2010

Disaster recovery best practices for Dominican Republic's contact center

Dhariana Gutiérrez Almonte

Disaster Recovery Best Practices for Dominican Republic's Contact Center

By

Dhariana Gutierrez Almonte

Thesis submitted in partial fulfillment of the requirements
for the degree of
Master of Science in
Networking and Systems Administration

Rochester Institute of Technology

B. Thomas Golisano College
of
Computing and Information Sciences

April, 2010

Rochester Institute of Technology

B. Thomas Golisano College
of
Computing and Information Sciences

Master of Science in
Computer Security and Information Assurance

Thesis Approval Form

Student Name: Dhariana Gutierrez Almonte

Thesis Title: Disaster Recovery Best Practices for Dominican Republic's Contact Center

Thesis Committee

Name	Signature	Date
PhD. Yin Pan Chair		
PhD. Charles Border Committee Member		
Ms. Arlene Estevez Committee Member		

Thesis Reproduction Permission Form

Rochester Institute of Technology

B. Thomas Golisano College
of
Computing and Information Sciences

Master of Science in
Computer Security and Information Assurance

Disaster Recovery Best Practices for Dominican Republic's Contact Center

I, Dhariana Gutierrez Almonte, hereby grant permission to the Wallace Library of the Rochester Institute of Technology to reproduce my thesis in whole or in part. Any reproduction must not be for commercial use or profit.

Date: 30 /April/2010 Signature of Author: Dhariana Gutierrez

Rochester Institute of Technology
Pontificia Universidad Católica Madre y Maestra

B. Thomas Golisano College
of
Computing and Information Sciences

DISASTER RECOVERY BEST PRACTICES FOR DOMINICAN REPUBLIC'S CONTACT CENTER

PROJECT

DHARIANA GUTIERREZ ALMONTE
APRIL, 2010

Abstract

Contact Centers are an important growing industry in the Dominican Republic which provides employment, foreign exchange and exposition of the country on the international market. The international competition requires standardization of the systems and processes to be in compliance with international requirements. One of the important elements to be validated is Disaster Recovery planning because of the exposures of the Dominican Republic to events that may affect the continuity of service that Contact Centers must provide to customers and clients.

In this paper an analysis is elaborated about the risks that the Dominican Republic encounters for disastrous events and a set of best practices are summarized to help a Contact Center to be prepared for incidents and design their own Disaster Recovery Plan.

Table of Contents

Table of Figures

Acronyms

ICT	Information and Communication Technologies
DR	Disaster Recovery
ISP	Internet Service Provider
SLA	Service Level Agreement
BIA	Business Impact Analysis
PBX	Private Branch Exchange
IVR	Interactive Voice Response
ACD	Automatic Call Distributor
PD	Predictive Dialer
BPO	Business process outsourcing
QA	Quality Assurance
APPS	Applications
RS	Richter scale
MMS	Moment Magnitude scale

Considerations about the Project

In the following report, sections 1 and 4 were jointly developed by Patricia Ortiz, Yudit Maria and Dhariana Gutierrez.

1 Introduction

The Dominican Republic has experienced big changes in the technological sector in the last years. Santo Domingo, capital city of the Dominican Republic, is home of *NAP del Caribe*, a specialized data center [1] that started operating in the last quarter of 2008 [2]. Besides establishing the country in an extremely favorable position in worldwide connectivity, NAP del Caribe is also expected to impact not only the way telecommunications are managed, but also the costs of telecommunication services that are estimated to be considerably reduced. There have been several other facts that evidence a positive evolution and fast growing [3] of technology and telecommunications in the Dominican Republic. This has been one of the incentives, although not the main one, for expansion of businesses of different areas; one of them is the Contact Center industry.

Currently about 65 Contact Centers are operating in the Dominican Republic, mainly in Santo Domingo and Santiago [4]. This industry continues to grow because the country offers attractive conditions for the development of the sector, such as geographical location, human resources, and as mentioned before technological infrastructure among others [5]. In 2006, it was estimated that the call center industry was going to provide more than 30,000 employments in the near future [5]. In 2008, Eddy Martínez, director of the CEI-RD (Centro de Exportación e Inversion de la República Dominicana - Center for Export and Investment of the Dominican Republic), affirmed that contact centers were already generating employment for 25,000 people [6]. This same institution estimates that contact centers will continue growing within the next years [7]. In the period of 2003-2009, the sector revealed an expansion of 490%, going from 11 Contact Centers in 2003 to 65 contact centers in the first semester of 2009 [4]. The vast majority of Contact Centers in the Dominican Republic works for corporations outside the country, and this is precisely their main target, outsourcing.

However the Dominican Republic is not the only country exploiting this relative new area of services. Countries like India, Philippines, Panama, Costa Rica, Jamaica, Mexico and El Salvador, just to name a few are also serious opponents in the race for outsourcing. Factors such as operational costs, quality of labor force, education, training, political issues [8] and the facilities offered from each country will determine the election of one over the other. There are also other considerations, which are equally important when choosing an outsource business associate, an example of these considerations is security because depending on the type of operations that an organization performs, there is a need for different security levels. Also the reliability that can be offered to a partner is a critical and determinant factor to make a decision. That is why it is so important to meet certain requirements to be considered as an alternative.

Despite the fast growth that is being experienced by this sector in Dominican Republic, and probably as a direct consequence of it, there are no general applicable policies, best practices, standards or guidelines to regulate the operations and security of Contact Centers. Neither there is wide documentation on Risk Assessment, Disaster Recovery, Infrastructure Standard Requirements, Contingency Plan, Data Protection or Privacy Practices, just to mention a few areas that are critical to ensure services continuity and security.

From the facts expressed in the previous paragraph it can be inferred that there is a gap that needs to be covered right away if the country wants to continue the trajectory of development that has reached so far, and most importantly to be a competitive option given the current and diverse amount of choices available in the worldwide market. It is imperative for Dominican Republic as a country to face this issue and turn it into a big improvement opportunity that later will contribute to its economy. The following project is oriented to set adequate best practices for Disaster Recovery planning for Contact Centers.

2 Scope

Disaster Recovery planning is a set of activities that aims to detail what needs to be done to recover from a major event that affects normal business operations. In a company, both human and technological infrastructure protection must be contemplated in Disaster Recovery Plans but this project will only cover the Disaster Recovery plan prepared for Information and Communication Technology (ICT). A Risk Assessment won't be elaborated in this project and a Disaster Recovery Plan won't be created for a real Contact Center, it will only specify guidelines for the proper elaboration of a Disaster Recovery plan in the Dominican Republic.

3 Literature Review

Contact Centers must provide continuous availability as an industry of services. Part of the operational risks that they must face as an enterprise is the possibility of destructive events, both natural and man-made. Fearing these disasters we must take in consideration the current environment and geographical circumstances.

Disasters happen frequently and when they occur it becomes evident if organizations are prepared or not to avoid being affected by these events. Most of them get affected severely because there are no Disaster Recovery plans [9] or if these do exist they fail to test them on regular basis [10]. This is equivalent to not having any because it fails to achieve its goal: uninterrupted service and the least admitted downtime. This planning is important for the Contact Center industry because service is their selling item and no availability represents a violation to their Service Level Agreements (SLAs). In order to stay ahead in the race these organizations need to offer, and be able to keep up with what they offer: the closest to zero downtime. Hurricane Katrina and the earthquake in Haiti are examples that demonstrate that disasters are superior issues and that organizations should look further and contemplate more than just single events [9]. Since organizations today have their core operations based on technology, what will happen if these IT resources aren't available? The management must have a clear understanding regarding this possibility and what needs to be done previous and afterwards of possible incidents.

The disasters to be contemplated aren't only natural disasters that happen in Dominican Republic such as hurricanes, floods, strong winds, earthquakes; some other threats must be considered that originate a service disruption. For example: fires, electrical power issues, hardware and software issues and malwares [9]. An important note about hurricanes is that each year the hurricane season for the country runs from June 1st to November 30th, but during all year it is typical to be under the effect of various tropical storms that affect and produce a lot of rain and strong winds [11].

The need of practices for Disaster Recovery for Contact Centers rests in the fact that this is a growing sector in the country and as it is intended to help the economy, must have enough preparation in these matters to be in compliance with internationally accepted standards and guidelines. This compliance will help the country to keep gaining and maintaining a position in the global market in this area. First these practices have a purpose, it's not to hassle the staff at all, it's to assure the SLAs that are part of the negotiation in service industries and the quality of these services offered. Second, those potential customers always evaluate the robustness of the organizations that they will negotiate with. As the competition is expanding in the Contact Center sector, it is imperative to be set correctly in this regard.

Contact Centers are mostly real time service providers so disasters and events affect strongly their performance, SLAs and quality of procedures and service to customers.

3.1 Domain Modeling

One of the tools that will be used is a Domain Model. Domain Modeling techniques will be used to create a prototype of Contact Center's operations in Dominican Republic. The objective is to target every procedure in a Contact Center, find its inputs and outputs, operation requirements and represent them in a way that can be generally applicable to any Contact Center working in the same field. This Domain Model should serve as a base of common knowledge about the operations of Contact Centers in Dominican Republic; it should be useful for problem solving, development of new ideas for this area as well as a basis to detect flaws and weaknesses that can be improved along that industry. It will

serve as the base to create a disaster recovery plan and to identify the technological infrastructure requirements.

A domain model is a method to represent all the procedures and components in a system and the interrelation among them. The concept of domain modeling comes from the software designing area and was born from the software reuse concept [12] [13]. The idea behind domain modeling is to compose a general understanding of the domain that can later be generally applicable for similar domains. A domain is a problem space [14] and domain modeling would be the task of representing that problem space through diagrams (or any other adequate methods), showing the interrelation of the activities and objects conforming that space to get the most complete understanding of the situation. With a domain model it is possible to interconnect objects and clarify their relationship within a domain. In software engineering the objective of modeling a domain is to find things common to several systems so they can be re-used in different applications and systems that share the same characteristics.

As mentioned before domain modeling is a technique originally designed for programming but it is actually implemented on several other areas such as business because it is equally useful, permitting to design a picture that describes a system, environment or situation not necessarily related to software. A domain model *"is a model of the domain within which an enterprise conducts its business"*. If an enterprise conducts business on one domain then the domain model should be the same for another enterprise using the same domain [15].

3.2 Historical Trend of Disasters

The geographical position of the Dominican Republic makes it prone to natural disasters such as the hurricanes, earthquakes and the catastrophic events that follow these actions of nature. The island of Santo Domingo, which was before named La Hispaniola, is located in the Caribbean Sea as part of the Greater Antilles archipelago. The Dominican Republic shares this island with Haiti and occupies two thirds on the east side. The cause for earthquakes activities is because the island is located over the boundary of two tectonic plates and the interactions among themselves cause faults, which are breaks in

the Earth's crust after the movement of the plates, and as a result earthquakes zones are formed [16].

Historically the island has suffered catastrophic seismic movements that have destroyed complete cities since we have record after the colonization. The history of earthquakes in the Dominican Republic shows a pattern of certain frequency, every year earth movements occurs, but usually these earthquakes are less than 3.5 in the Richter scale. The movements that can be felt are those over 4.0, but damage begin to occur above 5.0 in poorly designed edifications and over 6.0 in any other. The following list is of earthquakes over magnitude 6.0 that have occurred in the Dominican Republic in the twentieth century:

- 1918 (7.5 magnitude of the RS) on the Mona Passage
- 1946 (8.0 magnitude of the RS) in Samana on August 4th and then an aftershock on August 8th (7.6 magnitude of the RS)
- 1984 (6.7 magnitude of the RS)
- 2003 (6.5 magnitude of the RS)

The oldest earthquakes record was in 1562, from the documents left by discoverers, it happened in the north central part of the island in the province of La Vega and buried the city. There is also evidence of earthquakes that happened before the twentieth century in 1615, 1673, 1751, 1761, 1842 and 1948 according to a recompilation done by Héctor Iñiguez from chronicles and official reports especially from the clergy available since the time of the Spanish crown and the colonization period. The Richter scale (RS) was developed in 1935 and it was the traditional used scale for earthquakes but it was not very precise for big earthquakes (over 7.0) and in 1979 the Moment Magnitude scale (MMS) was introduced to address the shortcoming of the RS. For medium magnitude quakes the measure would be the same in both scales but it doesn't saturate for bigger than 7.0 earthquakes, in contrary it's not very precise for smaller quakes so the RS is used instead for 3.5 magnitude and lower quakes.

More frequent than earthquakes, the island suffers the effects of hurricanes. The island is in the center of the Greater Antilles and constantly suffers from hurricanes formed in the Atlantic Ocean that pass through the Caribbean Sea. The most affected zones of the island are the coasts but as a small island interior provinces are vulnerable as well.

For hurricanes the scale used is the Saffir-Simpson, which categorizes the intensity of a hurricane from 1 to 5 depending on the speed of the wind. Any storm that produces torrential raining and strong winds, whether a hurricane or not, may cause damage to a city because of the side effects such as floods and river overgrowth, mudslides, trees and electricity poles downed and as a direct consequence of all this, the destruction or damage of roads, bridges, buildings and other infrastructures and the most painful effect, human deaths.

In the twentieth century the following are some of the most devastating hurricanes that have landed as a category 3 or more in the island:

- In 1930, San Zenon, which was a category 4 hurricane destroyed the city of Santo Domingo
- In 1966, Inez, affected mostly the cities of Pedernales as it made landfall in the south tip of the island as a category 4
- In 1979 another category 4 hurricane struck the city of Santo Domingo, it was called David
- In 1998, George, a category 3 hurricane caused a lot of damage to the east coast.

Many others have passed near the coast causing serious damage as a side effect of the rains and the strong winds such as: Katie in 1955, Edith in 1963, Beulah in 1967, Emily in 1987, Hortense in 1996, Jeanne in 2004, Alpha in 2005, Noel, Olga and Dean in 2007 and Gustav in 2008. The year 2009 was tranquil. For details on these storms and others that occurred from 1909 to 2009 refer to Appendix 13.2 "*Report of Hurricanes and Catastrophic Tropical Storms that have passed near or over the Dominican Republic in the last 100 years".*

4 Domain Model of the Contact Center industry in the Dominican Republic

4.1 Contact Center General Diagram for Project Outsourcing

Contact Centers are interested in acquiring clients to offer their outsourcing services. Most of the target market of Dominican Contact Centers is focused in the United States. But Contact Centers may be interested in providing services to other markets such as United Kingdom, Spain and Canada. Like an airline, have their seats “sold up to capacity" is one of the goals of a Contact Center.

The following diagram presents a general overview of Contact Center' processes from the moment they capture a new or potential client until the moment its operations are fully implemented.

