LATIN AMERICAN
AND CARIBBEAN
ECONOMIC SYSTEM

EXPORTBelize
connecting global opportunities

SBDCBelize
making small business happen

Beltraide

Guidelines for continuity of business and operations of MSMES vis-à-vis disaster scenarios

Preview Version

Economic and Technical Cooperation

Training Workshop for MSMEs on continuity of business and operations vis-à-vis natural disasters
28, 29 and 30 June 2017
Belize City, Belize
SP/TC-MIPYMESCNOFD/DT N° 2-17

CONTENTS

FOREWORD

This document is in line with the Work Programme of the Permanent Secretariat of the Latin American and Caribbean Economic System (SELA) for the year 2017, related to the Latin American and Caribbean Programme for the Small and Medium-sized Enterprises (SELA-SME Programme), particularly to the activity entitled "Training Workshop for MSMEs on continuity of business and operations vis-à-vis natural disasters".

This activity is also associated with the initiatives undertaken by the Permanent Secretariat in the field of the public-private partnerships for disaster risk reduction, in collaboration and coordination with the United Nations Office for Disaster Risk Reduction (UN/ISDR).

The "Guide for continuity of business and operations of MSMES vis-à-vis disaster scenarios" (SP/TC-MIPYMESCNOFD/DT N° 2-17) is a new contribution of the Permanent Secretariat of SELA to the efforts to strengthen the preventive culture in the region and complement the study carried out in 2013 on "Continuity of business and operations during disasters in Latin America and the Caribbean, balance and recommendations". On this occasion, this document focuses on MSMEs in order to contribute to the sustainability of the sector of micro, small and medium-sized enterprises vis-à-vis the occurrence of adverse events that could jeopardize the continuity of their operations.

The document consists of an introduction and nine sections which address the following subjects: i) Empowerment and Governance in the Continuity of Business and Operations by top management; ii) Identify priority and urgent activities to recover in case a major event occurs and disrupts operations; iii) Protection of the most urgent activities aimed at mitigating the possibility that a major event can disrupt MSME operations; iv) Establish continuity and recovery strategies for the most critical activities; v) Document the plans of action to apply at the time of the event; vi) Training for and testing the plans of action, vii) Raising awareness and competences in MSMEs; viii) Maintaining continuity of business and operations; and finally ix) Use of indicators on continuity of business and operations.

This study has been prepared by Consultant Yves Davila Cainero, to whom the Permanent Secretariat expresses its recognition for his efforts and its gratitude.

EXECUTIVE SUMMARY

This guide for continuity of business and operations of MSMEs vis-à-vis disaster scenarios considers as its main input the base study prepared on the occasion of the II Regional Seminar on "Partnership between public and private sectors for disaster risk reduction: Continuity of government and continuity of business operations during disasters" (Cartagena de Indias, Colombia, 1 and 2 August 2013), entitled "Continuity of business and operations during disasters in Latin America and the Caribbean: Balance and recommendations (SP/TRSDPYMESA/Di N° 15-13).

The concepts and methodology presented are aligned with best practices and existing international standards, especially ISO 22301, 6 professional practices of the Business Continuity Institute (BCI) and 10 professional practices of the Disaster Recovery International Institute (DRII). For more details or information about the methodology in its entirety or some of its parts, it is highly recommended that suitable professional practices are revised and studied.

The 9 methodological phases are as follows: 1) Empowerment and Governance of continuity of business and operations by the Top Management; 2) Identification of priority and urgent activities to be recovered in case a major event occurs that disrupts operations; 3) Protection of the most urgent activities in order to mitigate the chances that a major event may paralyze operations of the MSME; 4) Establishing strategies for continuity and recovery of the most critical activities; 5) Documenting the plans for continuity to be applied at the moment of the event; 6) Train for and test the continuity plans; 7) Raising awareness and competences in MSMEs; 8) Maintaining continuity of business and operations; and finally 9) Use of indicators on continuity of business and operations.

The present methodology has been prepared considering the practical and functional application for the case of an MSME. Each MSME will be able to take into consideration what initially it can implement of these guidelines; however, progressively, year by year, it should complete all the aspects that this guide proposes

.

GENERAL GUIDELINES

This section provides a general overview about each one of the methodological aspects to be considered for the implementation of a Programme of Continuity of Business and Operations in MSMEs.

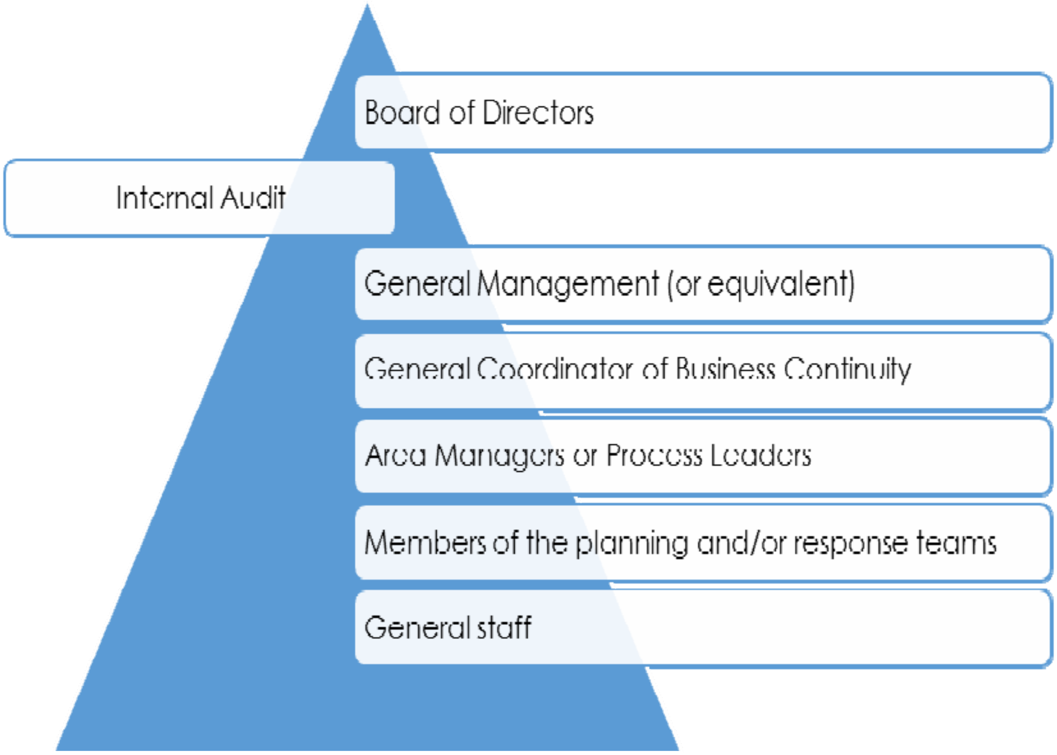
1. Empowerment and Governance in the Continuity of Business and Operations

The continuity of business and operations represents a big challenge for the MSMEs of our region. The risk of losing all what was invested, either by the occurrence of an unexpected major event or the intervention of some public authority because the service to our clients is affected, is always present. However, despite that Top Management could be aware of the importance of implementing the continuity of operations, many times nothing is done in this regard, or in any case these initiatives are very poor.

Moreover, many times the continuity of business and operations is confused with having the document of the contingency plan and, that is another very common error. The contingency plan or continuity plan should be a consequence of an existing permanent process in the organization called Business and Operations Continuity Management.

To attain the appropriate empowerment depending on the level of hierarchy: (owners, managers, leaders and experts on the knowledge about the activities of the organization) is one of the first objectives to achieve in order to manage the permanent process of business and operations continuity. These roles are defined in the following way:

CHART 1
Roles participating in business continuity


Board of Directors
Internal Audit
General Management (or equivalent)
General Coordinator of Business Continuity
Area Managers or Process Leaders
Members of the planning and/or response teams
General staff

Board of Directors. It is responsible for business and operations continuity of the organization, it assigns this responsibility to the highest hierarchical ranking authority in the organization, which is a general manager, and demands from him accountability on the topic at the end of each period that has deemed convenient. The Board of Directors is also responsible for approving, as corresponds, the necessary investments in resources to implement business and operations continuity. The Board must also make evident that business and operations continuity supports the continuity and survival of the organization's strategic goals by approving the scope of its application within the organization.

General Management (or equivalent authority). It is responsible for implementing business and operations continuity in the organization. For this purpose, it should implement and constantly go through the process of business and operations continuity management, by assigning it to a single responsible individual with the adequate political hierarchy and the necessary competences to carry out the job. The General Management is also responsible for approving, as corresponds, the necessary investments in resources to implement business and operations continuity.

The authorities of the organization, under the leadership of the general management, should establish, maintain and practice a scheme of response to incidents and crises that can be presented at operation level, emergency level or when reputation is affected; for this, there should be defined a response team, and assign roles of governance of the incident and crisis, and offer it what is necessary to create the competences needed.

General Coordinator of Business Continuity. This person is responsible for implementing and maintaining the business and operations continuity programme and reporting the progress to the General Management (or equivalent authority). In the case of an MSME, this function could be shared with other functions assigned to some role within the organization. In larger organizations, this function could be exclusive and full time. The implementation of the continuity programme should follow a methodological order in accordance with one or a set of international standards mentioned in the introduction, and should involve the Area Managers or Process Leaders.

The General Coordinator of Business Continuity should have the necessary competences, documents confirming specialized training and will have to participate in the forums and conferences on business continuity at the local, regional and international levels.

Area Managers or Process Leaders. They are responsible for implementing and maintaining business and operations continuity to their operations' scope and responsibility. Therefore, they should appoint, if possible, a person responsible for the operational continuity of such area or process with the necessary authority to organize the internal efforts, in coordination and under the leadership of the general coordinator of business and operations continuity of the organization. In the case that the appointment of the responsible person cannot be done, the heads will be directly responsible for implementing and maintaining business continuity.

