alternative temporary means for massive transportation, financial viability for the reconstruction of affected infrastructure, and to facilitate availability of cash among the poorest population, and alternative media, among other aspects that may be considered.

Thus, public, regional and local authorities are called upon to take due account of these concepts in implementing the contingency or continuity plans for the most vulnerable sectors of the population and gradually incorporate the rest of the population.
BIBLIOGRAPHY


International Telecommunication Union. Estadísticas de la UIT respecto al uso de la tecnología de información a nivel mundial - "Core indicators on access to, and use of, ICT by households and individuals, latest available data", (available at http://www.itu.int)