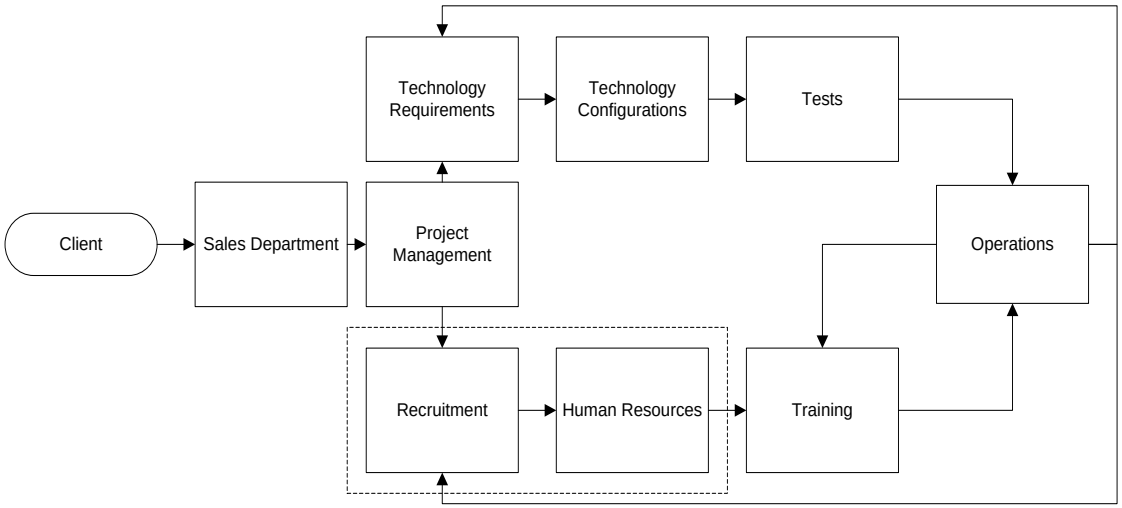


Figure 1: Contact Center General Diagram for Project Outsourcing

As it can be seen, potential clients get in touch with Contact Centers through the Sales Department (or equivalent) to negotiate their required services, needs and to get quotations. When an agreement has been established between the client and the Contact Center, a project management team is in charge of developing the human, operational and technological requirements for the new project. Once this plan is complete, Human

Resources department is in charge of recruiting the appropriated personnel taking into consideration the desired profile. During this process candidates are evaluated and depurated. Selected candidates receive a job offer from Human Resources and after they are hired the induction and training are provided.

Training could cover from basic Contact Center processes to client-specific courses. After training is complete the employees start working in the operational environment. Training is a continuous process and employees have to be prepared constantly, either on changes within the current processes, new requirements or quality improvements. If more staff is needed, the Operations department will ask Recruitment/Human Resources to provide more workers and the same process will be repeated.

While the recruitment process is being performed the technology team is in charge of developing the technical platform that is required for the project. They are in charge of acquiring any new technology platforms and/or services and make any changes and configurations to current systems and services if needed. The following step is to test that all the technology is ready for the operation of the new project. After everything is set, operations are ready to begin. Technology changes and new implementations are also constant within the Contact Center environment because Operations requires them, thus the same process of gathering information, configuring and testing has to be followed once again.

It is important to notice that the Operations department becomes the representative of the client within the Contact Center and any new requirement should be arranged by them.

4.2 Human Resources key processes within the Contact Center:

The Recruitment/Human Resources process is very important on a Contact Center, because the operations rely not only in the technological infrastructure but also on the human capacity. Commonly Contact Centers tend to have high rotation rates making the process a constant task.

The relevant processes that are going to be addressed are recruitment, selection and hiring. The following diagram shows these key processes with an overview of their functions:

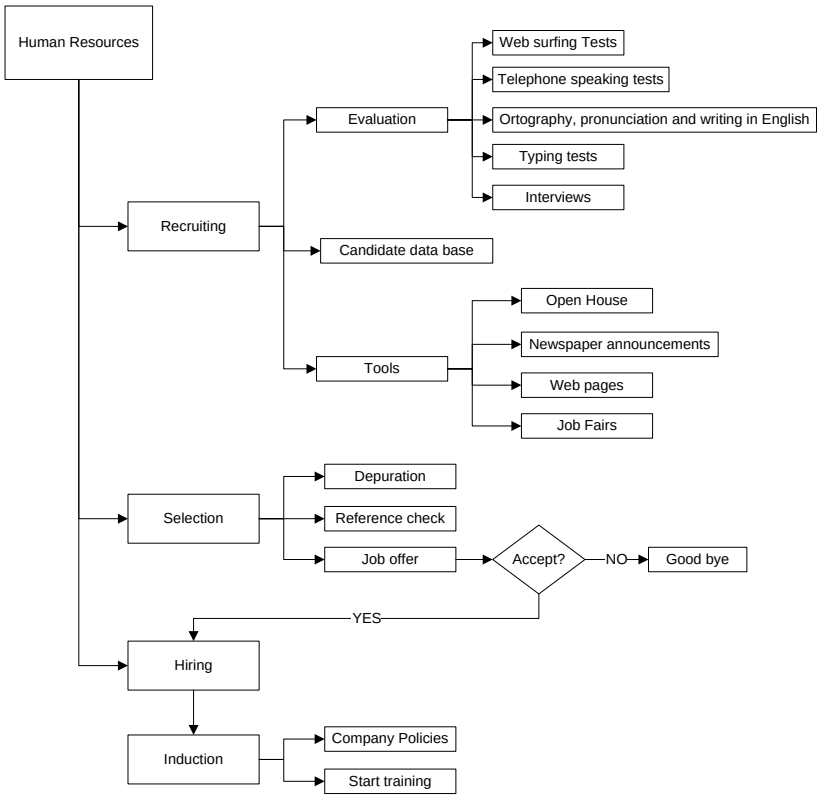


Figure 2: Human Resources key processes within the Contact Center

4.2.1 Recruitment process:

For Contact Centers outsourcing, recruitment has to be accomplished taking into consideration a defined profile established by the client.

Recruitment	Evaluation	Different evaluations should be developed according to the specific requirements for each project. Evaluations could range from simple interviews up to technical knowledge or abilities.
	Candidates Database	A database of potential candidates has to be continuously developed to create a selection pool that will permit a fastest response to recruitment requirements.
	Tools	Since the rotation rates tend to be high on Contact Centers, a combination of different tools comes in handy for employees' uptake. Tools as newspaper's ads and job fairs are commonly used.

4.2.2 Selection process:

Selection is the next step in the process, after a set of candidates has been recruited.

Selection	Depuration	The evaluations of the aspirants are checked and the most outstanding candidates are chosen.
	Reference Check	Background checks are completed for elected candidates to make sure they comply with company's hiring policies. Also claimed competency may be verified.
	Job Offer	Elected candidates receive a job offer from the Human Resources department.

4.2.3 Hiring process:

Candidates that have accepted job offers will go through the hiring process.

Hiring	Induction	New employees receive information related to the company's policies and procedures.

4.3 Training key components within the Contact Center:

After the employees have been hired, they start their training phase. The training's key tasks involve Contact Center's specific courses and client procedures and tasks. It is important to consider several different aspects such as trainers, training methodologies, training tools, locations and the training cycle itself.

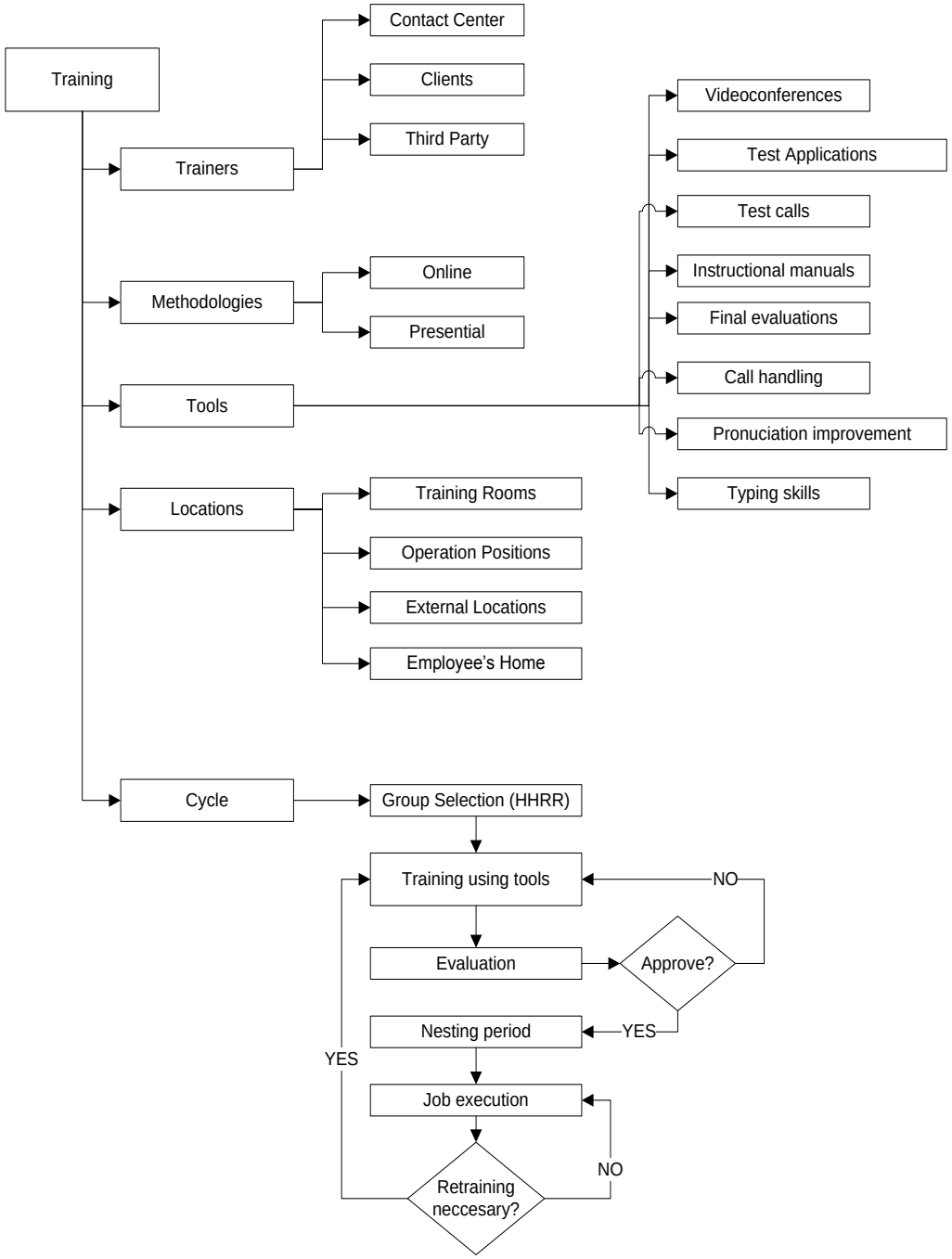


Figure 3: Training key components within the Contact Center

4.3.1 Trainers:

Trainers	Contact Center Trainers	Many Contact Centers have dedicated or partially dedicated trainers. Some trainers are devoted to client's specific courses and others provide general Contact Center trainings.
	Client Trainers	Some courses are imparted by trainers from the client's side. In some occasions client's trainers prepare Contact Center trainers that will continue the process.
	Third Party Trainers	Some special courses require third party institutions/trainers who will deliver the course.

4.3.2 Training Methodologies:

Trainings can be delivered using different types of methodologies.

Methodologies	Online	Using any web-based or remote based application and sometimes through phone conferences.
	In Person	Trainer is on site. A dedicated space for the training is needed for most of the occasions.

4.3.3 Training Tools:

To have effective trainings, trainers utilize a set of different tools to make sure the personnel is prepared to handle the tasks of Operation's environment.

Tools	The set of tools utilized by trainers include (but not limited to) video conferences, test applications that simulates the real production environment, test calls, instruction manuals, final evaluations to determine the level of preparation of the employee, etc.

4.3.4 Training Locations:

Whether training is online or in person it can be imparted in different types of locations, and the selected location should be suited for an effective training.

Locations	Training Rooms	Most medium to big size Contact Centers usually dedicate one or more areas for training purposes. Most of these areas are equipped with the same capabilities as operational environment plus additional training aids.
	Operation positions	Even if it is not desirable, operation positions are used in some occasions for training purposes. Most of this trainings are minor or to enforce previous ones.
	External locations	Some training sessions are carried outside of the Contact Center. These external locations should have the required capabilities for the class that is going to be imparted.
	Employee's home	Online trainings may be accessed by employees from their homes through their personal computers if this is in compliance with the company and clients security policies.

4.3.5 The training cycle:

The training cycle starts after an employee has been hired and has received his or her induction as a Contact Center's employee. Training is continuous and is directly related to Operation's activities. Client's processes are prone to suffer constant changes and new tasks might be added. Also employees' quality is periodically evaluated and retraining may be pertinent.

4.4 Operations key components within the Contact Center:

Operations are the heart of the Contact Center since they are in charge of completing the job. If operations are not working properly, the Contact Center is not working properly.

Operations as a department, has several key components and players that needs to be taken into consideration are:

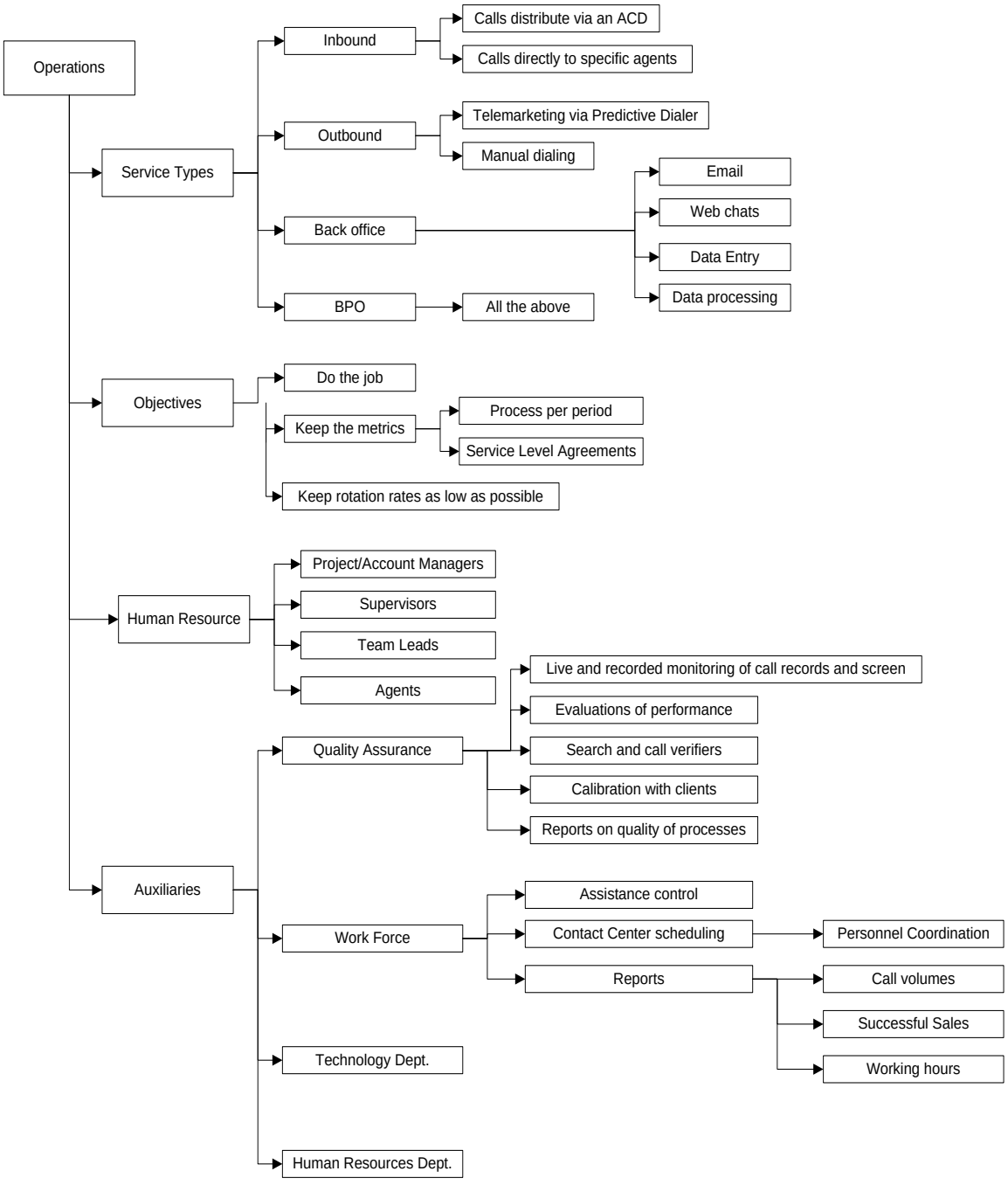


Figure 4: Operations key components within the Contact Center

4.4.1 Services Types:

A Contact Center can offer one or more different types of services.