In the case of the Area Managers supporting operations, such as Security, Human Resources, General Services, Information Technologies, and others, they should participate by leading the response to the incident of the most common events within their scope (pandemics, fires, earthquakes, computer centre taken down, etc.), as well as supporting the response to incidents that disrupt the operations of the most critical activities of the organization.

The managers and leaders of processes should have the necessary competences, documents accrediting their specialized education in topics like leadership, business and operations continuity.

Members of the planning and/or response teams. These teams are usually part of the operation personnel below the managers, who during the process of implementation and maintenance of business and operations continuity provide expert knowledge on recovery priorities and needs. During an exercise or a real incident they participate in the response to the incident applying the continuity plans and strategies prepared during the planning stage.

The members of the planning and/or response teams should have the necessary competences, documents accrediting specialized education in the topics of business and operations continuity, they should also know their plans and have experience in the response to incidents when applying their plans.

General staff. It is usually formed by the operation personnel below the heads during the process of implementation and maintenance of business and operations continuity, it provides expert knowledge on recovery priorities and needs, and during an exercise, or a real incident, participates in the response to the incident applying the continuity plans and strategies prepared during the planning stage.

In addition to the responsibilities described above in the organizational structure, the organizations also need to define a policy of business and operations continuity. This policy mentions the scope at the level of services, areas or places that are considered within the extent of the continuity programme, thus all that is not in reach, is because it is not urgent to recover and, therefore, there will be enough time available to re-establish such non-urgent activities as soon as the incident occurs without the need for planning anything beforehand.

Governance is also implemented with the follow-up and revision meetings convened by the General Manager, recommended once every two or three months. If the meetings take longer to be held one from the other, it is likely that the solution to the issues that could arise during implementation or maintenance of the continuity programme will not be attained.

The internal audit also plays an important role in the governance of business and operations continuity. The audit should guarantee that the continuity process is carried out according to the instructions given by the Board of Directors and in accordance with the best professional practices in this respect. The auditor must be someone independent and should have the adequate competences to offer opportunities of improvement aligned with the objectives of the process of continuity and does not identify observations that stray off the objectives of continuity.

2. Identify priority and urgent activities to recover

The identification of priority activities has the goals of establishing the extent of preparation for the occurrence of a disruptive incident; identifying the order and recovery time of the activities and the dependence between them; identifying the necessary minimal resources at the time of the disruptive incident; and serving as a basis for proposing strategic continuity or recovery options that are cost effective.

The scope of business and operations continuity is important to limit the efforts of the MSME to what is really urgent to recover. A disruptive and severe incident does not occur frequently and probably many MSMEs have never experienced it.

The scope of business continuity can be established in several ways, and it will depend on the sector to which it belongs. The most recommended way is to establish the scope by services[1] that the organization offers, that is, in the case of a disruptive incident, which services will continue to be provided as a minimum and which are not guaranteed to continue?

Once the scope is established at service level, it is easier to identify the geographical extent to consider, in the case that the MSME has several locations or plants where it operates the services within the scope; and it is also easier to establish the extent at the level of processes or activities with which to provide prioritized services, and therefore, the extent at the level of departments or functional units.

A common mistake that often happens between those responsible for implementing business and operations continuity is to consider a very broad extent for business continuity, making that the organization dedicates a big effort either in trained personnel, personnel's own time, and investments in alternative options of operation that are very expensive to be used in disruptive incidents, that although they may occur with some frequency, rarely affect the organization.

In order to identify the recovery time of the activities, first, it is necessary to establish the non-tolerance thresholds for the organization. This means for the understanding of the Board of Directors, what they would not stand that happens to the organization in each one of the categories of possible impacts: economic or financial (how much compromised money is intolerable to the organization?), users or clients affected (how many affected clients or users are intolerable to the organization?, legal or regulatory (what level of sanctions or judgments for non-compliance is intolerable to the organization?), environmental (what environmental damage is intolerable to the organization?), safety of the people (what level of impact on the people is intolerable to the organization?).

The answers to the above-mentioned questions posed should be given by the Top Management of the organization considering what they understand as the vision or perception of the interested parties of the organization would have during a disruptive event. Examples of these interested parties are: users or clients, owners or shareholders, public authorities and regulating organizations, business partners, organization's personnel, community or town where it operates, among others. The answers will give as a result the definition of the non-tolerable[2] thresholds of the organization.

The following step is to assess the Maximum Tolerable Period of Disruption (MTPD), which is the result of posing the following question: in the case of disruption of service/ location / department / process / activity (it can be any of them, depending on the type of prioritization that is being made) How long will it take to reach the non-tolerable thresholds? The possible answers can be varied: not apply, minutes, hours, days, weeks, or months.

To answer the question is also necessary to make the assumption that what scenario stresses the most the analysed element and at what moment it is stressed the most. This is aimed at identifying if the most compelling answer comes when the disruptive incident only affected the organization or massively impacted on other organizations; and also if the greater impact occurs at any specific date of the week, month or year.

[1] Also there can be mentioned either way the words product or service.

[2] Non-tolerable thresholds are not necessarily unique values, and can be considered in different ways, such as: “It is intolerable not to provide the service to a thousand clients, or not to provide the service to ABC S.A.C. or not to provide the service to ten clients of the strategic type”.

The MTPD will be defined as the shorter time of all the given answers for the different types of impacts of the non-tolerable thresholds and will always be estimated considering the "worst scenario" that in fact is the most stressing one for the organization and not necessarily that causing the greater damage to the community. What continuity seeks is to protect the organization facing the worst scenario, not against the most probable one.

TABLE 1
MTPD estimation matrix

Service or Activity			**How long does it take to reach non-tolerable thresholds?**				
Description	Critical seasonality	Most stressful scenario	Economic	Clients or users	Legal or regulatory	Environmental	Security of people
Service 1							
...							
Activity 1							
...							

Having defined the MTPD, a Recovery Time Objective should be estimated, which is a time value expressed between zero and the MTPD. As it is the closer to zero, the strategic option to continue operations will be very expensive; whereas the closer to the MTPD, it will be extremely risky. The best balance between cost and risk will give the most appropriate RTO.

The dependence between services / facilities / business units / processes / activities should also be analysed to identify or correct the MTPDs and RTOs from those on which they are based considering that they should be smaller than the MTPDs and RTOs of the dependent ones.

This process of estimating MTPDs and RTOs can be made at different levels, at a strategic level might be by service (or plant, or functional unit), and at operation level will be by activity (or process). Estimating MTPDs and RTOs should be a continuous task in the organization due to the changes that this can have, the appearance of new services (or new facilities or plants, or new functional units) and new activities (or processes) will make necessary to revaluate the recovery urgency priorities; the same might happen if a service (or plant, or functional unit) takes on greater relevance than another. If the recovery priorities are not updated at a certain time, a disruptive incident can happen where decision making will be wrong because of counting on outdated information.

After the RTOs are defined, the services (or plants, or functional units), or the activities (or processes) are grouped by RTOs, creating recovery time windows that are services or activities recovered in zero time (if they exist), those recovered in hours (if they exist), those recovered in days (there can be one day, two, three or simply days), those recovered in weeks (there can be one week, two or simply weeks) and those recovered in one month or more.

When the recovery windows are consolidated, there is a need to identify the minimal necessary resources to consider during a disruptive event. The types of resources will be organized[3] by: people, transport, communications; Infrastructure: buildings, public services; Equipment: work environments, equipment, consumables; Information technology: computer services, information and data; Finance: financial feasibility; Regulation: regulatory aspects to comply with; Suppliers: partners and suppliers; Interested parties to contact: clients, public authorities, and community in general.

The Personnel resources are identified by taking into account the necessary minimal profiles to continue operating services / activities for each one of the recovery windows, and even if the personnel of the organization appropriately complies with the profiles.

The Transport resources are identified by considering the facilities of mobility with which the organization counts on to be provided to the personnel during the disruptive incident.

The Communications resources are identified by considering the communication capacities among the personnel, with which the organization counts on and that might be available during the disruptive incident.

The Facilities or buildings resources are identified by considering the options of work places, or other sites, or plants from where the operations might continue during the disruptive incident.

The Public Services resources are identified by considering the options of the provision of power, water and drainage, gas and telephony that can be used during the disruptive incident.

The Work environment and equipment resources are identified by considering the options of operation in other work environments, or with an alternative equipment located in another site that can be used during the disruptive incident.

The Consumables resources are identified by considering the options of material (or raw material), consumables or other perishable consumables or not, that are necessary to consider at the time of the disruptive incident and the locations where they are currently found.

The Information technology resources (systems, information and data) are identify by considering the IT services that should be used at the time of the disruptive incident, as well as the information or another data necessary for the analysed service or activity.

The Financial feasibility resources are identified by considering the needs for the availability of financial resources in cash or not, to face the disruptive incident.

The Regulation resources are identified by considering the legal or regulatory obligations that should be continued during the disruptive incident and if there exist alternatives in the case of non-compliance.

[3] In accordance with the ISO 22301 standard.

The suppliers and business partners are identified by considering those that support the critical services, their contacts and other options of suppliers in the case that these are also impacted as a result from the incident. The other interested parties as clients, public authorities and community are identified by considering the necessary contacts to make in the case of a disruptive incident.

This information obtained at the resource level is the basis for the identification of continuity and recovery strategy options and their corresponding implementation budget estimate.

3. Protect the most urgent activities

The continuity of the most urgent activities should be guaranteed not only with the identification of options of post disruptive incident strategies, but also preventive options for the disruptive incident; whereby, continuity looks for evaluating if the currently existing protection and security measures, in the sites where the urgent activities of the organization operate, are enough or if they require to be improved or even if new protection and security measures are required.

Different methods can be used to evaluate if the protection measures are sufficient, the most recommended method is the risk analysis proposed in the ISO 31000 standard, which calculates the risk as a combination of the probability and the impact of a risk event.

To delimit the risk events that can be of any interest for continuity, it is necessary to be concentrated in the consequences of the threats that a disruptive event could create due to the absence of the necessary resources to operate. Examples of risk events to be considered by continuity would be: "impact on personnel given the occurrence of an earthquake", "impact on the building given the occurrence of an earthquake", "impact on the suppliers facing the occurrence of a pandemic".

It is also necessary to delimit the threats to which the organization is exposed and could occur, those are called dangers. These dangers should be identified starting from the most comprehensive threats to the most specific ones applicable to the organization. For example, if the organization is established in the Caribbean, the cyclonic and hurricane season is an applicable threat, that is danger, but in the case of South America, the hurricanes will not be an applicable threat. But a pandemic, although it has happened in China, because of its worldwide expansion, yes, it is an applicable threat for the Caribbean as well as South America. If we reduce the extent of the threats to more local topics, very likely crime, civil demonstrations, and other examples of threats, they will be considered as dangers more in some cities of our region than in others.

The objective of the risk analysis in business and operations continuity is to identify new options of prevention or improve the already existing security measures for each one of the risks events considered; therefore, the first step will be to identify those prevention and security measures that already exist in the organization, the security measures will be related to the security aspects regarding personnel, physical infrastructure, work environments, consumables, information systems, suppliers, and each one of the other resources associated with continuity and that result relevant for the organization.

As previously indicated, the risk is estimated combining probability and impact, it can be calculated by qualitative or quantitative methods. The problem of the quantitative methods is that they need historical data in addition to complex statistical formulas of projection of the occurrence of disruptive events resulting from the threats. In many cases it is not clear that the objective of continuity is to propose preventive measures and not necessarily the accurate estimation of the probability and, therefore, the risk in a mathematically exact way. Due to this, the organizations decide to estimate the level of qualitative risk, and the following is an example of it:

a) The risk matrix is defined by identifying the probability scales and the impact scales. If there exists a risk management department in the organization it is more advisable to be aligned with the size of the matrix already in use, although the scale meanings are different for continuity (an issue that will be dealt with later on). If the organization does not have a risk matrix, one should be defined.

TABLE 2
Risk matrix five x five example

Impact Probability	Very low	Low	Medium	High	Very high
Very high	🟨	🟧	🟧	🟥	🟥 **Extreme**
High	🟨	🟨	🟧	🟧 **High**	🟥
Medium	🟩	🟨	🟨 **Medium**	🟧	🟧
Low	🟩	🟩 **Low**	🟨	🟨	🟧
Very low	🟩	🟩	🟩	🟨	🟨

b) The risk matrix scales may be three times three, or four times four, or five times five, or a different combination depending on the best way in which the organization understands that it can assess the risks.

c) The level of risk is estimated by identifying the combination of probability and impact, in the chart shown above there can be seen four levels of risk: extreme, represented in red background and the treatment must be immediate; high, represented in orange background and the treatment must be provided in the short term; medium, represented in yellow background and the treatment must be provided in the long term; and low, represented in green background and it is not necessary to provide treatment to the risk.

d) The probability scale is defined based on the incidence of the risk event in time by considering the context applicable to the organization. Example of probability scales are: Very High, the incident occurs at least once a year in the last five years; High, it occurs at least once every five years in the last 25 years; Medium, it occurs at least once every 10 years in the last 50 years; Low, it occurs at least once every 25 years; and Very Low, it occurs in time spans longer than 25 years.

e) The impact scale is defined based on the level of damage that it might cause in the organization, in continuity the damage is understood as the time of unavailability or disruption of the incident. Where the most urgent activities are undertaken the highest impact will be in a matter of hours; where the least urgent activities are done the highest impact will be in a matter of days or weeks as it corresponds.

After having defined the risk event, the risk matrix and its corresponding scales of probability, impact and risk, and also the existing controls, there is estimated the probability of occurrence of the risk event and its impact, by convening the experts in the organization that know about the threats and effectiveness of the controls implemented, which determine the resulting level of risk according to their expert judgment.

Where there result extreme, high or medium risks, it is necessary to implement new preventive measures or controls, or in any case improve them to help reduce the level of risk, all at the suggestion of the experts mentioned above. The priority of implementation of the new or to be improved measures will be given as a function of the level of risk that they seek to protect, that is in the first order there should not be allowed extreme risks, these resolved, there should not be allowed high risks, and thus it also follows on medium risks.

4. Establish strategies for continuity and recovery of the activities

The strategy options can be preventive or reactive. The preventive options are identified using the risk analysis made for the risk events that the organization has assessed and their main objective is to mitigate or reduce the vulnerability of the services and/or the most urgent activities of the organization. The reactive options are identified from the outcomes of the prioritization of the services and activities in accordance with the MTPDs and RTOs, and above all, taking into account the necessary minimal resources identified.

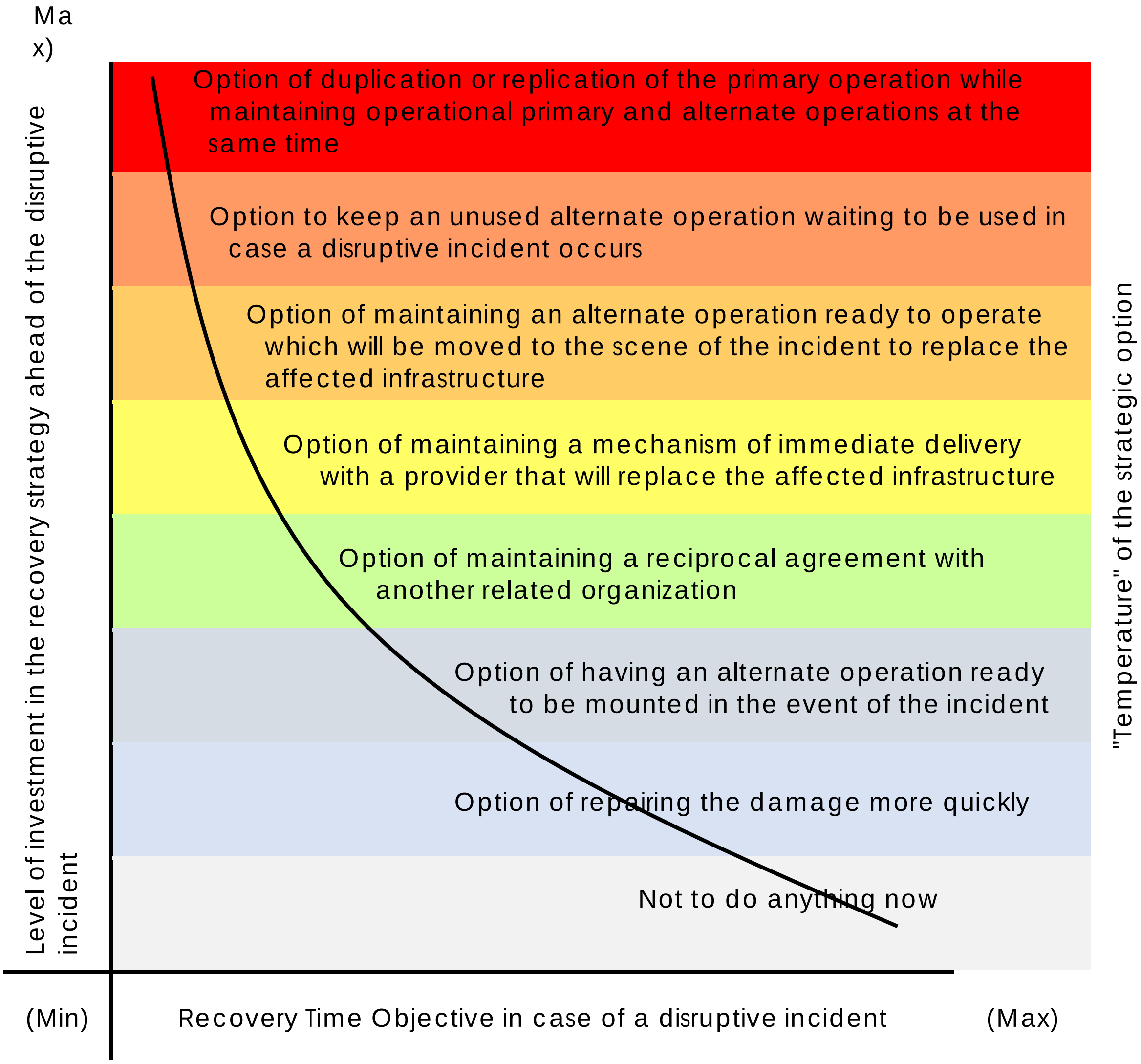
The strategic options should also consider the cost of their implementation and meet the established RTO. If it were necessary to adjust the RTO value because of considerations of technical feasibility or very high costs, so it should be done, bearing in mind to inspect the dependences of such an activity and redefine its new RTOs with these dependences.

The options can range from the most demanding and expensive to the less demanding and more economical, thus defining how "hot" or "cold" should be the option chosen. The "hotter" options go through dividing the operations into two or more parts and locate such parts in a safe place, beyond the extent of the risk scenarios of wider geographical coverage; to have an empty infrastructure waiting to be occupied immediately as soon as an event happens. The "warmer" options have schemes transportable to the operation sites where the service has been affected; or a space in use that will be emptied to be used for the more urgent activities than the ones operating there. The "colder" options have almost nothing pre-assembled waiting for the event to happen or even do nothing at the present time and leave everything for the time the incident of continuity happens and seek to react at such time.

All the options can be implemented in their own way, that is maintained and operated by the organization itself, or to look for a third party to be in charge of providing such options.

What is important about selecting the appropriate strategy or set of strategies is not to risk the recovery of the business; i.e., to comply with the established RTO and not to risk the MTPD for anything, because of looking for savings in the chosen option. The organization might use a combination of options, for example, for services or activities that can never stop not even in the face of a disruptive incident the option of separating the operations will be the appropriate one, in spite of the cost; for the one that can wait only hours, the option of having something ready for the personnel to come will be the suitable one; if the activity can wait days then a transportable scheme can be the appropriate one; however, there cannot be used the strategy of immediate delivery for example, if the recovery time objective consists of only hours.