Service Types	Inbound	Inbound calls can be delivered to employees either by an Automatic Call Distribution equipment or manually directed to a specific employee (transferred call or dialed by extension/direct phone number)	A well known example of Inbound services is the customer care service lines. Customers call to a toll free number and calls are routed to customers sales/service representative that will provide assistance to the customer.
	Outbound	Outbound calls are either manually performed by the employee or automatically dialed by a Predictive Dialing system.	Telemarketing is a well know example of outbound services.
	Back Office	Back Office Tasks are usually carried on without live contact (or almost without live contact) with customers.	Examples includes data digitalization, e-mail processing, etc.
	Business Process Outsourcing	Business Process Outsourcing involves a mix of Inbound, Outbound and Back Office services towards the completion of a predefined function.	Examples include outsourced payroll processes or financial related tasks.

4.4.2 Operations Objectives:

The Operations objectives are simple:

- Do the job the Contact Center was hired for.
- Keep the metrics. Completing the job is not enough; the job has to be done in compliance with several production and quality metrics.
- Keep rotation rates as low as possible. Recruitment, hiring and training processes cost money to Contact Centers. Operations, with the support of Human Resources, should elaborate plans to maintain a low rotation rate.

4.4.3 Operations human resources:

The Operation's department is formed by different types of people fulfilling different types of functions.

Operations Human Resources	Project/Account Managers	They are the direct contact with the client on the Contact Center. They must ensure client's needs and requests are met.
	Supervisors	They are in charge of supervising the different groups of Call Center Agents.
	Team Leads	Help Supervisors and in some occasions handle "supervisor calls."
	Agents	The ones doing the job.

4.4.4 Other sub departments of Operations or auxiliaries are:

Auxiliaries	Quality Assurance	QA is in charge of evaluating and monitoring the work of the Contact Center agents. Their main goal is to ensure that the metrics are achieved while the quality is preserved.
	Work Force Management	The Work Force Management department is in charge of generating performance reports for the different projects. They also manage schedules of the agents and develop production volumes forecasts for the different campaigns.
	Technology and Human Resources Departments	These departments are not precisely sub - departments of Operations, but should provide constant support to the production.

4.5 Technology key components within the Contact Center:

Technology is for a Contact Center as sewing machines are to a textile factory. Without some type of technology Contact Centers will not operate.

Technology activities comprise a variety of tasks which includes Project Management, Telephony and Network Administration, Application Development, Help Desk, Technological Security and Contact Center Activities. Figure 5 presents a better view of these tasks.

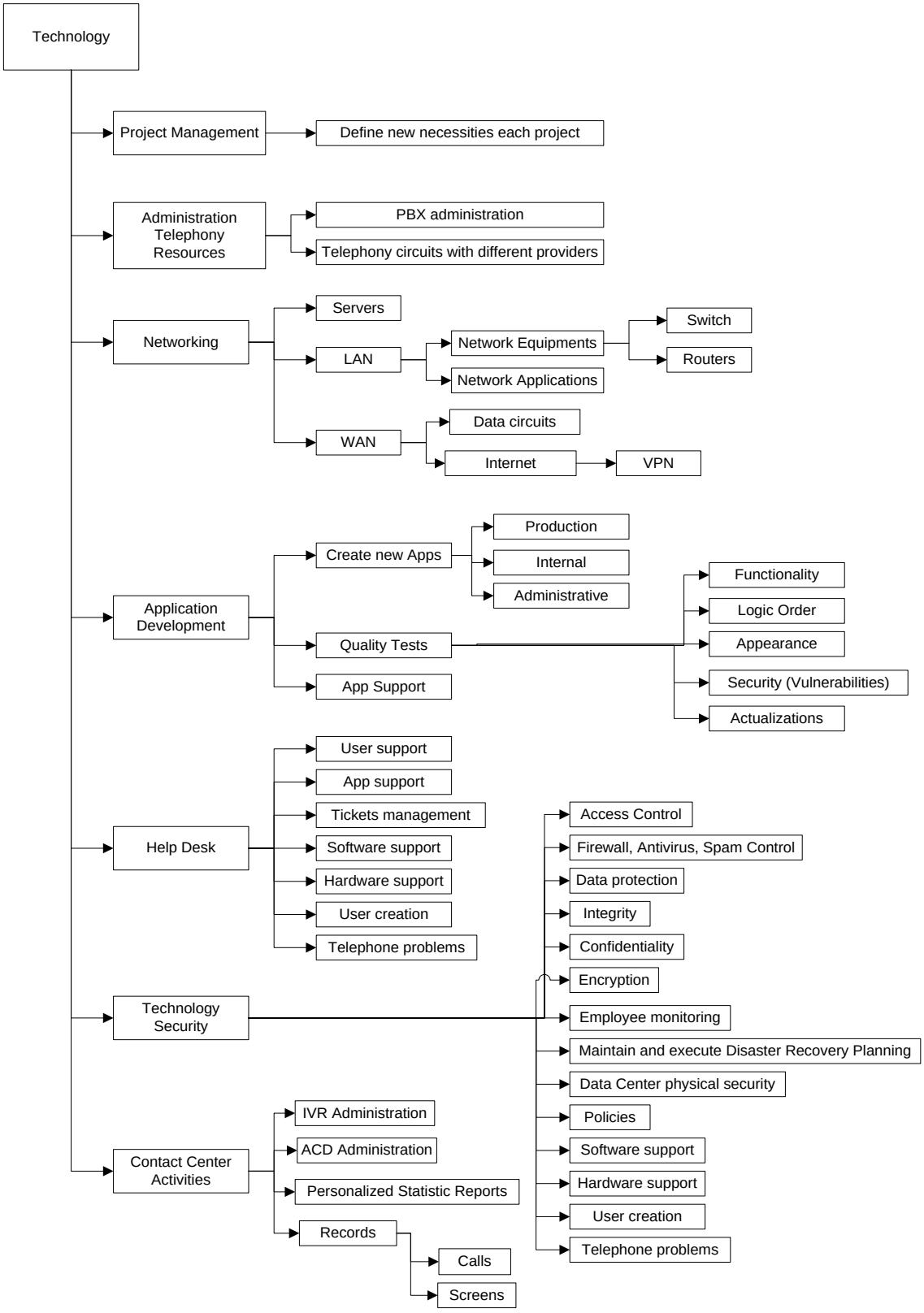


Figure 5: Technology Key Components within the Contact Center

Project Management	Each Contact Center client has specific technological demands that have to be met. These requirements could be similar or completely different from current clients which imply a change in the existent set of technologies. For each new project, the IT department should analyze the technological necessities and develop a plan to make sure all the specifications are met.

Administration of Telephony Resources	For Contact Centers that handle calls (either Inbound or Outbound), there should be a technological entity in charge of administering any kind of telephony circuit that is being used. Also many Contact Centers have their own PBX that also needs to be managed and maintained.

Networking	Like in other kind of modern organizations, Contact Centers have computer networks that must have resources dedicated to its administration. Downtimes either on the Network or the Telephony System could mean lost for the Contact Center profits.

Application Development	Projects might require specific applications, customizations or some integration between different existent applications. For these types of requirements application developers will be needed. Also internal departments of the Contact Center may have similar needs of applications to achieve the goals of the business.

Help Desk	Due to the fact that Contact Center's personnel works with technology equipments, they may require help desk support. Malfunctioning systems can stop the production or part of it if they are not quickly attended. Help Desk resources are the first to attend any technological problem that is reported from any area.

Technology Security	Security is important in any business. Contact Centers are not the exception, especially because they handle information of their clients. Contact Centers should ensure their clients feel confident letting them handle their information. Security comprises a lot of different topics that range from physical security to logical security, and everything in between.

Contact Center Activities	There are special equipment and technological activities within a Contact Center that are very specific to this kind of business. Examples of these are IVRs, ACDs, Call Recording Systems, Predictive Dialers, etc. All these equipments require personnel to administer and maintain it.

5 Logistics for Disaster Recovery Planning

It's known that the first part in Disaster Recovery planning is obtaining management's approval and support and define the boundaries of the plan to be developed, which generally results in the most difficult task. Then what follows is to develop the team in charge of designing the plan, this should involve people from all departments so each one can defend the needs of their unit. Once the team is formed, they must identify and prioritize the critical systems and functions of the business. The Risk and Business Impact Analysis is what follows to determine which threats the organization is more vulnerable to and how it affects the business when a critical point is affected.

Based on this information, the team must start developing the Disaster Recovery Strategy focusing on priority systems and determine the conditions under which the plan is to be activated. The strategy must be approved by management and especially by Finance. In this step, roles and responsibilities must be defined and selected for the execution of the plan. Once approved, the Policies and Procedures for Disaster Recovery can be elaborated. At this point begins a process of draft-corrections-draft-corrections-…-final and once defined the plan is approved (first phase). The team is responsible for the testing, training, distribution and maintenance of the DRP. After the testing, if any corrections are needed these should be made, and not only here, the maintenance of the plan is all about modifying and correcting upon the new needs that arise.

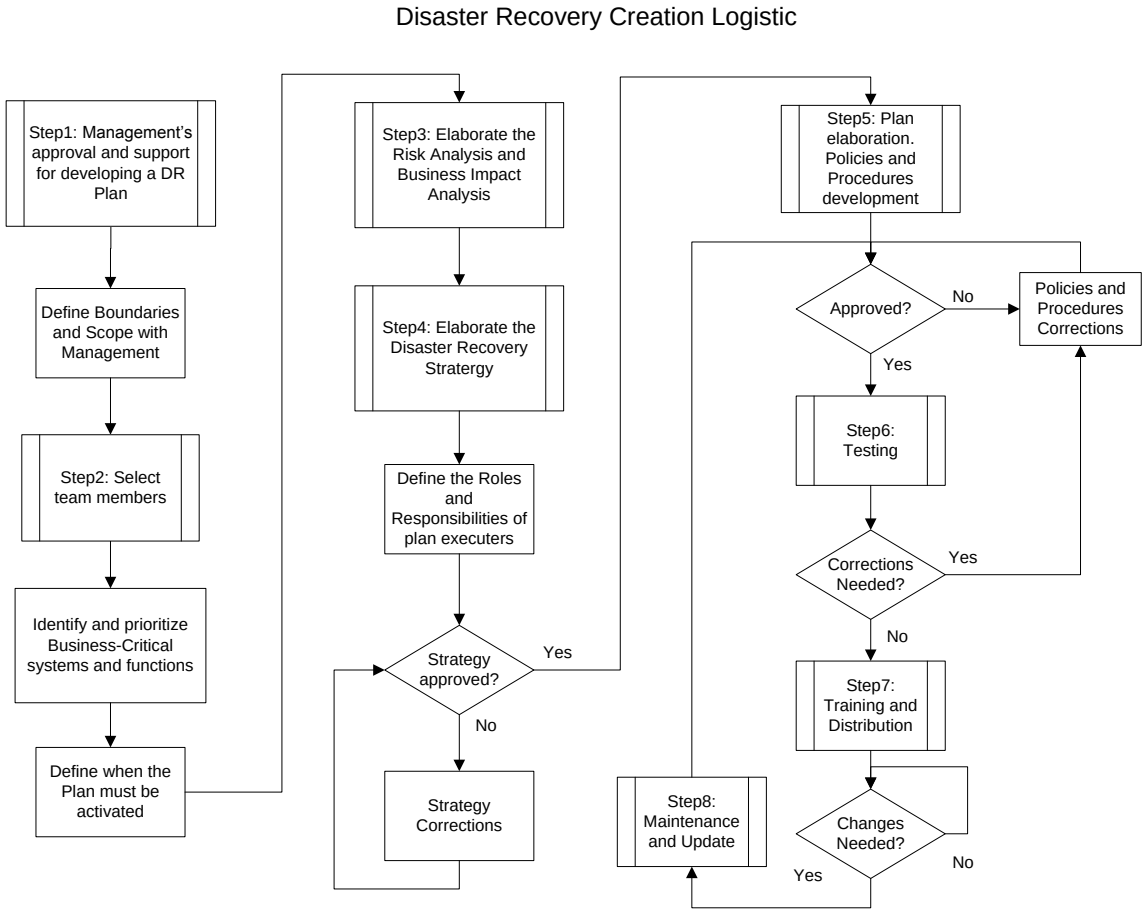


Figure 6: DR Logistic Flow Chart

6 Business Impact Analysis based on the Domain Model

In this project the elaborated general Business Impact Analysis sketch is limited to the Operations process from the overall Contact Center functional groups described in the Domain Model. A Risk Assessment won't be elaborated, instead threats based in general technologies are consider and the specific threats present in the Dominican Republic are contemplated in the following section.

The most critical functional department is Operations and in the event of a disaster the efforts will be focused in providing the Basic Service Coverage, which is the business's critical process. The basic operations can be defined by the service type offered by the center: Basic Call Handling for Inbound, Outbound and BPO and Basic Internet Access for Back Office and BPO. In both cases there are a set of business, technical and

logistical requirements that must be defined in order to provide these basic service. From the business point of view it's necessary to establish what is to be called a disaster and when to activate the DR plan. From the technical point of view it's required to define the infrastructure needed to provide the basic service, and from logistics' point of view the steps of the Disaster Recovery plan must be designed in a proper and timely fashion [16].

There are a set of threats that in general technology based companies are exposed such as network problems, hardware and software failures, malware, viruses, trojans, worms, exploits to vulnerabilities, power failures, voltage issues, overheating, wrong configuration changes, incompatible updates, SPAM, fires, floods, hurricane, earthquakes, cyber attacks and others. Some are originated by humans like sabotage, negligence, mistakes, robbery and terrorism. All of these threats can affect the infrastructure needed to provide the basic service to customers.

From the output of a Business Impact Analysis, two very necessary parameters are defined, the Recovery Time Objective (RTO) and Recovery Point Objective (RPO). These two parameters are very specific for each company because they are related to the timeframe established depending on the combination of all clients of a Contact Center thus they cannot be defined with a general value.

The RTO is the established time frame since the event that caused the disaster until the business is back in operation. This is the time that the DR team has to recover to the normal state. The RPO is the amount of data in terms of time that is allowed to be lost. For example if the business can only lose three hours worth of data but five hours after the last backup a disaster occurs, then five hours of data is lost (two more than the alloweb by the RPO). The RPO is very important when establishing any backup strategy, depending on the amount of time of data you can afford to lose the more or less frequent backups must be done. There can be zero data loss, where the strategy is oriented to recover data till the point of failure, start of the current business day (SoD), end of the previous business day (EoD) and intraday that would be a point between the last backup and the point of failure; after defining this, the backup frequency must meet the company's needs [17].

Based on the operation model of Contact Centers there are some elements that are specific for this type of business but others are basics for any enterprise. The following are the important assets that constitute the vertebral spine of a Contact Center and we must prevent the unavailability of these core elements. Refer to *Appendix 13.1 Business Impact Analyses Guide for Contact Centers.*

6.1 Core elements to protect

One of the most important elements is power generation and it applies for almost all businesses. Without electrical power all systems may operate temporally with UPSs and then with an alternative source of energy, but the total absence of it for long time can cause that the operations stop working. The impact of energy absence ends in an economic issue due to the cost of any alternative solution and the losses of non operation time. Most Contact Centers receive payment in a per hour basis which means that less productive hours equals to less revenues. The potential threats can be regular power blackouts, power grid/general failures from the Energy Provider, destruction of electricity poles caused by hurricanes or backup energy failure. Electricity is the source of energy for hardware systems; a company will be completely out of service without a power source.

Internet Connection and Voice and Data lines from ISPs are very important for most companies but for Contact Centers they represent a crucial element to offer their services. The consequences of unavailability go from communication interruption with customers, downgrade of the SLAs, non-working agents and in worse case scenarios the Contact Center can be unreachable. The economic element is also present here, because of the need for redundant data and voice lines.