CHART 2
Cost-benefit analysis for continuity strategy options


Ma
x)
Level of investment in the recovery strategy ahead of the disruptive incident
Option of duplication or replication of the primary operation while maintaining operational primary and alternate operations at the same time
Option to keep an unused alternate operation waiting to be used in case a disruptive incident occurs
Option of maintaining an alternate operation ready to operate which will be moved to the scene of the incident to replace the affected infrastructure
Option of maintaining a mechanism of immediate delivery with a provider that will replace the affected infrastructure
Option of maintaining a reciprocal agreement with another related organization
Option of having an alternate operation ready to be mounted in the event of the incident
Option of repairing the damage more quickly
Not to do anything now
"Temperature" of the strategic option
(Min)
Recovery Time Objective in case of a disruptive incident
(Max)

The continuity and recovery options should be applied at the level of the resources involved in the disruption of a service or activity. That is to say that to reactivate the disrupted service or activity, there have to be restore indeed the resources needed to operate, i.e. personnel, transport and communications, physical infrastructure, facilities and public services, materials, consumables, equipment, computer systems, data and information, financial feasibility, suppliers, relations with clients, regulatory demands, internal and external communication mechanisms, and options of relationships with public authorities and the community in general.

Some examples of recovery options at the level of personnel are the definition of a plan of succession, or a primary and alternate plan, or alternate plans; travel ban policies of primary and alternate personnel traveling at the same time and using the same means; ban to take vacations simultaneously; implementation of health and emotional control programmes for personnel identified as critical.

Examples of recovery options at the level of physical infrastructure are the definition of alternative sites of operation with the guarantees of public services supply from different sources; agreements with hotels; training halls; to re-use the space of the sales force (if it were not urgent to recover).

Examples of recovery options at the level of materials, inputs or consumables are to create small inventories in strategic places; to establish agreements on the provision of inventories with several suppliers; to establish reciprocal agreements with similar organizations to provide mutual help in the case of a disruptive event.

Examples of recovery options at the level of equipment are renewal of equipment and to maintain the old ones for spare parts, maintain operational the obsolete services at a minimum level of operation; to assemble mock-ups or transportable machinery (if possible) to take it to the place affected; or to have identified the equipment of not so critical services to dismantle, take to the affected place and assemble it at that place.

Examples of recovery options at the level of computer systems are to replicate the computer centre in an alternate site whether entirely or a part of it in accordance with what has been identified as the most critical one; to outsource the IT service and move it to the "cloud"; to make backups and restore them as soon as they are needed.

Examples of recovery options at the level of financial feasibility are to maintain the contingent lines of credit to assume the needs at the time of the incident; to maintain cash available to have access to it and be able to comply with cash needs during the incident; to establish procedures for registration and control of damages and expenses associated with the incident for subsequent claims to the insurer; to have agreements on deferred payments with the suppliers in the case of major incidents.

Examples of recovery options at the level of suppliers are to have more than one supplier for the provision of a good or a service and, if it cannot be, to establish joint response procedures in the face of a disruptive incident; to measure the level of maturity in accordance with the BCMM[4] of the supplier to demand in time the appropriate level of preparation in view of disruptive events.

An example of recovery options at the level of relations with the clients is to have crisis communication procedures considering possible scenarios of image tarnishing and prioritizing the affected audiences.

Examples of options at the level of internal and external communications are to maintain the acquisition and assembly of a massive notification system and collaboration platform to be used during the disruptive incident; to acquire mobile phones from different suppliers; to acquire satellite phones; to have pre-established agreements with the media and broadcasters to disseminate key messages in case there is no other means available.

Finally, an example of an option of the relationships with regulators and public authorities is to establish beforehand channels to be mutually notified and helped as soon as the disruptive incident occurs.

[4] The BCMM (Business Continuity Maturity Model) is a model developed by the Virtual Corporation company to be explained later on.

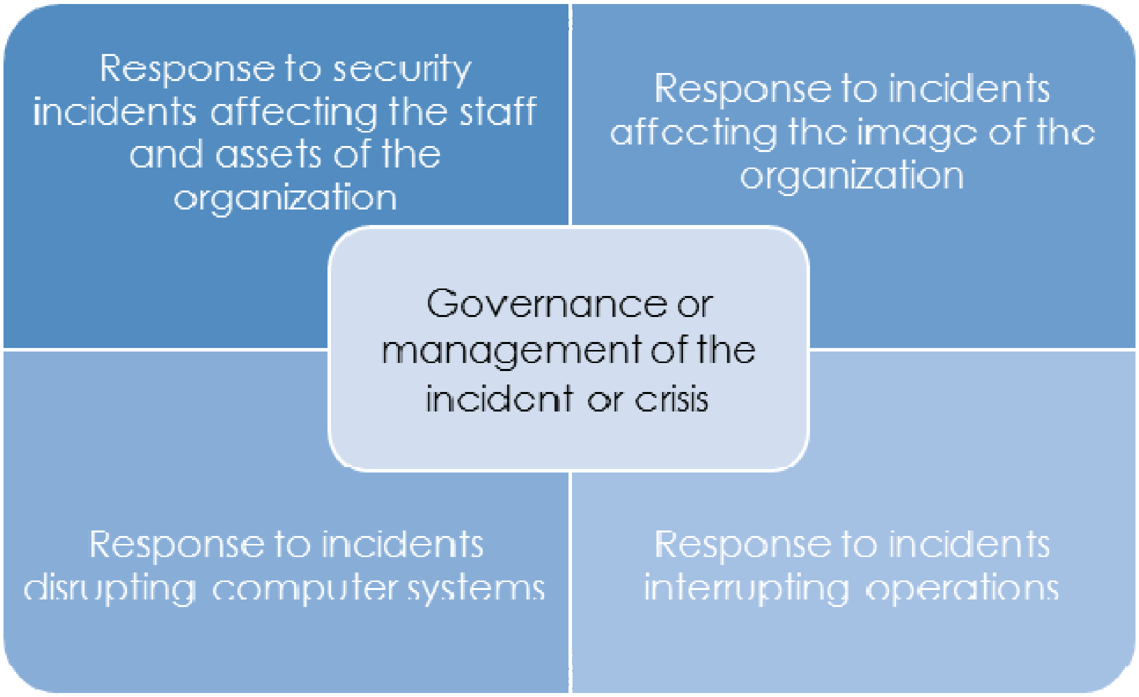
5. Document the plans of action to apply at the time of the event

The continuity plans formalize the strategies in a document that should be consulted and used during the disruptive incident. So it is important that it is easy to read and be made as an aide-memoire to remember what has to be done; it is not a procedure at the minimum level detailing the steps to take by any person available at the time of the disruptive incident, even worst if that person is inexperienced with the service or activity to recover.

Before documenting the protocol of action, it is important to create a document model or template that will not necessarily follow the same guidelines that are followed in the procedures for consultation, guidance, or training in the daily activities of the organization and that are used in normal situations; therefore, it is necessary to create a space to talk and make understand the differences between a procedure for continuity and a day-to-day procedure. A procedure for continuity does not look for documenting new procedures of operation invented for the contingency; indeed, the premise is that the same daily procedures will continue, but with different priorities, even at the point of not doing any non-urgent activity in months. A procedure for continuity might incorporate manual procedures to be used when the systems are not available; the manual procedures are an additional form of operating the day-to-day activities without computer systems; although nowadays it is probable that to think about operating manually is no longer an option due to the need for operating large volumes of transactions or orders, in addition to the security and fraud risks to which the organization is exposed.

The general structure of any continuity plan will be: objectives and extent; recovery priorities by MTPDs and RTOs; team for response, or continuity, or recovery; team activities, preferably by role; strategy to use at personnel level, that is, personnel assigned to the roles (more than one per role); strategy to use at physical infrastructure level, that is options of operations sites; strategy to use at the level of materials, consumables, that is where the necessary resources are found; and thus for each one of the types of resources that have been considered in the recovery strategies; there can be complemented with annexes such as contact data, location blueprints, templates to use at the time of the incident.

TABLE 3
Types of plans by type of objective


Response to security incidents affecting the staff and assets of the organization
Response to incidents affecting the image of the organization
Governance or management of the incident or crisis
Response to incidents disrupting computer systems
Response to incidents interrupting operations

The continuity plan from a general perspective can be classified into five categories according to the objective of what is intended to protect: continuity plans for response to security incidents affecting personnel and physical assets of the organization; continuity plans for response to incidents tarnishing the image of the organization; continuity plans for response to incidents disrupting computer systems; continuity plans for response to incidents disrupting operations; and the continuity plan that controls the management of any of the incidents through a Crisis Committee.

In the case of the continuity plans for response to security incidents of personnel and assets of the organization, the main objective is to try to safeguard the operation of service or activity in the physical place where it has been affected in face of specific scenarios, for example: what to do to minimize the impact on personnel in the case of a pandemic, what to do to minimize the impact on personnel and the assets of the organization in case of a fire or earthquake, what to do to minimize the damages to the personnel and the assets of the organization in the case of a dangerous spill. The type of incidents will be related with the risk assessment of the most probable or stronger impact threats.

In this case, the teams will be more oriented to first response brigades, such as: evacuation, fire, among others, and they will prioritize the protection of the physical assets according to the urgency level of the processes that use them, whose information was identified along with the MTPDs and RTOs.

In the case of the continuity plans for response to incidents tarnishing the image of the organization,, the main objective is to safeguard the reputation of the organization establishing what possible risks of image tarnishing exist, what audiences are affected and what is the priority, what media are appropriate for each audience and which spokesmen are established to send the message. The team in this case will be led by the person responsible for the institutional image and his support personnel, as well as the own spokesmen.