The impact of less availability can generate economic losses and reliability degradation with clients. The potential threats for the telecommunications services can be providers' internal problems, physical damage to the providers' line, and malfunction of Contact Center’s internal equipments (Routers and PBX). Without Internet most data flow wouldn't be successful.

The PBX is another critical element; without the PBX, calls aren't managed and aren't distributed to agents or the other areas of the Company. Most Call Centers offer inbound services, which receive calls, or outbound services, where they make calls, when calls aren't managed, no service is being offered to the customers of clients and sales are not being made. The impact here can be economical and in terms of the SLAs. The potential threats can be new configuration errors, incompatible updates, voltage problems, module failures and hardware failures.

The Predictive Dialer (PD) is the equipment that makes the calls automatically from a list of numbers provided. It filters those lists and connect the agents,making this process efficient, error free and controlled. Without the PD the agents would have to dial manually the numbers of the customers they are calling, errors can occur during the dialing process which would cause an extra call charge to an undesired number. Agents' productivity would be reduced because of the time they'd lose while dialing and waiting for someone to answer. Also answering machines prompts would represent time and minute losses, the result of all would be fewer sales. This equipment is commonly used in Contact Centers that offer outbound services. Some potential threats can be hardware failure, errors while modifying configuration, in-house systems errors which communicate with the PD, errors in the lists provided to the PD or not providing them at all.

Interactive Voice Response (IVRs) interact with calling customers to determine through a voice recorded menu the service needed by the clients. Without this automatic menu a person would have to be included in the function of receptionist asking the customer what he or she needs and then manually transferring them to the correct queue of agents. This would be inefficient and productivity would be reduced significantly. The impact of unavailability is mostly in SLAs downgrade because of longer calls and an increased waiting time for customers. Some potential threats can be new configuration errors, incompatible updates, voltage problems and hardware/module failures.

Automatic Call Distributors (ACD) control the flow of a call once it enters to the PBX. It organize the queue depending on the number that the customer dialed, the options he

selected from the menu (IVR) and the group of agents to which the call will be forwarded to; usually the agents are grouped depending on the set of skills that they were trained. Without this organization a customer would encounter a lot of delays in the system to be attended and a call would last longer if it needs to be transferred multiple times. The impact of unavailability would be customer dissatisfaction, SLA downgrade, bad handled system which turns in delay and longer service calls. Potential threats are bad configuration modifications, problematic firmware updates, hardware/module failure.

The Computer Telephony Integration (CTI) system integrates the computer used by agents with the telephone system, which by default makes a consolidation of the communication channels. While the customer passes by the IVR and ACD, the CTI collects information about the customer. Without this, the agent would have to ask all this information during the conversation sustained with the client instead of automatically, this process of asking questions to the caller would reduce the efficient time, make calls longer and generate less agent availability. The system also provides statistics for admin staff, control of agent status, call controls for QA and reporting. With this system unavailable there would be less agent availability because of the poor efficiency on the call handling, SLA downgrade, less reporting and QA control and finally it would be more difficult to generate statistical information. Because it's a specialized equipment, the potential threats that may affect IVRs and ACDs can also be experimented by the CTI.

Quality Assurance (QA) is a process that helps the Contact Center to stay in compliance with the clients requests in terms of quality. In QA calls are monitored and feedback is provided to the agents to improve their performance. Without this department quality can be affected and SLAs downgraded. Some potential threats can be a bad job monitoring the calls and screens, problems with the voice recording systems and problems with the hardware where the records are kept.

Voice Recording systems are the base for QA. The conditions of recording sometimes are requested by the clients, they determine the percentage of the calls that they want to be recorded. Some potential threats can be voltage problems, hardware failures, no media

drives available (tapes, CD-ROMs, hard drives, etc) where to record the conversations, loss of data before it's stored in external media and overwriting non backed up data.

The following elements are also important and most are general for most type of businesses: Storage/File Servers, Network Apps Servers, Network Equipments (Routers, Switches), VPN, Computers and Telephones, Ticket System, E-mail Apps, Custom Apps, Air Conditioners and Databases. Refer to *Appendix 13.1 Business Impact Analyses Guide for Contact Centers*.

7 Circumstances for Disasters and Incidents in Dominican Republic

7.1 Development of the industry

The set of elements where the Contact Center industry relies on in the Dominican Republic are: the geographical location, its human resources and the technological infrastructure, but from our interviews it was learned that at least the last two elements are relatively ideal points. The deficiencies expressed by Contact Center staff were the lack of well prepared human resources for bilingual programs, as the best qualified are already working elsewhere, and the high costs of telecommunications in current time. Some changes are expected in the telecommunication's cost in the Dominican Republic with the construction and start of the *NAP del Caribe* but as it just started to operate, the effects aren't felt yet. Usually these counterparts don't affect international investments because the operational costs are still lower by outsourcing and the country does have the geographical location, the availability of the technology and human resources willing to learn, adapt and without a strong Spanish accent.

7.2 Socio-Political circumstances

One of the main problems of the Dominican Republic is the electrical problem. It's an historical issue as it has been inherited from the Trujillo Era (1930-1961) [18] were a culture of not paying the consumed electricity was developed and 95% was not billed at that time. It was priority back then to wire the whole territory for electricity and no concerns were taken on whom to charge for the energy consumption, from this point

forward the debts started to be generated. In the 80's only 40% of the energy generated was charged having the government to subsidize more than 1,500 million pesos a year [19]. In 2008, the subsidy of the government was of 43,200 million pesos [20].

In addition to this, a considerable part of the actual power grid is dated from the 1920's, 1930's and 1940's and it originates great transmissions losses making the operational costs even higher and producing high electricity bills distributed within the few that do pay, businesses and particulars all over the country. The bigger problem is that because of all the debts the government has accumulated with generators, with the few people that pay and the huge amount that consumes, the energy produced by the generators isn't sufficient and this is why we suffer from frequent blackouts nationwide.

Because of the high electrical bills and the blackouts, companies must invest in alternative power options, since everything works with power, especially in a Contact Center where a computer or any system is down and they are already losing money.

As determined in [21], the business environment in Dominican Republic is often impacted by the political stability, stable governments help healthy business operations but with weak governments the unstable fiscal, monetary and general economy affects its development.

Riots are also common, these manifestations aren't that dangerous countrywide but there are specific sectors that have very violent reactions. What affects most is the support given by some sectors such as transportation which reduces the amount of workers that will be able to go to work, mostly workers that might live in dangerous neighborhoods. Fortunately this is not a general problem.

The Dominican Republic is not very prone to terrorism attacks that adds business costs, it scored 6.0 in a scale from 1 (adds costs) to 7 (doesn't impose significant costs) in a global competitiveness report from EUI. But in terms of crime and violence business costs, the country scores 3.1. [21]

Voltage problems and fires aren't that typical but they do happen due to regular electricity problems and overheated equipments that may produce short circuits. Power Distribution Units (PDUs) may be overloaded and the consumption of equipments may overpass the voltage supported, resulting this also in short circuits. Since cooling system problems are a side effect of the electricity irregularities, a room that doesn't comply with the standard temperature for data centers can turn into a area vulnerable to combustion. A fire is a very harmful disaster that can take equipments down for good or even entire sites. It must be considered in the Disaster Recovery Plan and prevention measures must be taken to avoid them.

7.3 Geographical conditions and typical hazards

The Dominican Republic is a country that shares the island of the Hispaniola with Haiti; this island is part of the Greater Antilles archipelago in the Caribbean. It is occasionally affected by tropical storms and hurricanes that are originated in the mid-Atlantic and southeastern Caribbean [22]. The annual hurricane period occurs from June to November.

The effects of hurricanes depending in the category and direction can produce strong winds and heavy rains, thunderstorms and floods. All these can cause trees to fall, electricity poles fall and water filtration originating disruption of essential services, damages to the installations or worst scenarios such as the destruction of the company's site. From the previous we may infer that the absence of electricity may not only be caused by blackouts it also can be a side effect of natural disasters. We must be prepared if water gets in our building with all the rain, if agents can't make it home, if our ISP is down or other situations.

The latest hurricane of major category, four or more, that passed near the southern part of the Hispaniola Island was hurricane Dean in August, 2007. It produced a lot of rain, 6 deaths in Dominican Republic and about 14 In Haiti [23]. A complete report of the hurricanes from 1909 to 2009 can been seen in *Appendix 13.2 Report of Hurricanes and Catastrophic Tropical Storms that have passed near or over the Dominican Republic in the last 100 years.*

Another circumstance of the Hispaniola is the location of the island over the boundary of the Caribbean plate tectonics and the North America plate tectonics, which means that these plates' interactions among themselves (by convergence: plates moving towards each other, divergence: plates moving apart, or transform motion: plates sliding against each other) are the cause of faults and earthquakes zones [24]. The island is affected by the following seismic faults: the *Puerto Rico trench- North Hispaniola* fault inside the Atlantic ocean on the northeast of the island; the *Septentrional* fault which goes from the northwest to the northeast and is similar to the fault that affects San Francisco, California, US; the *Enriquillo – Plantain Garden* fault that enters through the Haiti side (west) of the island; the *Muertos trench* inside the Caribbean Sea on the south of the island [25].

Faults are breaks in the Earth's crust where there have been movement of the plates like any type of the mentioned above and trenches are depressions of the sea floor created by the plate's interactions, these are the deepest parts of the ocean floor and they define the natural boundaries of the lithosphere plates. Both originate earthquake zones.

Very important catastrophic events have occurred in the Dominican Republic, there are records kept from back when the island was discover. They where dated in 1562, 1615, 1673, 1751, 1761, 1842, 1897 and one of the biggest earthquakes of the 20th century in the Caribbean, with an 8.1 scale of Richter was in 1946 [26]. Back in 2003, an earthquake of 6.5 scale of Richter occurred in Puerto Plata, coast city in the North of Dominican Republic, and it destroyed schools, other buildings and generated panic all over the country. According to experts a catastrophic event was supposed to happen soon because the natural activity of plates activate after a certain time and the event of 2003 was only a warning.

The following figure shows the seismic faults that affect the island and historical earthquakes:

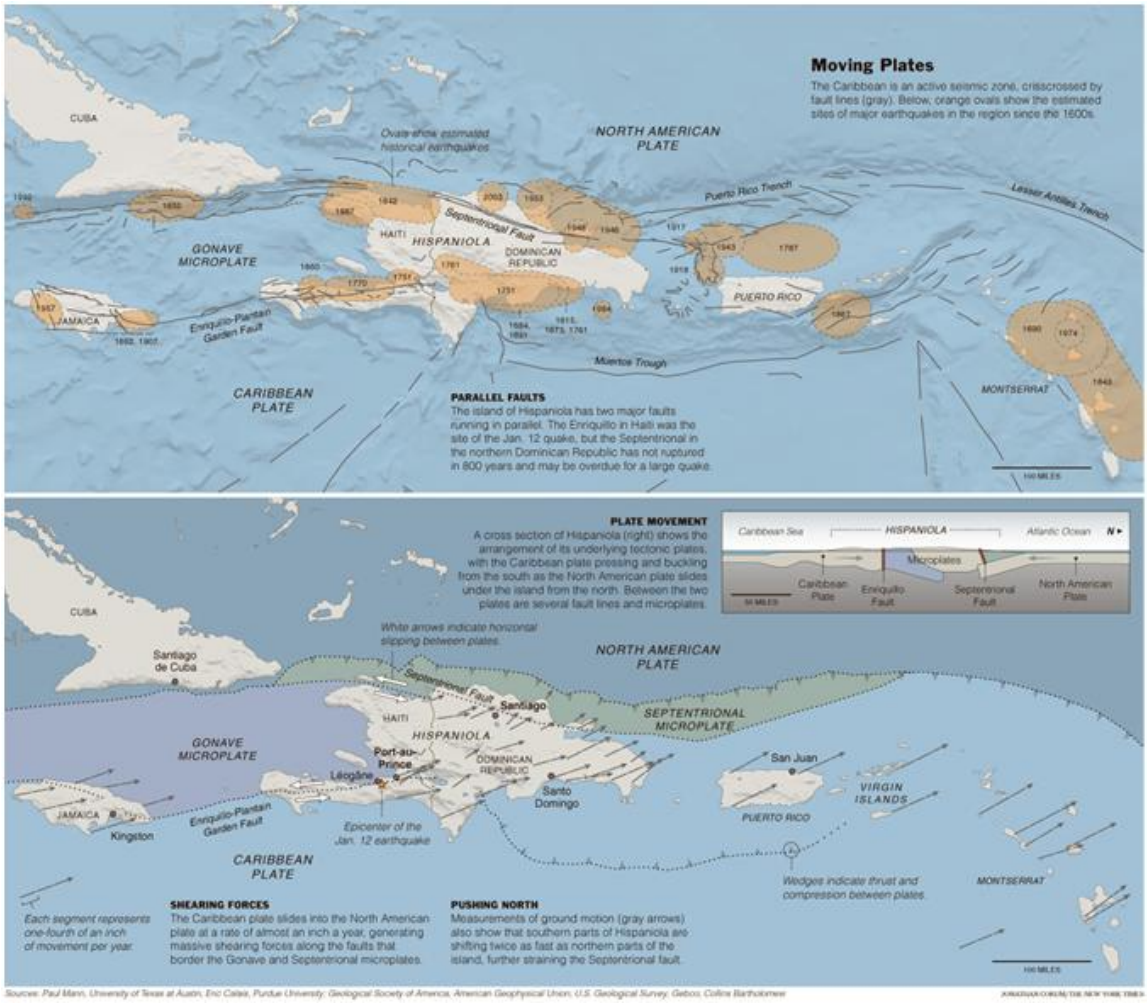


Figure 7 Historical earthquakes and fault zones in the region around the island of Hispaniola (New York Times, January 26, 2010)

This prediction happened over the island and affected our neighbors on the west side, Haiti. A terrible earthquake of magnitude 7.0 MMS occurred early 2010 and had devastating effects near the capital, Port Au Prince. A lot of buildings were destroyed including the Presidential Palace, Hotels, hospitals, roads, houses and the mayor lost of all, hundreds of thousands of lives. There was panic all over the island and the results were devastating in a country that was not prepared for such a disaster in any sense. The movements occurred in the *Enriquillo – Plantain Garden* fault.

A bad news about the status of the Dominican Republic is that it is not well prepared to handle such disasters of big magnitudes; one of the principal reasons is that there isn't a seismic memory since the segment of the population that now have decision making

positions in the public and private sector were not born or can't remember since it has been 64 years since that big catastrophic event in 1946 [26]. *"it could've happened in our side of the island."*

There are best practices that are mandatory for the design and construction of buildings in the country that are required by the government's office for public constructions (Secretaria de Estado de Obras Publicas y Communications, SEOP&C). The problem is that most constructions of buildings aren't regulated by the government office, also all constructions that date from before 1979 are in risk if they haven't collapsed yet.

In [21], the Dominican Republic scored 4.3, in a scale from 1(significant impact) to 7 (no impact), in respect to the impact of disasters on business operations and decisions. This reveals that these hazards that happen in Dominican Republic have a sufficient economic effect to the business sector. [21]

7.4 Incidents: man in the equation

Despite the fact that natural disasters are very destructive there is other category of events that could get to be as dangerous as these gigantic disasters of Mother Nature. Why so dangerous? Because when the hand of the man is involved, the nature and effects of these events can be unexpected. Disasters caused by human action, mistakes or negligence, involves not only engineering errors, environmental circumstances but also human emotions which complicates the equation.

Regular incidents that happen are thefts of physical equipments with company data, remote attacks through Internet, inside organized crimes, this being very dangerous for Contact Centers because of the important information they handle, information of clients and customers of these clients. Vandalism attacks are frequent in Dominican Republic; a typical scenario is the theft of the feeder cables of telecommunications companies to be sold in the black market after the copper is extracted.

The alteration of the exterior installations of a TELCO company takes some time to resolve. While digging the streets to make repairs it has happened more than once that

underground fibers are cut by the machinery. This accident can cause thousands of dollars to all companies that have service with that ISP.

The Dominican Republic has a weak control over IP protection and this is very favorable for delinquencies acts, the country has a 3.4 in a scale from 1 (weak or non-existent) to 7 (world's most stringent) in the implementation of IP protection laws and also the percent of software piracy rates gets as high as 77% [21].

The bank sector in the Dominican Republic has suffered various attacks but, like in the Contact Center field, most of these attacks can't be made public. In some occasions the damage is felt by the customers and there is a need to make public announcements. These attacks can be executed from hackers all over the world; last year a small Contact Center was closed because they were involved in a fraud to the U.S. Treasury Department's Internal Revenue Service. From FBI investigations, eleven Dominicans were accused of swindling US$100 million in chased checks in 2008 [27], they were filling tax returns and then sending them to United States physically and through the Internet, the group used the Contact Center business as a cover for their fraud.

8 Disaster Recovery Planning in Dominican Republic

8.1 Specific considerations for a Disaster Recovery plan

From the background that it has been reviewed, it can be said that Disaster Recovery planning is an imperative measure for companies to be in compliance, to provide outsourcing services and to protect themselves from possible disasters and incidents. Departing from the BIA and the vulnerabilities of the country, the following considerations have to be taken.

8.1.1 Data Center and digital information

One of the major preoccupations in Dominican Republic are the electricity problems consequences over equipment, especially the expensive data center equipments which might cause unavailability of the servers, network, its services and the data itself. The air conditioning can be a separate problem, originated by hardware failure or simply maintenance but sometimes can also be attached to the same electricity problem. To

protect the equipments in the design it must be contemplated voltage protectors, UPS systems, and alternative generators in a much more prime matter than perhaps in other countries, especially those that would outsource because these tend to be more developed and it doesn't represent a constant issue.

Not because electricity is a major problem, other issues are invisible: environmental conditions such as humidity, access control, fire protection, room isolation, surveillance and other security measures can't be forgotten. All of them can help recover from disasters and even better, mitigate them or ideally, avoid them. Environmental control and monitoring is something that we must include for the data centers.

To preserve the data, backup strategies must be designed as it may help us after an incident to restore the data from the backups stored in external media and it must be done in a regular frequency. All company data (databases, fileservers and config files) must be included in the plan that should be executed sharply.

Encryption is a good idea for backup media that would be kept off site because this is information that can be stolen, even if it is in a secure place; company data can be vulnerable anywhere, in the server itself, in the company and outside. But we must be careful not to hide the data so well that not even we can decrypt it afterwards. From the security of the transportation medium used to transfer the backup media, to the security in the remote location to be stored, all this helps assure the availability of the information. This of course when backups are done in physical media, because it can also be transferred at night replicating systems through data links to other company servers and in those cases the need for security will still stand in the same point.

A redundancy strategy is very necessary for data centers in the country and worldwide, because it provides a sort of relief for sudden situations. In the redundancy policy it's not only about equipments, but also cables, services, terminals and personnel, it's never healthy to have only one person in charge of various systems, general or specialized, because it can really affect us if any accident occurs to that person. IT staff isn't that easy to find and when you have special equipments or systems you need enough people that

can manage those equipments and systems. The general situation is to have a person in charge and a backup for that person.

In the country there are no standards or regulations for Contact Center and only two laws exists that are not very well known or clear to the population, Law 53-07 about Internet Crimes (*name in Spanish: Ley Contra Crimenes y delitos de alta Tecnologia*) and Law 126-02 about Electronic Documents and Digital Signatures (*name in Spanish: Ley de Comercio Electronico, Documentos y Firmas Digitales*). Because of this, there is a need to have good legal advice and orientation that can underwrite the company and make them comply with any legal implications. Since most Contact Center services are offered to outsourcing international companies it is usual that these must comply with some necessary standard required by the foreign country. Besides this, standard certifications are recommended as a global Best Practice for all. In the country there are companies certified or working to achieve PCI and ISO 27001 compliance. Standards such as the ISO/IEC 27001 Information Technology-Security Techniques-Information Security Management Systems-Requirements, *ISO/IEC 27002* Information technology-Security techniques- Code of practice for information security management and *ISO/IEC 24762:2008* Information Technology-Security Techniques-Guidelines for Information and Communications Technology Disaster Recovery Services, are recommended.

8.1.2 Voice lines and Data connections with ISPs

ISPs can turn into a big nightmare as we depend so much of them, they offer us the connections we need to the world and their unavailability can just break our peace. The relationship with them can be compared to marriage; everything is fine most of the time but struggling moments also happen. The problem in Dominican Republic is mostly with the cost of telecommunication and not the availability. In the past there only existed one Telco and this created a monopoly tendency over telecommunications during decades; because of this they were the most powerful company for years and had the greatest external plant infrastructure even after new Telco's arise. As a result of this, newer Telco share at some point these resources, as it was cheaper for them to lease lines in some parts in order to extend their range nationwide than to rebuilding a full new skeleton from scratch, specially for outside of the country connections. This affects the designs for

disaster recovery planning, because it might be thought that these are two independent communication lines and truly they're not. Then the following situation may happen: that the primary and backup providers have the same point of failure where does that leave your backup strategy.

Data connections are very important for Contact Centers, both Internet and direct data lines; this is their gateway for exterior communication. The ideal scenario would be to have three different providers but not in all cases this may apply. One of these providers could be via satellite which will help us be protected against fiber failure in some common point for ISPs using common media. We must be aware that backup lines via satellite may just not have enough quality and our SLAs will be affected but at least we can offer the basic service; this is one of the things that should be carefully considered and analyzed.

Usually in a Contact Center, the voice lines that are contracted aren't for the agents because inside the Contact Center they have their own PBX to manage calls in-house but these voice lines are used directly by the PBX equipment to manage all calls. When a T1 of voice fails or the module to which it's connected we will have less lines available, 23 or 24 less depending in the signaling, to handle the calls of the clients. If any incident could put us in this situation, we would have to make all configuration changes to balance the load with other available resources. Since voice lines are delivered just like data, the same crucial considerations apply for both; the strategy decision is with the ISP.

8.1.3 Equipments

Contact Centers have very expensive equipments as they are specialized for functions proper of the business. The ideal situation would be to have a replacement for everything, but that is an almost impossible mission. What can be done is to take the measures needed to diminish, as much as possible, the probabilities for such destruction. As earlier discussed, certifying the data centers security is one of the best ways to go, but in addition to that we must prepare for what happens if.

For some equipment, like servers, we can have cluster configurations and virtualized servers that give us the flexibility to clone the images and have these as backup, it's fair

to say that some servers do have their backup replacement because their affordability and criticality permit it. In the case of other equipments like the PBX itself and the recorder, which are special, expensive and dedicated appliances that can't be substituted, the cares should be more. Where replacing is not an option, we must look into the option of repairing and troubleshooting as fast as possible. For this, experience is a key such as having available contact information of the gurus that manage our important equipment. Maybe we cannot replace the whole equipment but with the modular feature of most of these specialized equipments it is possible to buy and have replacements for some parts.

Good communication and relationship with your account manager from the vendors of equipments can help you with the facilities of lending equipments temporally or just getting them for you in a shorter time. Another option we can consider is the agreement with major providers to lease spare from them.

Other equipments needed such as computers, laptops, telephones, printers and other supplies and spare parts like ink, RAM, mice, keyboards, power supplies, power cords, monitors, monitor cable and others, are important replacements that should be kept in sufficient amount in store for quick supplies and problem solving by Technical Support. It's also important to have hardware tools available like network kits, blow drier, soldering iron, patch cables and other handy supplies according to typical problems. For computer quick replacement it's good to have cloned images of the basic set of programs frequently used in this environment in order to give faster support.

The complicated about all of these is the economical disposition of management to support all redundancy plans, but it's a commitment they must encounter when needing to comply and designing a disaster recovery plan. They do know this but, most of the time they push to make the numbers small in terms of investment.

8.1.4 Natural Disasters, Power failures and Fires

In terms of natural disasters, the island of the Dominican Republic is certainly positioned where hurricanes and earthquakes can cause a strong impact. It's not that they strike everyday but a periodicity occurs and preventing is about preparing before anything happens to avoid devastating consequences to our business.

On January of 2010 a terrible earthquake affected the west side of the Hispaniola; the country of Haiti was devastated after a 7.0 MMS (Moment Magnitude Scale) quake near the capital city, Port Au Prince. Thousands of lives lost, buildings, streets, bridges collapsed over the habitants and panic was all over the island. This was produced by the movement of the plate's tectonics in the seismic fault over which the island is; specifically it was a rupture over the *Enriquillo-Plantain Garden fault.*

This quake was very strong and the damages were to happen but the situation was worsen by the fact that the edifications in Haiti are built with minor regulations and less quality and quantity of the materials needed for constructions. In the Dominican Republic some regulations exist for constructions but not all follow them and there is a lack of control for constructions. This situation helps us realize how exposed we are and that there is a need for Dominican companies to invest in Disaster Recovery planning, build ant seismic edifications, protect the buildings that are constructed already, protect their assets, protect their people, and never assume that there is no need to be ready and no need to invest.

Probably after that strong quake and the continuous seismic movements, measures will be taken to enforce the prevention mechanism and construction regulations, as well as the contingency plans for earthquakes, rescue teams equipments and trainees. According to the Dominican's Emergency Operation Center, in the whole country only the Firefighters from the capital city, Santo Domingo, have equipments for the search and rescue in collapsed buildings [28].

About power failures, the most important thing to highlight is the need for alternative power, no matter which province of the country, all businesses will need to invest in power generators because the one provided by the energy company is very inconsistent; not only in terms of amount of service time but also the quality of it (voltage levels variations). Some companies in the country are experimenting with solar panels and other alternative energy source because the prices of the derivate products from petroleum are very high and the costs for traditional electrical power generators raise costs. This is why for the majority of companies the operation costs are high, but looking at it from the bright perspective, it forces them to be prepared in order to keep the business operating.

For Data Centers, additional to the company's general power a UPS solution is needed for emergencies and to help everything during the period where the electricity goes out and the generators turn on.

Fires are huge disasters, and prevention regulations must be followed. In the country some companies have smoke detectors, extinguishers and water spreading systems but the maintenance given to these not in all cases is the best. The rates of fires aren't very high but the devastating effects are, and this is why there should be a protection strategy for this threat despite the low frequency of occurrence. A local company had a fire on their data center in 2008 due to a short circuit while changing a motherboard on modular equipment during the morning. The firefighters arrived and their intention was to start spreading water all over the place, inclusive over the core systems in the data center. Thankfully the data center had an oxygen suppression system the fire was contained. Even though some damage occurred to equipments and there was a service outage during business hours for a couple of hours and production was affected. Occasionally fires do happen and this is why these types of disasters need to be contemplated in DR plans.

There is a huge set of threats that should be prevented that count as disasters even if these aren't hurricanes, earthquakes and fires because they affect our operation and jeopardize our company, such as: networks issues, hardware and software failures, malware, cyber attacks, configuration errors, bad updates/firmware, SPAM, sabotage and diseases; and organizations should consider these in the Disaster Recovery Plan. All the previous mentioned are Security breaks and to handle them there is a need for Incident Response Management.

8.1.5 Testing, Training, Distributing and Maintaining

As important as designing the strategy and elaborating the plan, there are four other subsequent tasks that define the success or failure of the overall process. After a plan has been developed the team must test the plan to verify if it will fulfill its purpose. The testing stage is important as it helps determine any weakness of the plan and to observe how the executers would follow it. It can never be said that the way they react on a simulation is the same way they would during the moment of the disaster, but at least the

process flow towards recovery can be reviewed. The errors can be corrected, any not considered system or process can be detected, coordination, performance of the alternate systems or equipments, load distribution over the recovery team, and any other flaw can be measured. Good observation is needed to be able to determine all details. Usually this phase can be done while the DR plan is being elaborated and afterwards when making any maintenance changes, it's not very common, but it is very necessary because after any significant variation on the system and infrastructure, the plan might need a change. It can be said that these four stages (*testing, training, distributing and maintaining*) are like a cycle and should be followed one after the other.

Even if we have a perfect plan it could be followed wrong, and this is why the training part is essential for the organization. The training of the people on how the instructions are designed takes the plan to the real level and assures the knowledge is set to the team members of the company so they can follow the plan.

The distribution part is very important; copies of the approved plan should be handled among staff. Since the DR Plan discussed in this project is just oriented for ICT, not all company staff should have it because of the confidential information that it contains. When working with general Disaster Recovery plan that include evacuation plans, then all staff is involved. It should be in the hands of management, IT staff, Supervisors, Project Managers and the related personnel involved in the Recovery process that must have full knowledge of the plan. A good practice is that during the induction, while starting a job, besides training them for their functions they also start being oriented about the DR plan and how that person will be involved, this of course according to the position and its role and importance in the DR plan.

The plan should be hard copied and safe not only in the company but also accessible from the outside in case of mayor disaster. Soft copies can be saved on electronic media, digital on storage online, and hard copied on another location; the more accessible the better. It's recommended that each member of the recovery process would have two copies of the plan, one at their workspace and another at their houses. There must be a control with sequence numbers of the copies to help keep track and assure that all

members have updated copies; when handing in new copies it should be demanded to turn in the older versions each person has to avoid that outdated copies can be accessible and confused with the newer ones.

The maintaining process is a commitment to the overall process, without it the plan can become obsolete, useless and turned into a waste of time. Changes happen all the time, it's constant, and the need for updates will happen because of these changes. The sad part is that even when there might be periods were the enthusiasm will succeed and this goal can be followed there could also be some points that this can stop happening. To maintain this, a person should be assigned as the project manager for the DR planning; that person will be held as the responsible for that maintenance and it will be part of his/her functions. This can give us the peace that there is a position responsible that can give a constant maintenance. Updates should be scheduled with a certain periodicity such as annually and in case of the appearance of new threats or weak points. A copy must be kept wherever backup media is saved.

In Dominican Republic, there isn't a very strong culture of documenting. This problem has increased but efforts are being made to adopt a change. The whole DR planning might be seen as a painful process and these four stages for DR continuity are not accomplished with much enthusiasm. Usually it happens when something is done to fulfill a requirement but it's not assumed with commitment.

Very important is the post disaster analysis that must be done to evaluate the plan and do any corrections necessary. This gives the chance to improve the plan with the experience of past events.

8.2 Alternative site considerations

In the Dominican Republic offsite locations aren't considered a regular strategy because of insufficient funds. Not even all big companies have alternative sites and less will the small businesses. This can be more common if they have more than one location and would arm a secondary data center with the basic systems and equipments but even like

this, the sites aren't identical. Maybe banks have alternative site, but it's doubtful that Contact Center do.

Having other sites and a replica of all the systems and equipments to balance load and serve as backup, is a very ideal plan because it requires a huge investment and not all types of business can accomplish that goal. It is not very common that companies have alternative sites even that it's the best solution for DR; this is something that happens only in this country, but also in others.

8.3 Incident Response Management

Incident Response strategies are very important for Disaster Recovery; these are the section in the DRP dedicated for events provoked by humans. When a security vulnerability is exploited and there has been a breach or attack, such as SQL injection, malware, Denial of Service, unauthorized access and other incidents, the incident response strategies are the path to handle the situation limiting the damage and reducing the costs and time of recovery.