In the case of the continuity plans for response to incidents disrupting computer systems, the main objective is to continue providing the services of information technology and communications along with the organization's data and information. The recovery priorities will be set as a function of the RTOs that have been defined for the information technology (IT) services, and in regard to the services or activities they support; that is, an IT service RTO should be the minimum of all the RTOs of services or activities that use such IT service. The recovery team of the information technology services will be formed by the authority in information technology that will participate in the most important decisions in the recovery, in addition to maintaining informed the authorities of the organization. There is also part of this team the technical personnel, at the level of servers, databases, telecommunications and applications, responsible for the recovery at the operation level of the information technology services.

In the case of the continuity plans for response to incidents disrupting operations, the main objective is to continue providing the services and activities of the organization. The recovery priorities will be set as a function of the RTOs defined for the services or activities. The recovery team of operations continuity will be led by the heads of the functional units or leaders of the processes (depending on the best way in which the organization is structured to respond to a disruptive incident, the key part being the leadership capacity that the organization can assume during the incident). There is part of the team the personnel of the key posts to carry out the minimal activities according to the established RTOs.

In the case of the continuity plan to control the management of any incident,, the main objective is decision making for decisions on any of the types of plans mentioned above through the establishment of an Incident or Crisis Management Committee. This crisis committee formed by the organization authorities will be the team that must be convened to support the decisions of the team responding to the security incident of personnel, or the team that is protecting the reputation, or the one recovering the information technology services, or that recovering the functional units of the business.

Since the disruptive incident might occur when the organization has not finished implementing its recovery strategy options (for example, an alternate site not implemented yet), then it is the work of the Incident or Crisis Management Committee to improvise and succeed in implementing the missing strategy, so that the other continuity and recovery teams that depend on such strategic options can achieve the objective of responding to the disruptive incident.

6. Train for and test the plans of action

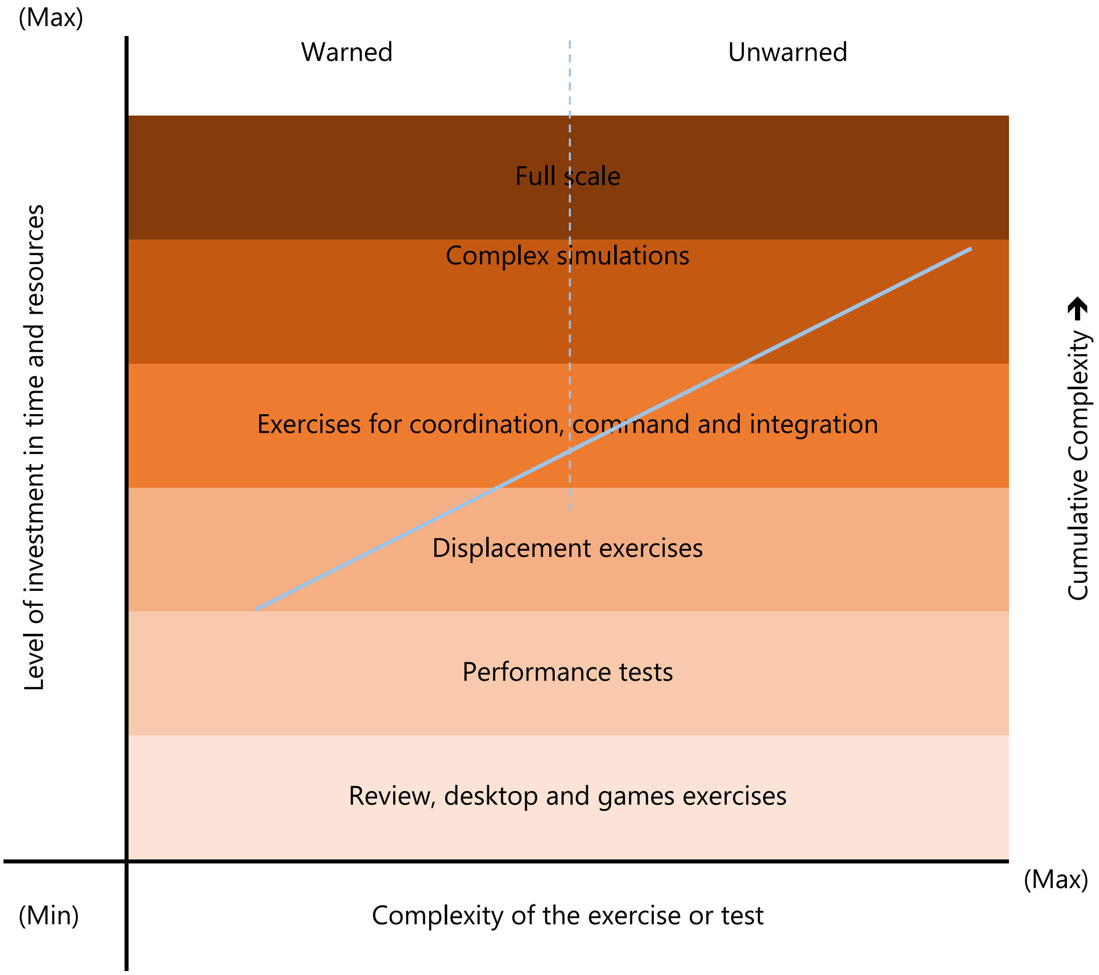
The plans of action will be only paper and will not go any further without training, and indeed the success of the plan at the time of a disruptive event is not in how well documented the plan is, but how well it has been trained for and internalized, therefore, the main objective of an exercise is training in the plan and exposing it, progressively, to the highest stress possible to identify the opportunities for improvement that it can have and/or determine the additional skills the participant personnel need to be trained in, thus the objective of training in the plan is not to see whether it works or not, but in view of the tested scenario to determine what the plan and the people lack to be able to respond better. When the test scenario is already tamed, it should be increased in complexity or in any case changed, but always according to the maturity of continuity in the organization.

A real life example that helps understand what was previously said is "go out for a run". There can be taken the objective scenario "to go running in a week around the block" as well as "to go running in a week the 42 kilometre marathon hoping to achieve a classifying time for the next Olympic Games". What does it depend on to choose a less stressful scenario or another scenario of total stress? Clearly, the level of preparation of the person. It would be unwise to force an enthusiast person that has never been prepared to run professionally to participate in the marathon and classify for the Olympic games because it might likely cause him a considerable health damage; on the other hand, it is not reasonable to ask a person who runs four kilometres daily to exercise running around one block, since the opportunities for improvement have not been forced to appear in the technique of running of the person or in the implements used. The ideal will be to identify what preparation the person has and according to that the objective scenario will be set. If the person has never gone out to run, clearly asking to run around one block will be an adequate objective; but once that objective is fulfilled, the objective will have to be increased, maybe now the person should be asked to run one kilometre, and so on. But not to be judge and part in the preparation of the person, this should be readied in time, for example, in three months, what does this person expect to achieve? It could be for the first month to run around a single block, the second month to run one kilometre, and the third month four kilometres.

As in the previous example, an organization that is just starting its business continuity programme cannot have the super complex proof that implies to shut off its operations and operate with the alternative options that the strategies defined, and in a time shorter than the required RTOs. Probably it only starts with a general fire scenario with desk exercises, validating the functioning of certain critical equipment, and emphasizing the evacuation of personnel; afterwards, there may be the same fire scenario with wounded people, as a result part of the personnel is indisposed after the evacuation, therefore, the alternates will participate in the desk exercises; thus progressively the exercise complexity will be increased. It is clear that there is no need to wait ten years for the alternate infrastructure of information technology to function properly; it is likely that the first scenarios will aim at ensuring that the alternate information technology is ready and in operation in two or three years.

Also, the organization must plan its test objectives over time, i.e., what does it expect to achieve in one year, two, three, maybe five years, and thus, the organization itself sets its own objectives which will be validated year after year. It is good to keep in mind that unlike the example of the runner where he surely goes out to train daily, the organization in regard to continuity will not do the exercises daily; the frequency of the exercises should be relative to give room to the organization in meeting its operation objectives; as a result the complexity levels in business continuity will be progressive at the very pace that the organization established, of course, not to let much time pass so that the personnel forgets, or in view of the changes in the organization the plans no longer work.

CHART 3
Exercises by complexity


(Max)
Warned
Unwarned
Full scale
Complex simulations
Exercises for coordination, command and integration
Displacement exercises
Performance tests
Review, desktop and games exercises
Level of investment in time and resources
Cumulative Complexity
(Min)
Complexity of the exercise or test
(Max)

The types of exercises range from the least complex and in turn less expensive to the most complex and expensive. The least complex ones are the exercises of review, desk and games, whose objective is mainly to disseminate and create knowledge on the use of the plan and the strategy options that are available in the organization. Then there are the performance tests of the infrastructure and the equipment to ensure that they are operational and functioning, and the personnel that operates such equipment knows their operation and does it fast within the established time objectives. Then there are the displacement exercises that intend to offer knowledge about the places where to move to, how or with what means to move and be able to move within the established time objectives. Then there are the exercises for coordination, command and integration where more than a team of response, or continuity, or recovery participate in an integrated way under the coordination of the incident or Crisis Management Committee. Then there are the more complex simulations that can be a combination of the previous ones and usually it is the objective exercise of the year for which, with the use of the previous exercise, the organization has been preparing but always without affecting or shutting off some critical service. And finally, there is the full scale exercise where in addition to what is simulated, it seeks to shut off a critical service and recover it within the expected times with the risks that this represents, and to the greatest possible extent in controlled environments.

The purpose of performing an exercise without warning does not seek "to see if the plan works". If there is no warning it is because it seeks to create in the personnel competences in dealing with stress and adequate levels of alert for a disruptive event; although the participants are not notified, the corresponding authority must always be informed so that any risk of unavailability of the service can be anticipated. The exercises with no warning can belong to any of the types of exercises, for example, there might be no warning for a desk exercise and, in this way, to evaluate the level of commitment and importance of the people, regarding business and operations continuity.

7. Raising awareness and competences in the organization

The personnel of the organization has the responsibility of undertaking the activities for which it has been appointed, although the topic of continuity could be recognized as important, the day-to-day activities will make that within its priorities the topic of continuity drops each time in importance over time. Therefore, creating a culture of continuity of business and operations within the organization is a task that should be constant.

If the topic of continuity has not been implemented yet in the organization, the type of awareness will be different and will seek to sell or justify the need for establishing a business continuity programme, either from: past incidents, incidents that happened in other organizations, regulatory or legal obligations, or audit requirements. If the continuity is already implemented, then the objective will be to remind the personnel that it is an important topic to be prepared for because "it might happen".

It is necessary to work with the person responsible for internal communications of the organization to structure the best ways to deliver the message to the personnel and use the appropriate means to do it. Mechanisms that can be used are: bulletins, Web sites, posters, talks, games, and once a year the workday or the week for continuity.

Awareness raising must be focused on the type of target audience and should always have indicators to measure whether the desired results are being achieved; otherwise there is no way to know if the method used is being effective and there is no way to enter the cycle of continuous improvement.

The creation of competences has a different objective from that of raising awareness, and it is mainly to create knowledge and experience in different subjects or disciplines of continuity. The subjects may deal with concepts of continuity of business and operations, considering the specializations: response to incidents of security of personnel and critical assets, response to incidents of image tarnishing, response to incidents of disruption to information technology, response to incidents of disruption to operations, or governance and management of incidents or crisis; also the use and application of the options of recovery strategies and continuity plans where the exercises will be very successful as tools of creation of knowledge and experience; and also in the carrying out of day-to-day activities by the alternates, especially, as it would be done by the one designated as primary.

Training should also be focused on the type of personnel and according to the capacities that need to be created; as well as awareness about the results should be measured to establish whether it is being effective and is complying with the objectives of capacity building.

8. Maintaining continuity of business and operations

The organization is always changing, people change, responsibilities change, services change, buildings and facilities change, systems change, suppliers and other parts of the organization change. Therefore, one of the most important challenges of continuity is to achieve that, despite the changes in the organization, continuity does not become outdated.

The success in change management hinges on identifying changes, and for this purpose it is necessary to know who can inform about it and how often the source of change must be asked. For example, the source of change in personnel can be Human Resources and the frequency to ask them is every fifteen days, the means used is a format showing hiring, dismissals and personnel movements, sent by e-mail. Another example has to do with the changes in computer systems, the source is the IT department and, specifically, the committee of IT changes and the frequency to ask is once a month, participating in the meetings by invitation of such committee.

Since the organization undergoes many changes, indeed the ones to get the attention are those that impact directly the continuity. They are: changes in services; processes or activities; people, transport and communications; physical infrastructure, public services and work environment; equipment, materials and consumables; information technology services; suppliers; financial feasibility, among others.

Once a change of interest for business continuity is identified, it should be registered in a logbook of change events and analyse the impact on the outdatedness of the programme of business and operations continuity. If the impact is low or moderate, it is possible to wait until the updating cycle of the next year to include it. If the impact is high or very high, the work plan of operations for the current year (of continuity) should be modified, and the update of the components of continuity should be conducted as necessary.

Once the change is made in one or more documents of the programme of continuity, a register should be kept of what changed, who changed it and who approved what was changed and, which 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 ask for the obsolete versions of the document and storage them or destroy them and hand over the new versions; even asking for the signing when receiving the new copies.

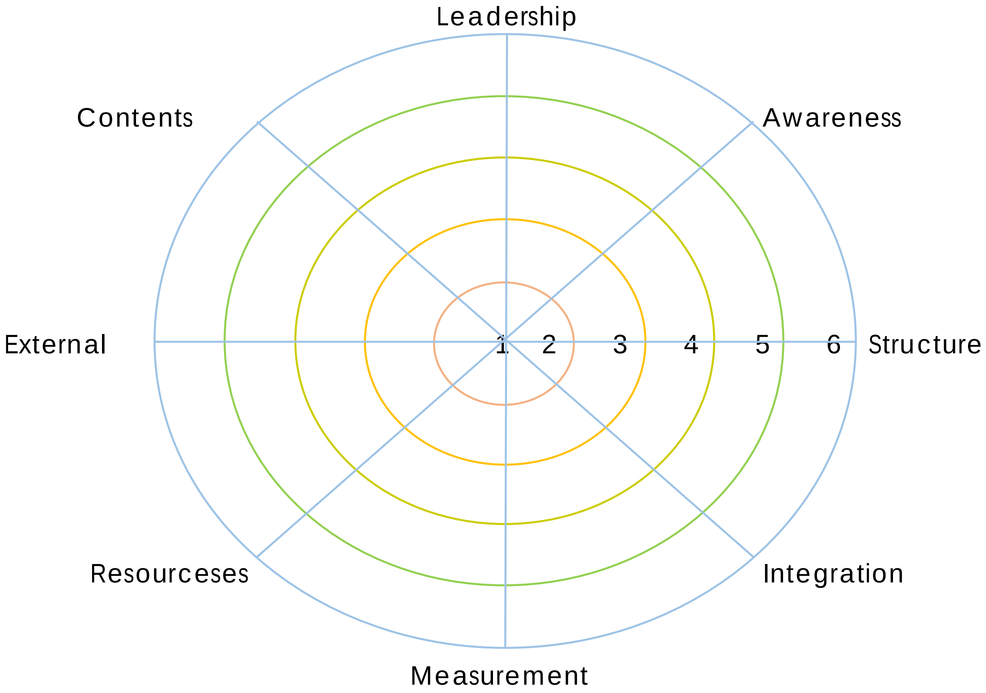
The document of the plan is a controlled document. The owner of the department or process of the plan is responsible for the content and the continuity coordinator is responsible for the access to the document and to distribute it only to those that need the plan to be handed over.

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

An organization without indicators that measure its progress or without a strategic plan will not have how to measure its improvement over time. The same happens with the programmes of continuity of business and operations; if its maturity is not measured and the strategic objectives are not formulated over time it may not show the authorities whether it is improving or not. A successful continuity of business and operations is not only measured by the generated continuity plans, but also by other factors that must be involved to say that the programme of continuity of business and operations is on the right track.

The BCMM Model is the oldest and most disseminated one in the industry and allows for comparing the degree of maturity of the programme of continuity of business and operations in the organization. It establishes eight competences that the organization must accomplish: (1) leadership from the authorities; (2) awareness and interest from the personnel in general; (3) structure, roles and responsibilities; (4) internalization and integration with the internal and external parties; (5) measurement of more accurate indicators of continuity; (6) to count on competent resources and make investments according to the desired scenarios to be protected; (7) assurance of the chain of supplies and the management of expectations of third parties; and (8) methodological order in line with best practices.

TABLE 4
Strategic variables of continuity according to the BCMM



The BCMM evaluates each corporative competence in a six level scale: level 1, the lowest one, where efforts in continuity are not put in; level two, where at least one functional department is putting some effort in, by its own initiative; level 3, where several functional departments try to coordinate efforts through a work commission; level 4, where the organization is applying a better practice and there has been established a function of continuity of business and operations; level 5, where the organization has gone from theory into practice in the application of the best practices and is implementing a programme of continuity of the organization in the whole organization (within the scope of continuity) although not with plenty of success in some departments; and level 6, where the organization carries out a regular and constant practice of excellence, and all the functional departments are highly compromised, there are strategic options, and they often put their plans into practice.

If the result from the evaluation of maturity obtained between one and two, then the model indicates that the organization is at risk; if it obtains three or four, then the model indicates that the organization is being competent; if it gets five or six it means that it is achieving excellence.

Based on the BCMM result there can be estimated progressive objectives over time, for example: the first year to reach level three; the second year to maintain the level; the third year to reach level three. Another example could be: the first year to reach level four in the competences in leadership and awareness, and in the rest at least level three for the departments with an RTO shorter than four hours; the second year to reach level four in all the competences for the departments with zero RTO, and for the departments with an RTO equal to twenty-four to reach level three in the competences in leadership and awareness.

Just like the previous examples, it could be possible to consider objectives for three, four or five years, and annually review their compliance and make a comparison to the previous year. If they are not met, the strategic objectives of continuity will have to be re-evaluated from time to time to assess them fully as the organization matures.

II. IMPLEMENTATION GUIDE

1. Guide for the Implementation of the 9 Methodological Phases

This section provides a methodological guide for the implementation of a Programme for Continuity of Business and Operations in MSMEs. With this guide, working plans may be structured both for the implementation for the first time of a business continuity program and its subsequent maintenance through time.

A program for continuity of business and operations is not to be understood as a project that ends once the plans are documented and the first trial is conducted, but as an ongoing process of continuous improvement that must be revised on an annual basis.