These Incident Response strategies should be reflected in the step by step indications included in the IT department manual of procedures and policies and in the DR plan. To maintain a standardized position and design the guidelines according to security best practices, one of the best set of steps for Incident Response strategy preparation are the steps designed by the SANS (SysAdmin, Audit, Network, Security) Institute. These guidelines serve to avoid bad decisions to be made during the panic moments, it's best to have a specific action plan as guide [29].

These set of steps are the ones that best suit the design of the strategy, which are: Preparation, Identification, Containment, Eradication, Recovery and Lessons Learn [30].

The Preparation is needed to diminish the risks of possible threats. In order to accomplish this, all security measures for the network and independent hosts and servers are needed. The Identification step is performed by the team in charge of identifying the event that just occurred and analyzing the evidence to officially determine what happened and which are the following steps. In the Containment step, the team must analyze how

expanded the problem is, how much has been affected and the measures that must be taken to contain the problem from spreading even more. These measures depend on the type of the attack and the methodology used. Typical solutions are to disconnect from the network or unplug the affected systems, reroute traffic, changes on configuration. After this is when backup copies of the affected systems should be made for Forensic analysis.

The following step, Eradication, depends on the previous one because what needs to be done here is to remove from the root the traces, codes, data and vulnerabilities related to the incident but in order to do this, the team needs first to discover the origin. Recovery is what follows; recover from backup data and config files or from scratch, after this step the systems are back to production. In this stage the team must assure that the system or any system on the network isn't vulnerable to the past threat and should be monitored. The final step is very important, it's about the Lessons Learned; here the incident that happened and the way the Incident Response procedure was followed are analyzed. This helps correct any flaws, recommendations are made and a final report must be elaborated of what, how, where, who and when happened.

9 Cost Implications in Disaster Recovery Planning

An important element in the Disaster Recovery plan's preparation is the cost that implies to make any changes needed to support the backup and redundancy strategies. It's a difficult task to get an approved budget, but one of the best negotiating strategies is to show them the numbers. In most of the cases an analysis on these previous events can prove that a DR plan could represent less in terms of money that the effect of the past disasters. What a DR team should do is to recompile information stored in the company about losses produced by events that have affected or stopped production and regular income and make a relation on the frequency of these incidents. And a percentage of those losses suffered can be suggested as an appropriated amount for DR budget.

No specific information was available to use as an example that revealed real economical losses in a Contact Center due to disastrous events.

Since most Contact Centers in Dominican Republic are small to medium organizations the considerations for alternative sites aren't cost effective solutions because of budget limitations. An excellent idea is to build up a general skeleton infrastructure of a Contact Center containing all basic elements, this created by an association of Contact Centers willing to share the costs of maintaining that site and services. Then each Contact Center would prepare their DR plan based in that alternative site for extreme cases, including training of the personnel, equipment configuration, traffic rerouting and all that is needed in order to recreate their regular scenario. This solution would be cheaper than alternative site solutions. Of course there are some other considerations with this solution such as the maintenance and usage agreements (especially when two or more of the contact centers are affected at the same time) defined by the society that would have to require good relationships, understanding and responsibilities among these Contact Centers.

In any case the team in charge of the DR planning should consider at least the estimated cost for ISP redundancy, workstations spare, special network equipment's spares and training. This should cover the basic for the initial development of the plan and can be enhanced as the management understands the importance of the prevention.

10 Proposed Best Practices for Disaster Recovery in Dominican Contact Centers

10.1 General Recommendations

The objective of a DR plan is to recover IT critical services and systems to support the strategy of providing basic service coverage for customers in case of an event.

The recovery objectives and timeline must be set consciously, it's not appropriate to establish impossible timelines, of course that it's best to resume operations as soon as possible but the objectives and timelines must be real and should be somehow flexible depending on the severity of the event so that the maximum outage time that goes along with the business needs and Service Level Agreements aren't violated.

As the SLAs are established when negotiating with the clients, also the RTO and RPO in case of disasters must be discussed to determine the values that can suit both parties, one

that the Contact Center may accomplish and that won't affect the client's company and service to their customers.

The process should be described in a simple fashion, the most important elements are the steps to follow, the order of importance of systems, processes and data to recover, contact information of DR team members, of the emergency agencies of the country, of the suppliers, partners and technical support. When developing the plan, we must assure that it can be executed by others; it must be elaborated so that anyone can follow it and the correct way of proving this is by making others to test it. Proceeding like this any unclear detail can be fixed.

Standards such as the ISO/IEC 27001:2005 Information Technology-Security Techniques-Information Security Management Systems-Requirements, ISO/IEC 27002:2005 Information technology-Security techniques- Code of practice for information security management and ISO/IEC 24762:2008 Information Technology-Security Techniques-Guidelines for Information and Communications Technology Disaster Recovery Services are compliances that help the path toward Disaster Recovery planning much more reachable.

10.2 Disaster Recovery Preparedness

10.2.1 Physical Security

Since most of the Contact Center specific equipments aren't found everywhere there must be special considerations designing the backup for these.

Virtualization is a very important helper for DR; with this accessible technology we are able to make snapshots of our real, physical servers and save these copies available to start any server with a virtual hypervisor. Several tools exist to make these copies. This is a measure that can help us to have actual copies of our servers' configurations and tasks can be schedule to take snapshots with the frequency needed according to our backup policies.

Another big issue is focused in the power problems, redundancy for power must be considered in all levels but especially for data centers. Mechanisms to consider are UPSs,

inverters and secondary power generators. Without power a company can cease all operations. Special attention should be given to this issue in Dominican Republic.

Redundancy is not only needed for services and power, spare for hardware and software must be kept in the company. For the equipments, there should be replacements kept in storage, in the cases where possible, such as extra computers, telephones, cables, peripherals but for others equipments like servers and Contact Center specific this can't always be possible, companies must work around this problem as these equipments are very important. For some servers, we may have more than one, for other systems we can take advantage of the modular composition of modern equipments. Good communication and relationship with account managers and providers can help the company get fast spare equipments or even get temporarily equipments for quick incident response in case of an event that may affect our physical equipments. We must also have good communication and all contact information needed from Technical support and gurus of the system.

For software redundancy it's a good practice to keep all installation CDs and executables organized in a specific place and each should have its respective serial. There should be a document listing all software, the location of their installers, its serial or license detail and the supplier information.

Good security policies for the whole network and equipments on the network will lead to a more robust force to fight against hackers, malware and other threats. Each host should be protected with antivirus, must be fully patched, and must have the firewalls activated. In the network it should also be firewall appliances, reliable authentication methods, Intrusion Prevention Systems (IPS), content filters, SPAM controllers, Demilitarized Zone (DMZ) when required, Data Loss Prevention (DLP) strategies, data encryption for backup medias and critical data systems. All security measures that are properly and strongly enforce will help the organization be able to try to diminish the disasters of attacks and hacks when humans are in the equation.

For physical facility's threats it's important to have good physical security with cameras for surveillance, environmental control such as humidity, air conditioning and fire suppression system, door access controls and security personnel in the buildings and important locations. For Data centers, even more restrictive access policies should be applied.

When buying a building or constructing one, a company must contemplate the anti-seismic properties, but the regular scenario is that the company is already located so they must protect the building and follow existing building security rules that may require certain modifications and reinforcement. The city should be prepared by enforcing the prevention mechanism and construction regulations as well as the contingency plans for earthquakes, rescue teams equipments and trainers.

Fires are dangerous hazards and their effects can destroy our valuable assets. For their protection: smoke detectors, extinguishers, water spreading systems and/or fire suppression systems are needed as well as the maintenance of the systems implemented.

10.2.2 Logical Security

To be able to handle a situation of disasters classified between a low and medium level, usually good security and redundancy measures make recovery a faster and better process.

Policies and Procedures must be designed to establish when to trigger the activation of the Disaster Recovery Plan. Here we must clarify what is considered a disaster and how it must be classified according to the levels of Low, Medium or High outage consequences; and also who has the authority to trigger the activation.

One of the most important measures for a company are the backup policies, most recovery strategies rely on these backups that must be based on the needs of the company. All technology based companies must backup their data, systems and equipments. In the backup policies we have to establish a frequency that will depend on the RPO, which is the amount of data in terms of time that the company can afford to lose in the case of an eventuality. For Contact Centers, data is less critical than the

telecommunications services and systems so they focus more on the backup and redundancy for these; nevertheless, backup strategies should be developed for databases, fileservers and config files.

Encryption should be considered for backed up data, stored data and for transmitted data over the network. Protocols that transmit in clear text shouldn't be used in the network, these aren't recommended.

Redundancy for ISP services is very critical, data/Internet and voice lines are the connection media to the clients and customers, and this is how Contact Centers can participate in the Outsourcing business model. In the backup policies the company must establish the amount of redundancy for each service and for the equipments. For the data/Internet and voice lines the best is to have contracts with more than one ISP.

Documentation is important and a good practice is to have the configuration of servers and network equipments documented so that if it's needed to start from zero we have those important details reachable. A technique for server's configuration backup, are the tools available that convert our real servers in virtual machines so that they can be powered on in a hypervisor afterwards.

Testing the backup media and redundancy lines and systems is very important as discussed earlier, for reliable disaster recovery.

Insurance policies can be handy for companies that have high investments like Contact Centers but it implies a much higher investment that not all companies are willing to make. In general, companies must invest in order to have security, redundancy and some sense of preparation to survive to disastrous situations and be ready to recover.

For prevention, vulnerability tests are helpful to identify some risks that the company is exposed to and by having knowledge of these issues on time, they can be solved. These vulnerabilities can become a way to past our security and turn into an organizational disaster, trespassed and attacked. This is very important for preparedness.

There exists another training that needs to be included; it's not only about training DR team members about the plan and how to follow it, there is also the need to train ends users for prevention for incidents. One of the less controllable vulnerabilities in a company are the end users, and they can be fooled by others using social engineering tricks, phishing, SPAM or compromised during web search on dangerous sites. All these tricks can seem inoffensive and that's why they are fooled. The problem with restricting the access to these users is that they may need most accesses for their work, and you can't restrict them totally instead what can be done is to try to educate them. Even with this education, they are still unreliable and the equation can turn complicated but the combination of all the measures is acting with prevention.

Campaigns can be set analyzing simple case scenarios that indicate the risk of posting work information on social networks, they should be educated on the dangers of opening certain kinds of mails or pressing any links from both company and personal email accounts, it should be about warning them of possible and popular social engineering tricks.

Host, Servers and Network controls are part of the IT security, it's important to control their access to USB storage media, implement SPAM blockers, Web filtering and access controls, antivirus, group policies, firewalls, VPNs, authentication methods and other security measures that would reduce the risks.

Companies must have written policies, procedures and forms for all operation process; this helps the company's organization and sets the dos and don'ts for employees since the beginning. It's a limit establisher of roles and responsibilities and can prevent some human mistakes or ignorance claim. With general policies some education can be given to end users, also IT policies and produces help the process flow for IT to be documented.

Maintenance is a very important resolution; this helps systems such as air conditioners, fire sprinklers, fire extinguishers, backup systems, power generators, UPSs and other systems to be available and functional when the time arrives for them to be used.

When changes are needed like patches, config modifications or replacements these should be analyzed and when possible, a lab environment to make such changes first should be created, test the results and be able to detect and solve problems that might occur. Virtualization can be used for this. Not all scenarios can be recreated but if there is a chance to do so, it can save some bad moments if something goes wrong on the production side. A change control should be kept where all changes are registered for each system or server configuration, this written historical is a better documented and reliable source than the human mind.

Another security measure to protect our network is to disable ports on servers that aren't needed for the services running on the network and log policies should be kept for all or important systems.

All the above is necessary and aligns with the first step of the SANS Institute best practices, Preparation [30].

10.3 Disaster Recovery Phases

In a proper order, the first step after management approval and team selection for Disaster Recovery is to do the Risk Analysis to determine these risks mentioned above and others that can be related to special conditions. This identification is what helps us seek the correct measures best oriented to really prepare for disasters. The DR team elaborates the strategies, define the roles and responsibilities and elaborate the plan and the needed policies and procedures to compliment the plan. Then after approved this plan is tested to identify flaws and correct them, taught to others, distributed among key personnel and then a maintenance policy must be followed to keep this plan updated.

In order to accomplish a more complete DR plan, for the strategy we can include a set of three level recovery strategies. Classification can consider Small, Medium or Large Outages based on the severity of the disaster and period of downtime; where large outages are more related to facility damages.

The maintenance is very crucial in order to have a successful plan and these updates will require repeating the cycle of testing, training and distributing.

Once an approved version of the plan is ready, in the incidence of a disaster the first phase is to identify what has occurred, what are the effects to our company and based on the policy for the plan activation, the responsible should indicate if the plan should be activated and in what level. Also it must contemplate the notification procedures to be followed and a damage assessment must be elaborated. Then the action plan should be executed as determined in the strategy designed, this is the execution phase. This starts the incident response and recovery process.

After the plan is completed and the reconstitution is done, we must start a post disaster analysis to evaluate the plan, the team and the upgrades that are needed to polish even more the Disaster Recovery Plan.

10.4 Outline for the Disaster Recovery Plan

A simple guide through Disaster Recovery Plan is the best methodology to achieve a plan that people under stress and living a non-idle situation can follow. The following are sections the must be included in the DR Plan:

10.4.1 Introduction

The purpose and objective of the plan must be indicated in this section. Despite that there is a specific section for roles, in this section it's good to define and establish the positions of the roles in charge of training and testing, these two roles aren't part of the execution of the plan but they are part of the team of creation and polishing of the plan.

10.4.2 Scope of the Plan

In the scope the coverage of the DR plan should be specified, the elements that are included to be recovered, the RTO and RPO defined, and if any classification is used according to disaster severity, it should be identified and described in this section.

10.4.3 Record of changes

This section is important to keep track of changes and version numbers. Here it must be defined which are the parameters for changes out of the maintenance periodicity, which will be the maintenance periodicity and the table of the last changes remaking the current version. The role and company position of maintenance and distribution can be defined here.

10.4.4 Plan activation

In this section the DR team must indicate when the Contact Center will begin to execute the DR Plan. They must establish what elements will trigger the plan and which elements serve to determine the level of a disaster. After a disaster occurs, if unexpected, there is a short time of analysis that happens before the plan activation, here is where the person in charge will determine the action to take by the company. When an incident occurs the team must analyze the causes and effects of what just occurred. For ICT in a Contact Center the best recommended members are IT staff and upper management. What needs to be established here is reflected to the second step of the SANS Institute best practices, Identification [30].

10.4.5 DR Team Members

Here should be included a diagram for better understanding of all the roles and a description of each one so that the participants get a refreshed understanding of their function in the process. There is no need to focus on proper names, instead they should be identified and referred by roles. In the Emergency Contact Information section a table will indicate the role, name of the person and all the contact information possible to reach that person. This table should be updated when any contact information changes, even if no other changes are made to the DR process.

Some general roles are Recovery Executive Leader, Communication Representative, Log Maintainer, Post Disaster Analyzer and specific Team Leaders for Network Support, Hardware, Applications Software and Systems, Database Applications, Security Analyst and a Helpdesk and Technical Support leader. Another simple strategy for selecting the team members is to name the Director of IT the General Manager of the DR team and then each Manager of each related sub-area are hold responsible as the Team Leader of their area, this can assure cross-functional participation.

The establishment of the Roles is very important and in the identification process, all areas must be included. Each company can select the method that suits them best, but what can never be forgotten is a Recovery General Manager, a Team Leader for each important IT area and a Post disaster Analyzer.

For each role their overall mission and important functions must be detailed in this section. In the DR team members' selection process, it's good to include key personnel that know the system, that are able of managing the process and that are active people.

10.4.6 Action Plan

This is the most important part in the DR plan, here it must be detailed what the team members need to do during the recovery processes and which are the steps that need to be followed. What needs to be done for each system? Who will perform the task? In which order the plan should be followed? These are some of the important questions to be answered. In this section not all technical details must be included because it can complicate the document. Instead it can refer to the IT manual of procedures and policies. This is something that not all companies have, but that should be created; it's a manual of the regular procedures in the IT department. Sadly, it's not very common in Dominican Republic because of the non-documenting culture, but this is an improvement point.