#	Phase	#	Methodological activity
1	Empowerment and Governance in the Continuity of Business and Operations	1	Identify participants or "owners" of specialties and disciplines of continuity of business, who will be involved, as deemed appropriate, in any of the methodological activities described in this guide. *Note: A suggestion is made to consider the following:* - *Executive Sponsor of business continuity* - *Owner of the sector related to communications amid crises* - *Owner of the sector related to emergencies and protection of staff and facilities* - *Owner of the sector related to key business processes* - *Owner of the sector related to information technologies*
		2	Define Roles and Responsibilities for Business Continuity
		3	Prepare and approve the Business Continuity Policy
2	Identify priority and urgent activities to recover	1	Establish the scope of the Business Continuity Programme at the level of Products and Services
		2	Identify the threats that are most likely to occur and could prevent the product or service within the scope from being delivered
		3	Define the non-tolerable thresholds for the organization
		4	Estimate the Maximum Tolerable Period of Disruption (MTPD) for the product or service considered within the scope *Note: Consider 2.2 and 2.3 as inputs*
		5	Estimate which would be the Minimum Business Continuity Objective (MBCO) for the product or service considered within the scope
		6	Identify the essential activities to support the product or service considered within the scope

#	Phase	#	Methodological activity
		7	For each activity, estimate the MTPD depending on the MTPD of the product or service
		8	For each activity, identify which could be the strategy for recovery (with current capabilities) and the time that that it would take *Note: This value could be the Recovery Time Objective (RTO) if it does not compromise the MTPD*
		9	For each activity, define the Recovery Time Objective (RTO)
		10	Identify the Functional Departments that are carrying out the activities
		11	For each Functional Department, identify the staff that needs to be considered for each RTO of the activities being carried out, taking into account the MBCO
		12	For each functional Department, identify the environment(s) that need to be considered for the RTO for each activity being carried out, taking into account the MBCO
		13	For each Functional Department, identify the equipment that needs to be considered for each RTO of the activities carried out, taking into account the MBCO
		14	For each Functional Department, identify the informatics systems that need to be considered for each RTO of the activities carried out, taking into account the MBCO
		15	For each Functional Department, identify the key information that needs to be considered for each RTO of the activities carried out, taking into account the MBCO
		16	For each Functional Department, identify the key suppliers that need to be considered for each RTO of the activities carried out, taking into account the MBCO
		17	For each Functional Department, identify the economic and financial resources that need to be considered for each RTO of the activities carried out, taking into account the MBCO
3	Protect the most urgent activities	1	Define which are the most urgent activities *Note: Consider 2.9 as an input, and that the definition of urgent could be RTO less or equal to one week (as a suggestion)*
		2	Identify the most critical offices of MSMEs where the most urgent activities are conducted

#	Phase	#	Methodological activity
		3	Identify global, continental, regional, national, local and internal threats that could cause an interruption of the resources that are required for urgent activities
		4	Define the risk matrix, identifying the applicable probability scales and impact scales, and which is the level of unwanted risk
		5	For each office, identify and assess the efficiency of existing controls to mitigate a stoppage of each resource vis-à-vis the possible occurrence of each identified threat
		6	For each office, for each threat, for each resource, assess the risk level (probability and impact), considering existing controls
		7	In case there are resources exposed to unwanted risk levels, identify improvements or new control measures to lower the risk level
4	Establish strategies for continuity and recovery of the activities	1	Consolidate at the level of all MSMEs the amounts of resources for each one of the RTOs that have been identified for each Functional Department *Note: Consider 2.11, 2.12, 2.13, 2.14, 2.15, 2.16 and 2.17 as inputs*
		2	For each type of resource and for each time frame, define the most appropriate and cost-efficient strategies, in accordance with the required amounts *Note: As a suggestion, the following time frames could be considered: Minutes, Hours, 1 Day, Some Days, 1 Week, 2 Weeks, 1 Month and More than 1 Month*
		3	Define response strategies related to crisis management - Create the Incident or Crisis Management Committee - Define the place(s) for a Crisis Management Room - Identify the resources needed for a Crisis Toom - Define a general action mechanism for the Incident or Crisis Management Committee
		4	Define response strategies related to communications amid crisis - Identify reputation risks - Identify audiences affected by each risk (scenarios) - Identify communication mechanisms / ways / means - Identify appropriate roles and spokesmen by

#	Phase	#	Methodological activity
			audience - Design key pre-designed templates or messages - Define a general performance mechanism of the identified roles and spokesmen
		5	Define the response strategies related to safeguarding lives and facilities - Define the most relevant scenarios (considering 3.3 as an input) - For each scenario, create an appropriate brigade team - Define the necessary equipment to be used during the emergency - Define a general mechanism for action for the brigade team
		6	Establish an implementation plan for the identified preventive, continuity and response strategies *Note: Consider 4.2, 4.3, 4.4 and 4.5 as inputs*
		7	Execute a plan of action for implementation of the strategies
5	Document the plans of action to apply at the time of the event	1	Identify a team of experts to document business continuity procedures
		2	Define the structure and amount of plans to outline on the basis of the size and complexity of the organization *Note: Consider as suggestions:* - Small organization: ▪ *A document for management, communications amid crises and business continuity* ▪ *A document for scenarios or type of emergency for emergency response* - Mid-sized organization: ▪ *A document for management and communications amid crises* ▪ *A document for continuity of business* ▪ *A document for continuity of informatics systems (Disaster Recovery Plan, DRP)* ▪ *A document for response depending on scenarios or type of emergency*
		3	Define templates to document plans in a standardized way
		4	Prepare documents on procedures for Emergency Management
		5	Prepare documents on procedures for Incident

#	Phase	#	Methodological activity
			Management or Crisis Management
		6	Prepare documents on procedures for Communications amid Crises
		7	Prepare documents on procedures for Continuity of Business in case of disruption of operations in MSMEs
		8	Prepare documents on procedures for Continuity of Business in case of disruption of informatics systems in MSMEs
6	Train for and test the plans of action for continuity	1	Prepare a Programme of Tests and Exercises that consists of a series of exercises each one more complex than the previous one Note: A recommendation is made for the Programme to have a 3-year span, but the first time it can be one year
		2	For each exercise, to establish: - Objectives / purpose - Scope of what is being tested, or not - Type of exercise / test - Scenario under consideration (Note: Consider 3.3, 3.6 and 3.7 as inputs) - Participants - Schedule for preparing the exercise - Script for execution (during the exercise) - Injectors to consider during the exercise - Formats to use for evaluation during the exercise - Expected results - Risks of the exercise - Special considerations to take into account as a result of previous actual incidents or exercises conducted before
		3	For each exercise, identify expectations of interested parties
		4	For each exercise, confirm objective, scope and scenarios that best serve to meet the expectations of interested parties
		5	For each exercise, define participants according to their roles: Planner, Facilitator(s), Observer(s), Executor(s)
		6	For each exercise, prepare the script determining the baseline and injectors that will be considered during its execution
		7	For each exercise, prepare all logistics aspects (transport, meals, coffee, water, permits, among others)

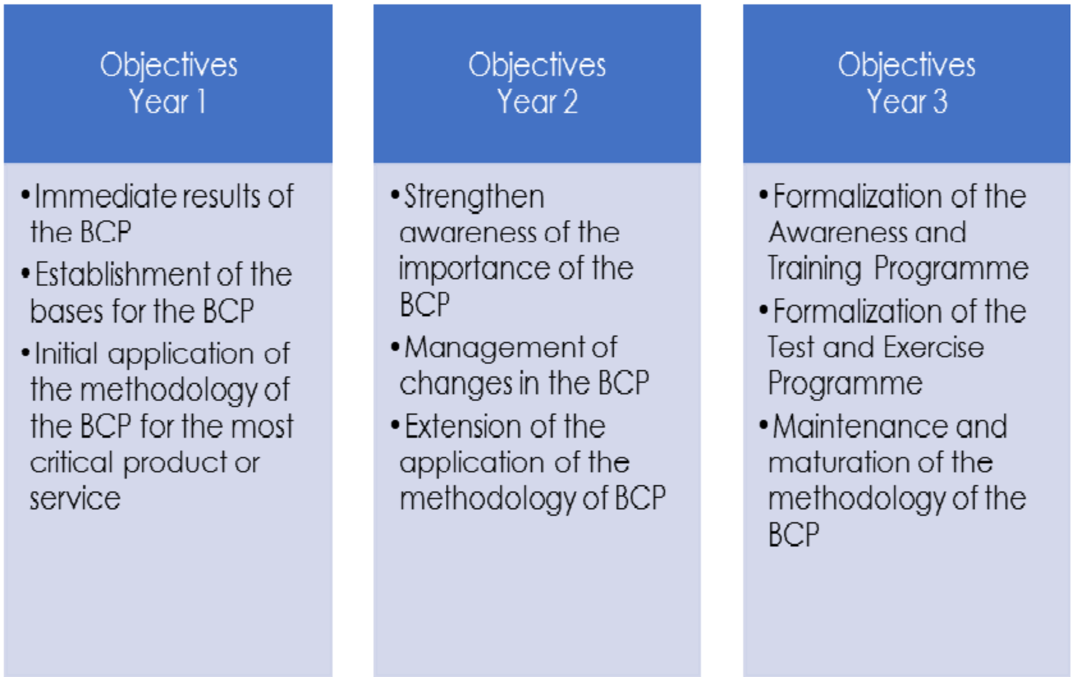
#	Phase	#	Methodological activity
			Note: Those elements that form part of the scope of the exercise and should be procured by the participants during the execution of the exercise should not be considered
		8	For each exercise, prepare the formats for evaluation of the exercise
		9	Carry out exercise in accordance with the established script
		10	Once the exercise is completed, to make an immediate session on lessons learned
		11	Prepare a report on the exercise, determining if the objectives were met and if the observations of previous exercise were overcome
		12	Submit a report and make recommendations for future exercises
		13	If necessary, update the Test and Exercises Programme
		14	Apply all the recommendations and updates that have been suggested in the report on the exercise
7	Raising awareness and competences in the organization	1	Jointly with the Human Resources department, define the competencies required for each role in business continuity
		2	Make an evaluation of the level of competition achieved by each person according to his/her role in business continuity
		3	Determine annual objectives to improve the level of competence of each person
		4	According to the identified improvements, propose capacity building initiatives
		5	Add up initiatives for raising awareness on issues concerning business continuity and formalize a Business Continuity Training and Awareness Programme *Note: For raising awareness consider the following ideas:* - Posters - Screen savers - A business continuity day - Publications in the internal bulletins of MSMEs
		6	For each initiative, consult with the communications or human resources departments in order to outline the form of execution
		7	Execute initiatives

#	Phase	#	Methodological activity
		8	Measure the results achieved at the end of each initiative and keep corresponding records
		9	Assess whether the objectives of the Business Continuity Training and Awareness Programme are being achieved or if adjustments are required on the basis of obtained results
8	Maintaining continuity of business and operations	1	Identify areas of the organization that may be sources to identify changes in the organization
		2	Reach agreements with those areas by establishing the frequency of exchanges of information on possible changes
		3	Apply the agreements and identify the changes in a permanent way
		4	For each change, evaluate the impact on the Business Continuity Programme. If it is a high impact change, define the most appropriate date to execute the update as soon as possible; otherwise, consider the change as an input for the annual working plan of the Business Continuity Programme for the following year *Note: A change in one component of the programme could involve changes in other components of the programme. For example, a change at the level of people may involve a change in the training program to include new staff in the training programme*
		5	In case of an update of the business continuity programme, keep track of the changes in the corresponding documents and control of the corresponding versions
		6	In case of a change in any of the business continuity plans, distribute new versions and ensure the collection, retention, and further destruction of non-current versions
		7	At the end of the year, prepare an annual working plan for updating the Business Continuity Program based on visible changes in the organization and the identified changes that were not prioritized as urgent during the year
9	Indicator of maturity and strategic planning for continuity of business and operations	1	Understand the application of the Business Continuity Maturity Model (BCMM)
		2	Plan the applications of the BCMM
		3	Apply the BCMM and identify the current situation of Business Continuity Plan
		4	Establish improvement targets for one, two and three

#	Phase	#	Methodological activity
			years in each of the Corporate Competences of BCMM Model
		5	Propose a Strategic Plan for Business Continuity which aims at implementing the opportunities for improvement identified
		6	Apply again the BCMM Model at least once a year and determine which objectives have been accomplished and, whenever necessary, to update the Strategic Plan for Business Continuity

2. Practical proposal to apply the 3-year Methodological Guide

Applying the nine-phase implementation guide, one after another, can be a major effort for MSMEs, with visible results in the medium term. In many organizations, mainly those exposed to frequent major risks, the need for results has to be more immediate. For this reason, we propose a three-year working plan with a practical perspective that leads to achieve more immediate results, while creating a Programme for Business Continuity that is more solid and sustainable over time.



Objectives Year 1

- Immediate results of the BCP
- Establishment of the bases for the BCP
- Initial application of the methodology of the BCP for the most critical product or service

Objectives Year 2

- Strengthen awareness of the importance of the BCP
- Management of changes in the BCP
- Extension of the application of the methodology of BCP

Objectives Year 3

- Formalization of the Awareness and Training Programme
- Formalization of the Test and Exercise Programme
- Maintenance and maturation of the methodology of the BCP

Year 1			
Objective	Specific objective	#	Methodologic Activities
Immediate results of the BCP	Engage the support of key personnel	1.1.	Identify participants or "owners" of specialties and disciplines for business continuity, who will become involved as appropriate in any of the methodological activities
		2.2.	Identify the threats most likely to occur and that could prevent products or

Year 1			
Objective	Specific objective	#	Methodologic Activities
			services from being delivered
		7.7.	Conduct an awareness raising talk on the importance of business continuity
	Prepare a Plan for Incident Management or Crisis Management	4.3.	Define the response strategies related to Crisis Management
		5.5.	Prepare documents on procedures for Incident Management or Crisis Management
		6.2. to 6.14.	Perform a desk exercise on Incident Management or Crisis Management
		4.7.	Implement the Response Strategies for incident Management or Crisis Management
	Complement the Plan for Incident Management or Crisis Management with Communications amid Crises	4.4.	Define response strategies related to communications amid crises
		5.6.	Prepare documents on procedures for communications amid crises
		6.2. to 6.14.	Conduct a desk exercise on communications amid crises
		4.7.	Implement the response strategies on communications amid crises
	Prepare an Emergency Response Plan for the most relevant scenarios	4.5.	Define the response strategies related to safeguarding lives and facilities
		5.4.	Prepare documents on procedures for Emergency Management
		6.2. to 6.14.	Conduct a desk exercise on Response to Emergencies
		4.7.	Implement the Emergency Response Strategies
Establishment of the bases for the BCP	Draft the Policy on Business Continuity	1.2.	Define Roles and Responsibilities for Business Continuity
		1.3.	Prepare and approve the Policy on Business Continuity
Initial application of the methodology of the BCP for the most critical product or service	Select the most critical Product or Service	2.1.	Establish the initial scope of the Programme for Business Continuity at the level of Products and Services
	Identify the most urgent activities to recover	2.3. to 2.17.	Make a Business Impact Analysis (BIA)
	Prepare recovery	4.1.	Consolidate resources and design

Year 1			
Objective	Specific objective	#	Methodologic Activities
	strategies	to 4.2.	recovery strategies
	Prepare the Plan for Business Continuity for the most critical Product or Service	5.1. to 5.3.	Identify team for preparing the plan and making preparations for documents
		5.7	Draft documents
		6.2. to 6.14.	Conduct a desk exercise on the prepared plan

Year 2			
Objective	Specific Objectives	#	Methodologic Activities
Strengthen awareness of the importance of the BCP	Build capacities in Business Continuity	7.7.	Execute a specialized training in business continuity for all the participants in the Business Continuity Programme
Management of changes in the BCP	Prepare an Annual Work Programme	8.7.	Prepare an annual work plan for updating the Business Continuity Program based on visible changes within the organization with respect to Year 1
	Update the activities conducted during Year 1	4.7.	Implement the Strategy for Continuity of Products and Services for Year 1
		8.5.	Make the changes in the program and keep track of the changes in the corresponding documents and control of the respective versions
		8.6.	In the event of any change in any of the plans drawn up during Year 1, distribute new versions and ensure the collection, retention and further destruction of non-current versions
Extension of the application of the methodology of BCP	Protect the most critical activities concerning the Products or Services for Year 1	3.1. to 3.7.	Conduct an analysis of threats and evaluate risks for the most critical activities
	Prepare Continuity Plans for the rest of key Products or Services, including Informatics Systems	2.1.	Determine the scope of the Business Continuity Programme at the level of Products and Services
		2.3. to 2.17.	Conduct the Business Impact Analysis (BIA) for the rest of Products or Services
		4.1. to 4.2.	Consolidate resources and outline a recovery strategy, including that corresponding to information

Year 1			
Objective	Specific objective	#	Methodologic Activities
			technologies
		5.1. to 5.3.	Identify team to document continuity plans and to make preparations for documents
		5.7	Draft documents
		6.2. to 6.14.	Conduct a desk exercise on the business continuity plans established during year 2, including recovery plans in case of disruption of informatics systems
	Conduct a more complex exercise	6.2. to 6.14.	Conduct a more complex exercise or simulation
	Measure the maturity of Business Continuity	9.1. to 9.3.	Apply the BCMM
Year 3			
Objective	Specific Objectives	#	Methodologic Activities
Formalization of the Awareness and Training Programme	Draft the Awareness Raising and Training Programme	7.1. to 7.6.	Outline initiatives for the Awareness Raising and Training Programme on Business Continuity
	Apply the Programme	7.7. to 7.9	Apply initiatives and measure results
Formalization of the Test and Exercise Programme	Draft the Test and Exercise Programme	6.1.	Design the Test and Exercise Programme
	Execute the exercises for the year	6.2. to 6.14	Execute exercises
Maintenance and maturation of the methodology of the BCP	Design the maintenance programme	8.1. to 8.2.	Identify areas that may provide information on possible changes and reach agreements with them
	Apply the maintenance programme	8.3. to 8.4.	Apply the maintenance programme
		8.5.	Make changes and keep track of the changes in the corresponding documents and control the respective versions
		8.6.	In case there is a change in any of the plans, distribute the new versions and ensure the collection, retention and further destruction of non-current

Year 1			
Objective	Specific objective	#	Methodologic Activities
			versions}
	Measure the maturity of Business Continuity	9.1. to 9.3.	Apply the BCMM
	Prepare a Strategic Plan for Business Continuity	9.4. to 9.6.	Draft a three-year Strategic Plan for Business Continuity
	Prepare and execute Annual Work Plan	8.7	Prepare and execute Annual Work Plan for Business Continuity, considering the changes and including the improvements suggested in the Strategic Plan

BIBLIOGRAPHY

ASIS International. *ASIS SPC.1: Resiliencia Organizacional: Sistemas de Gestión de la Seguridad, Preparación y Continuidad. United States*, 2009. (available at *http://www.ndsu.edu/fileadmin/emgt/ASIS_SPC.1-2009_Item_No._1842.pdf*)

Disaster Recovery Institute International. *Diez prácticas profesionales.* New York, United States, 2013. (available at *http://www.drii.org/*)

DRJ en Español. *Conferencias anuales República Dominicana 2012, México 2013, Panamá 2014, República Dominicana 2015 y Perú 2016* (available at *http://www.drjenespanol.com/)*

International Organization for Standardization. *ISO 22301: Seguridad de la Sociedad - Sistemas de Gestión de la Continuidad del Negocio.* Geneva, Switzerland, 2012. (available at *http://www.iso.org)*

International Organization for Standardization. *ISO/TS 22317: Seguridad de la Sociedad - Sistemas de Gestión de la Continuidad del Negocio. – Guía para el Análisis de Impacto al Negocio (BIA).* Geneva, Switzerland, 2015. (available at *http://www.iso.org)*

International Organization for Standardization. *ISO 31000: Gestión de Riesgos.* Geneva, Switzerland, 2012. (available at *http://www.iso.org*)

The Business Continuity Institute. *GBP 2013: Guías de Buenas Prácticas.*, London, England, 2013. (available at *http://www.thebci.org/)*

Latin American and Caribbean Economic System (SELA). *La continuidad de negocios y operaciones frente a situaciones de desastre en América Latina y el Caribe. Balance y recomendaciones*, Caracas, 2013. (available at http://www.sela.org/*)*

Virtual Corporation. *Modelo de Madurez en Continuidad del Negocio versión 2*, 2012. (available at *http://www.virtual-corp.net/)*