In the action plan it must be indicated how to proceed in the case of a disastrous incident. How to contain and stop the effects of such incident? What evidence do I need to conserve and handle? What needs to be done to remove the vulnerability and clean the affected systems? How to restore the systems or data back to normality?

The action plan should be designed in order to achieve its prime goal which is efficient and fast recovery, and the guidelines from the third, fourth and fifth step of the SANS Institute best practices which are Containment, Eradication and Recovery, are well suited for achieving this goal [30].

10.4.7 Restoration Order by Priority

Here the team must indicate all the systems to be recovered and their priority order. A good practice is to have first a table indicating the application name in the order of restoration and their priority value. Then general information about each system which could be only relevant information and for more details it could refer to a general document of the systems that could be appended.

10.4.8 Emergency Contact Information

There must be a section with all contact information, details such as cell phone, home number, office number, any other emergency number even any close family member. This list should include all DR Team Members, Emergency Country Services, Transportation & Airlines, Suppliers, Partners, Utilities and any other group considered necessary for the company.

10.4.9 Appendix

This section should be included to add the policies and procedures of the company that might be needed during the recovery process, such as the backup policies and procedures, the general IT procedures handbook, relevant system description and architecture, which other systems it might interact with, indicate the server's specs over where it's running, suppliers name and any relevant detail about its configuration. Even if a particular policy of procedure didn't exist if during the DR process it's indicated that it's needed it should be elaborated and included here. Afterwards it would be something that will help the documentation process of the company.

10.5 Important elements

Not only it is important to have a good plan designed, to have a good team to follow the plan but also we must analyze after a disaster what happened and how the plan was followed. This Post disaster analysis is very helpful to fix any passed detail and anything that went wrong due to a miscalculation in the design of the plan. Even thought when testing some errors are detected, the most reliable source of miscalculations comes in the post disaster phase, here those errors not visible over the previous phases jump to the fore. This last and constant phase goes according to the last step of the SANS Institute best practices, Lessons Learned [30].

11 Conclusions

As discussed in the world “a stitch in time, saves nine”; this is what Disaster Recovery represents for most companies a stitch but as the proverb says it’s worth it in order to save other nine. One of the strongest concerns from a company’s point of view in respect to it, it’s not the time and effort needed but instead the investment it represents to backup a proper strategy.

For Contact Centers, Disaster Recovery planning is an obligation because of, first their urgent need to be available in order to offer services to their clients and they represent an important part in the commercial business model because they are the point of contact between their clients and the customers of our clients. Nowadays this support and contact is a critical chain for the marketing and image of a company and that customer service might determine whether a customer would stay with one company or the other in this competitive world. What Contact Centers do is a very vital aspect for leadership in the market for those companies; and not only from the customer care position but also, sales and as whole backend operations centers for some others.

A second reason for Disaster Recovery being an obligation is the compliance requirements set from International laws and standards, that even if not applied to Dominican companies directly, they do affect them when doing business with companies from those foreign countries; this is part of the outsourcing model.

It has been discussed the importance of the Contact Center industry and the importance of Disaster Recovery Planning, and what’s the issue with Contact Centers in Dominican Republic? They rely on the fact that this is a sector in a maturing process and as an important economical sector it’s necessary to highlight this area of improvement that needs to be attended.

This project has exposed some little "well known secrets" in the Dominican Republic but that are important to know for foreigners in order to understand the Dominican people and business, why some actions have a pattern, the quality that Dominicans have gained from their history and this helps negotiation to improve faults.

A very interesting point is that Dominican Republic is growing in the sector and competing against other important countries in the world and this is just one of the steps that we must focus from the checklist used by investors to select a candidate and the country must assure that that particular box is checked.

An important mark form this research project is that when elaborating a Disaster Recovery plan you must integrate general guidelines with the particularities and needs of the industry sector type, the location and the social-economical-culturist factors in order to develop a plan tailored. The guidelines help the process and should orient a team to focus on a set of elements that you need to consider when customizing a Disaster Recovery plan and that might be overlooked.

12 Terms and definitions

Contact Center- "A contact center (also referred to as a *customer interaction center* or *e-contact center*) is a central point in an enterprise from which all customer contacts are managed. The contact center typically includes one or more online call centers but may include other types of customer contact as well, including e-mail newsletters, postal mail catalogs, Web site inquiries and chats, and the collection of information from customers during in-store purchasing. A contact center is generally part of an enterprise's overall customer relationship management (CRM)". [31]

Disaster Recovery- "A disaster recovery plan (DRP) describes how an organization is to deal with potential disasters. Just as a disaster is an event that makes the continuation of normal functions impossible, a disaster recovery plan consists of the precautions taken so that the effects of a disaster will be minimized and the organization will be able to either maintain or quickly resume mission-critical functions. Typically, disaster recovery planning involves an analysis of business processes and continuity needs; it may also include a significant focus on disaster prevention." [31]

INDOTEL- "Instituto Dominicano de Telecomunicaciones" Dominican Institute of Telecommunications. Is a state's agency created by the General Telecommunications Law (No. 153-98) that regulates and oversees the development of telecommunications. Its mission is "to regulate and promote the provision of telecommunications services for the benefit of society, in a free, fair and effective competition." [32]

CEI-RD- "Centro de Exportación e Inversión de la Republica Dominicana" Center for Export and Investment of the Dominican Republic is a "decentralized governmental institution, dedicated to the promotion of exports and promotion of foreign direct investment." [33]

ACC-RD- "Asociación de Contact Centers de Republica Dominicana" The Contact Center Association of the Dominican Republic (ACC-RD for its name in Spanish) is "the result of hard work and initiatives that had been in development in the industry for

several years and its mission is to promote and support the growth and development of the Dominican Republic contact center industry.” [34]

SLA- “A Service-Level Agreement (SLA) is a contract between a service provider and a customer that specifies, usually in measurable terms, what services the network service provider will furnish.” [31]

BIA- “Business impact analysis (BIA) is an essential component of an organization's business continuance plan; it includes an exploratory component to reveal any vulnerability, and a planning component to develop strategies for minimizing risk. The result of analysis is a business impact analysis report, which describes the potential risks specific to the organization studied.” [31]

PBX- “A PBX (Private Branch Exchange) is a telephone system within an enterprise that switches calls between enterprise users on local lines while allowing all users to share a certain number of external phone lines. The main purpose of a PBX is to save the cost of requiring a line for each user to the telephone company's central office.” [31]

IVR- “Interactive Voice Response (IVR) is an automated telephony system that interacts with callers, gathers information and routes calls to the appropriate recipient. An IVR system (IVRS) accepts a combination of voice telephone input and touch-tone keypad selection and provides appropriate responses in the form of voice, fax, callback, e-mail and perhaps other media.” [31]

ACD- “Automatic Call Distributor (ACD) is a telephone facility that manages incoming calls and handles them based on the number called and an associated database of handling instructions. Many companies offering sales and service support use ACDs to validate callers make outgoing responses or calls, forward calls to the right party, allow callers to record messages, gather usage statistics, balance the use of phone lines, and provide other services.” [31]

PD- “A predictive dialer is a telephone control system that automatically calls a list of telephone numbers in sequence, screening out no-answers, busy signals, answering

machines and disconnected numbers while predicting at what point a human caller will be able to handle the next call. Predictive dialers are commonly used for telemarketing, surveys, appointment confirmation, payment collection and service follow-ups." [31]

Outbound- "Outbound Call Center services pertain to activities where agents place calls to potential customers with the intention of selling products or services to the individual." [35]

- Telemarketing/Sales: "May be inbound or inbound sales performed through telephone communication by a contact center."
- Lead generation: "Lead Generation refers to the creation or generation of prospective consumer interest or inquiry into your products or services. It is associated with a marketing activity targeted at generating sales opportunities for your company's sales force. "
- Debt collection: "Activity to collect money owed by a company or a third party."
- Survey: "A tool utilized by social scientists, marketing researchers, pollsters, and statisticians, surveys establish the numbers and proportions involving your products, and measures public opinion on new products or services."
- Market research: "The process of systematically gathering, recording and analyzing data about your customers, your competitors and your product's niche. Market research is essential for creating most business plans, launching new products and services, fine tuning existing ones, expanding into new markets, etc. "
- Customer reminders: "Contact customers with service reminders and periodic reminder messages."

Inbound- "Inbound call center services deal with calls made by the consumer to obtain information, report a problem, or request for assistance. For inbound services, the subscriber typically provides a toll-free number. "

Customer Service- "An integral part of a company's value proposition, these involve activities that enhance your customer's level of satisfaction, with the aim of going beyond

their expectations. Some services offered are: Customer acquisition and retention, Tech Support, Sales, Appointment Settings, Third Party Verification, and Reservations." [35]

BPO- "Business Process Outsourcing (BPO) is the contracting of a specific business task, such as payroll, to a third-party service provider. Usually, BPO is implemented as a cost-saving measure for tasks that a company requires but does not depend upon to maintain their position in the marketplace. BPO is often divided into two categories: back office outsourcing which includes internal business functions such as billing or purchasing, and front office outsourcing which includes customer-related services such as marketing or tech support. Some services include: Software Development, Fulfillment, Order processing, online education support, Monitoring, Translation services." [31]

13 Appendix

13.1 Business Impact Analysis Guide for Contact Centers

Business Impact Analysis Guide Contact Centers in the Dominican Republic

Priority Systems/Processes	**Power generation**
Priority	5
Unavailability Consequence	All systems will operate temporally with UPS and then with an alternative source of energy. Cost will increment during the period that alternative power will be used. All operations can stop.
Dependent Systems/Processes	All operations and systems
Financial Impact	Losses per minute of non productive time. Increase in operation costs due to backup energy. Business completely halted. No revenues are perceived per complete unavailable time.
Quality Impact	SLAs downgrade. Complete failure of service availability. Reputation damage with clients of the company and clients of our clients (customers).
Remediation Costs	Expenses of alternative power generators maintenance. Lease of secondary generators. Any applicable refund for customers. Power grid/General failures from the Energy Provider. Hurricane destruction of electricity poles. Backup power generators run out of fuel. UPSs backup time ends.
Potential Threats	Regular power blackouts. Power grid/General failures from the Energy Provider. Hurricane destruction of electricity poles. Alternative backup energy failure. Backup power generators run out of fuel. UPSs backup time ends.
Recovery strategy	Install more backup capacity, or in case of extreme power outage lease external generators.

Priority Systems/Processes	**Internet Connections/Voice and Data lines with ISP**
Priority	5
Unavailability Consequence	The communication with clients will be interrupted. SLAs will drop. Agents unable to work. The CC will be unreachable. The business stops.
Dependent Systems/Processes	Communication systems. Online and voice services. All Internet transactions.
Financial Impact	The downtime per station is traduced as a lost of revenue. In case of a total loss of communication the entire CC will stop receiving benefits.
Quality Impact	SLAs downgrade. Reputation damage and possible loss of clients.
Remediation Costs	Provide a backup line for internet and at least half of the numbers of voice lines. The CC should accept the prices of another provider.
Potential Threats	Provider's internal problems. Physical damage to the provider's line. Malfunction of CC's internal equipments (routers and PBX).
Recovery strategy	Install a backup line for voice and data or in case of having already a backup line, use that line for critical operations. This backup is preferable with another provider.

Priority Systems/Processes	**Predictive Dialer**
Priority	3
Unavailability Consequence	This equipment makes the calls automatically from the list of numbers provided; it filters the calls and then passes them to the agents, which makes this process efficient, error free and controlled. Without it agents would have to dial manually the numbers of the customers they are calling, errors can occur during the dialing process which can cause an extra call charge to an undesired number. Agent productivity will be reduced because of the time they loose

	when dialing and waiting for answers. Also if answering machines prompt it would represent time and minute loss. Fewer sales will be made.
Dependent Systems/Processes	Outbound processes.
Financial Impact	Fewer sales which turns in less profits for the company and the agent itself because they usually win a selling commission. Pay for error calls or answer calls by machines.
Quality Impact	Productivity for outbound agents is reduced because of manual dialing.
Remediation Costs	Extra technical support, hardware module repair.
Potential Threats	Hardware failure, errors in modifying configuration, in-house systems errors which communicate with the PD, errors in the lists provided to the Predictive Dialer or not providing it at all.
Recovery strategy	Technical support information available, access to the lists to provide to the agents for manual dialing, restore from backup configuration files, programmers available for in-house apps related.

Priority Systems/Processes	**PBX**
Priority	5
Unavailability Consequence	Without the PBX calls aren't managed and aren't distributed to agents or the other areas of the Company. If calls don’t arrive to proceed to give assistance to the customers they are not providing any services. This affects less when the Contact Center is more oriented to BPO but still. Most Call Centers offer inbound services, which receive calls or outbound services, where they make calls to sell. When calls aren't manage, no service is being offered to the customers of our clients and sales are not being made.
Dependent Systems/Processes	Inbound/Customer Services, Outbound/Sales, all calls

Financial Impact	For outbound it implies more losses because each call is a possible sale that is not being made. Services paid by hours result in less payment due to this unavailable time.
Quality Impact	SLAs downgrade because of service unavailability.
Remediation Costs	Extra technical support, hardware module repair.
Potential Threats	New configuration errors, Incompatible updates. Voltage problems. Module failures. Hardware failures.
Recovery strategy	Technical support information available. Module change and quick set up.

Priority Systems/Processes	**Interactive Voice Respond (IVR)**
Priority	2
Unavailability Consequence	This system interacts with calling customers to determine through a voice recorded menu the service needed by the clients. Without this automatic menu a person would have to include the function of a receptionist asking the customer what it needs and then manually transferring them to the correct queue of agents. This would result inefficient and productivity would be reduced significantly.
Dependent Systems/Processes	Inbound/Customer Services calls
Financial Impact	Minimum
Quality Impact	SLAs downgrade. Longer calls and wait time for customers
Remediation Costs	Extra technical support, hardware module repair
Potential Threats	New configuration errors, Incompatible updates. Voltage problems. Hardware/Module failures.
Recovery strategy	Technical support information available. Module change and quick set up. Restart equipment.

Priority Systems/Processes	Automatic Call Distribution (ACD)
Priority	4
Unavailability Consequence	This controls the flow of a call once entered in the PBX. Organizes depending on the number the customer called to which agents the call will be forward to. Without this organization, a customer would encounter a lot of delays in the system to be attended and a call would last long if it needs to be transferred multiple times.
Dependent Systems/Processes	Inbound/Customer Services Calls
Financial Impact	With customer dissatisfaction and a SLA downgrade, clients can reconsider their negotiations with the Contact Center
Quality Impact	Customer dissatisfaction, SLA downgrade. Bad handling system which turns in delay and longer service calls.
Remediation Costs	Equipment substitution or repair costs, extra technical support, module replacement.
Potential Threats	Bad configuration modifications, hardware/module failure.
Recovery strategy	Technical support information available. Module change and quick set up. Restart equipment.

Priority Systems/Processes	Computer Telephony Integration (CTI)
Priority	4
Unavailability Consequence	This system integrates the computer used by agents with the telephone system, and this by default makes a consolidation of the communication channels. It gives a heads-up of the customer calling and this information is collected as the caller passes by the IVR and ACD. Without it the agent would have to confirm this information, instead of automatically, by asking questions to the caller and this reduces efficient time, make calls longer and generate less agent availability. The system also provides statistics for admin staff, control of agent status, call controls for QA, reporting.

Dependent Systems/Processes	Inbound/Customer Service, Outbound/Sales, all calls
Financial Impact	With less efficiency SLA can downgrade and clients can reconsider their negotiations with the Contact Center
Quality Impact	Less agent availability because of poor call handled efficiency, SLA downgrade, less reporting and QA control, more difficult to have statistical information.
Remediation Costs	Equipment substitution or repair costs, extra technical support, module replacement.
Potential Threats	Bad configuration modifications, hardware/module failure.
Recovery strategy	Technical support information available. Module change and quick set up. Restart equipment.

Priority Systems/Processes	**Quality Assurance**
Priority	2
Unavailability Consequence	This process helps Contact Center stay in compliance with the clients requests in terms of quality. In QA, calls are monitor and feedback is provided to the agents to better their performance. Without this department quality can be affected.
Dependent Systems/Processes	All services offered by the CC must be reviewed.
Financial Impact	Minimum
Quality Impact	SLAs downgrade
Remediation Costs	Minimum
Potential Threats	Bad job monitoring the calls and screens. Problems with the Voice Recording systems. Problems with the hardware where the records are kept.
Recovery strategy	Search the records in the backup media.

Priority Systems/Processes	**Voice Recording**
Priority	3
Unavailability Consequence	These systems are the base for QA. The conditions of recording sometimes are requested by the clients, they determine the percentage of the calls that they want to be recorded. If required, it can affect the SLAs.
Dependent Systems/Processes	Outbound and inbound calls
Financial Impact	If any law suit occurs and the recording is requested and not found, big losses can occurred.
Quality Impact	SLAs downgrade
Remediation Costs	Backup measures needed
Potential Threats	Voltage problems, Hardware failures. No media drives available (tapes, CD-ROMs, hard drives, etc) where to record the conversations. Loss of data before it's stored in external media. Overwriting non backed up data.
Recovery strategy	Reuse old media storage drives and over write information that can be erased. Configure alternative recording system from the PC if VoIP is used.

Priority Systems/Processes	**Air Conditioning System for Datacenter**
Priority	4
Unavailability Consequence	To avoid overheating in a country like Dominican Republic where it's always summer and knowing the heat generation from servers and other equipment, this is an important consideration.
Dependent Systems/Processes	All equipment in the data center
Financial Impact	Equipment hardware failure due to overheating.
Quality Impact	The sum of any system that may be affected.
Remediation Costs	Equipment replacement or repair and air conditioning

	replacement, repair or maintenance.
Potential Threats	Voltage problems. Neglect cleaning and maintenance. Hardware failure.
Recovery strategy	Technician information available for quick repair. Parts replacement. Fans if needed.

Priority Systems/Processes	**Databases**
Priority	3
Unavailability Consequence	Not all data is kept in Fileservers. Most is kept in databases as well, a lot of the applications considered among the list and others. The business's critical information won't be available. Delay in normal operation.
Dependent Systems/Processes	Systems with data contained in databases
Financial Impact	Data inconsistencies may have much affect financially. The systems that extract data from databases won't be available and during this time service can't be offered.
Quality Impact	SLAs downgrade.
Remediation Costs	Restore from the latest backup available and accept all financial losses that this may bring.
Potential Threats	Hardware failures. Corrupted data. Human mistakes (DELETE, UPDATE, INSERT, ALTER)
Recovery strategy	Restore from backup media.

Priority Systems/Processes	**Storage/File Servers**
Priority	3
Unavailability Consequence	The agents can't access or modify information about customers. The business's critical information won't be available. Delay in normal operation.

Dependent Systems/Processes	Users' profiles. Users' data. Databases. Financial information.
Financial Impact	Administration information could produce inconsistencies that may have a huge effect financially.
Quality Impact	SLAs downgrade. Customer service will be degraded. Internal information and processes could use wrong information. Without all information available inconsistent data/service can be originate. Advance procedures could be based on this data and people could take more time to do as before with less information. Source unreliability affects people's state of mind.
Remediation Costs	In case of a network problem, the costs of reestablishing the connection. In case of a storage server's hardware failure, the cost of replacing the server. Restore from the latest backup available and accept all financial losses that this may bring.
Potential Threats	Unreachable due to network problems. Hardware or software problems. Database corrupted.
Recovery strategy	Recover the data from the backup tapes or mirror servers. Technical support in case of hardware or software failure.

Priority Systems/Processes	**Network Apps Servers**
Priority	3
Unavailability Consequence	Disorganization on the CC's network. Possible lack of connection for some or all of the users. Possible unavailability of data. Interruption of data based services such as Internet and VoIP.
Dependent Systems/Processes	DNS, DHCP, e-Mail, Databases, VoIP, Internet, Intranet, Policies Server, Storage Servers, IPS, Web Server
Financial Impact	Medium impact. Possible loss of access from the outside could lead to business unavailability

Quality Impact	Lower accessibility.
Remediation Costs	In case of server failure in terms of hardware or software, it would be the cost of repairing or replacing the server. The lost of potential clients during service downtime.
Potential Threats	Viruses, Trojans, Worms. Exploited vulnerabilities: SQL Injection, Denial of Services, and SPAM. Networking problems. Voltage problems. Wrong configuration changes.
Recovery strategy	Restart services/equipments in some cases. Use redundant equipments. Replace equipments.

Priority Systems/Processes	**Network Equipments (Routers, Switches)**
Priority	3
Unavailability Consequence	Any problem with the company's gateway to the exterior will produce to be unreachable from the outside. In the case of switches, it can result in fragments of the internal network to isolate from access and communication. In case switches for VoIP it’s even more critical because not only will an agent be without data access but also without voice.
Dependent Systems/Processes	Internet, all communications between computers and servers among themselves, between each other and through the outside
Financial Impact	Medium impact. Possible loss of access from the outside could lead to business unavailability
Quality Impact	SLAs downgrade and lower accessibility.
Remediation Costs	Spare network equipments. These equipments are costly and it's not possible to use another temporally in the case of a Switch because you may not share a switch being used in full capacity.
Potential Threats	Voltage problems. Overheating problems. Wrong configuration changes.
Recovery strategy	Redundant equipments available or quick purchase to partner equipment providers/sellers. Restore from previous and healthy configuration backups.

Priority Systems/Processes	**VPN**
Priority	2
Unavailability Consequence	When VPN is used for directly accessing systems o general communications between the Contact Center and the client's site, this causes a direct impact over the client. No access can be provided and no service can be offered related to these systems. In case of VPN access for remote support it make more difficult their job having them to physically access the site to resolve any problem instead of assisting in a quick matter.
Dependent Systems/Processes	All systems acceded via VPN. All support given via VPN
Financial Impact	To access a System, the impact could be low depending how critical this access is.
Quality Impact	SLAs downgrade. Lost of reputation with the client. Less flexibility and major window of time for the remote support and resolution of a problem.
Remediation Costs	Purchase equipment if it was a hardware problem. Telephonic assistance or more expensive support.
Potential Threats	Wrong configuration changes. Voltage problems. External attacks.
Recovery strategy	Take advantage of any VPN feature that may have some other network equipment and configure for temporary access. Change the equipment if damage. Verify configuration changes in both endpoint equipments if it's site to site and if necessary, restore from backup configurations files.

Priority Systems/Processes	**Computers and Telephones**
Priority	2
Unavailability Consequence	Agents that aren't working produce SLA downgrade, because

	long queues supersede the maximum waiting time of a customer and this is an important parameter in SLA. It depends on their functions but usually they need the telephone, the computer or both to complete their jobs, and not having it available implies proving less service to the customers of our clients.
Dependent Systems/Processes	All the types of services offer by the Contact Center: sales, customer service, BPO, etc. All departments depend on it: finance, IT, administration and upper management, quality assurance, HR.
Financial Impact	In the case of outbound if an agent can't make a call to sell, there isn't any money produced. Inbound charges per hour, so the less mount of agents are connected the less the company is paid by their clients.
Quality Impact	SLAs downgrade. Unproductive time during the day.
Remediation Costs	Spare computers and telephones. Quick Help Desk technicians.
Potential Threats	General malware: viruses, Trojans, worms. Hardware failure. Voltage problems. Bad physical conditions that might affect the equipment. Port issues.
Recovery strategy	Have spare computers clone and ready to deploy using cloning techniques. Have spare telephones available.

Priority Systems/Processes	**Ticket System (Help Desk)**
Priority	1
Unavailability Consequence	Can turn problem management more problematic, less efficient and with delays.
Dependent Systems/Processes	Problem statistics and management. SLA measures.
Financial Impact	Minimum
Quality Impact	SLAs downgrade for Help Desk

Remediation Costs	Programmer extra time, if in-house; other would be new license of technical support.
Potential Threats	Hardware of Software issues in appliance. Bug fixed needed.
Probability	5%
Recovery strategy	Restore from backup system (comfit and database)

Priority Systems/Processes	**E-mail Apps**
Priority	1
Unavailability Consequence	Management, customer and client communication is done through e-mail, without it communication channels are reduced.
Dependent Systems/Processes	back office services and, internal and external communication
Financial Impact	Minimum
Quality Impact	Reduced communication channels
Remediation Costs	If a hardware problem the cost of repair or replacement.
Potential Threats	New configuration errors, Incompatible updates. Voltage problems, Hardware failures. Black list blocked, SPAM.
Recovery strategy	Acquire an anti-Spam solution; if marked as black list clear the mistake; hardware problems: make restore.

Priority Systems/Processes	**Customs Apps**
Priority	2
Unavailability Consequence	Most custom applications are to compliment operations with other software. Unavailable services can result in less efficient methods.
Dependent Systems/Processes	General services

Financial Impact	Depending on specific apps
Quality Impact	SLAs downgrade.
Remediation Costs	Minimum
Potential Threats	New configuration errors, Incompatible updates. Voltage problems, Hardware failures. Programming errors and changes.
Recovery strategy	Recheck the changes made and in last instance, undo changes. Make restore.

13.2 Report of Hurricanes and Catastrophic Tropical Storms that have passed near or over the Dominican Republic in the last 100 years (1909-2009)

Report of Hurricanes and Catastrophic Tropical Storms that have passed near or over the Dominican Republic in the last 100 years (1909-2009)

The principal source for the following report is AccuWeather[1], a weather authority in the United States that keeps records and tracks of the manifestations of Mother Nature. They keep an historical database of storm activity in all basins in their Hurricane Center. It was also used as reference the National Hurricane Center[2] and Storm Pulse[3].

In this report besides mentioning hurricanes that have passed over the island, which are the more devastating, it's also included hurricanes that passed near the island and some very dangerous tropical storms, as the winds and torrential rain produced by these can also affect the country and cause catastrophes. When the term "passed" is used it's referring to the route of the eye of the hurricane, the passing of the eye is dangerous as surrounding this hole in the middle of a storm are the stronger winds produced by the circular movement. Inside the eye everything is calmed, but only for a period of time because afterwards the winds will strike back with high intensity and it's dangerous as it creates a false alarm that things are over. From the eye wall to the total diameter of the hurricane, the effects are strong winds and torrential rains. This is why even if the eye does or doesn't make a landfall, it can still affect a small island like the Dominican Republic. The following images are for better understanding of what has been exposed in the previous lines; these are satellite pictures of hurricanes near or over the island extracted from the NASA website[4]:

[1] http://www.accuweather.com/

[2] http://www.nhc.noaa.gov/

[3] http://www.stormpulse.com/

[4] http://www.nasa.gov/

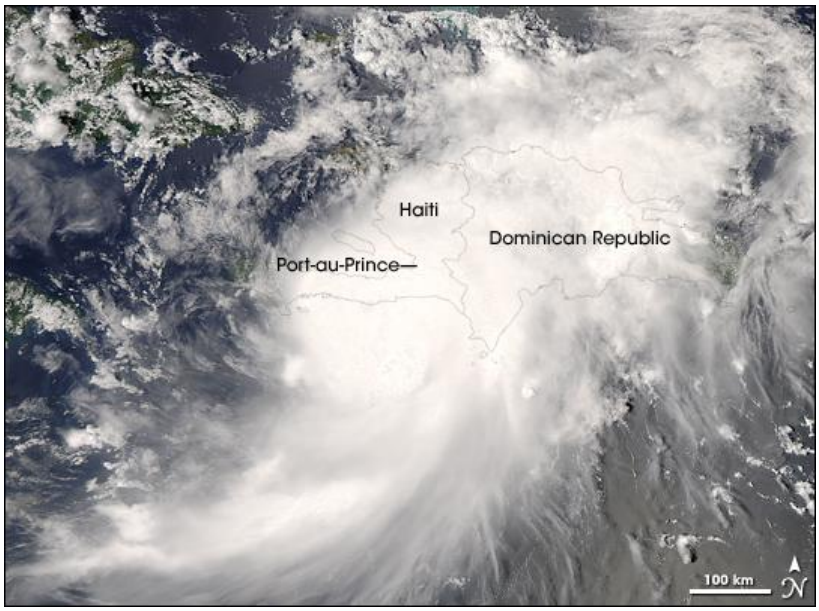
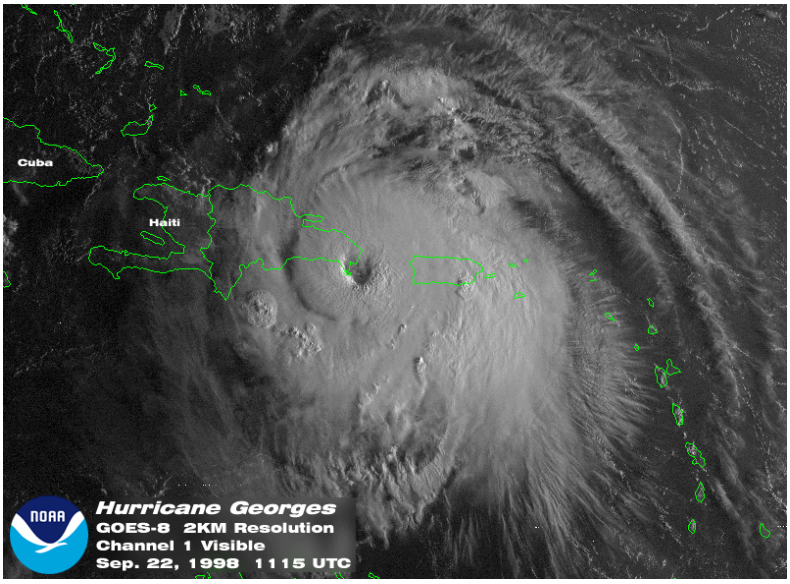
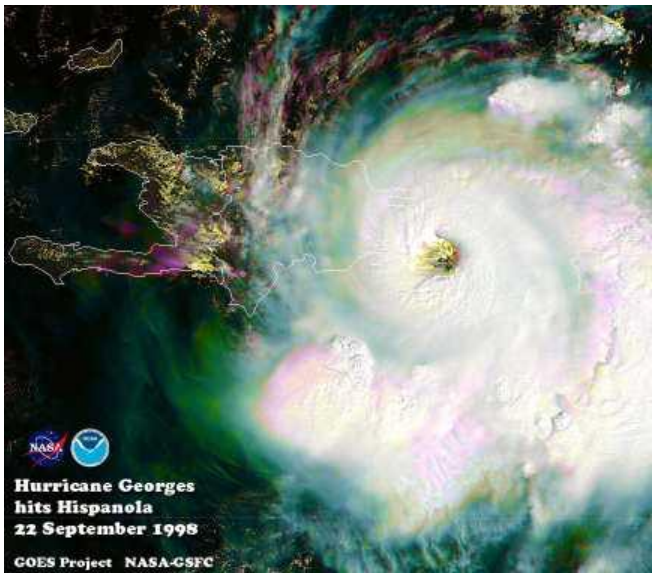


Figure1. Hurricane Gustav in 2008 over the Dominican Republic as a Category One Hurricane.



Figures 2. Hurricane Georges in 1998 making a landfall on the southeast part of the island.



Figures 3. Hurricane Georges in 1998 making a landfall on the southeast part of the island.

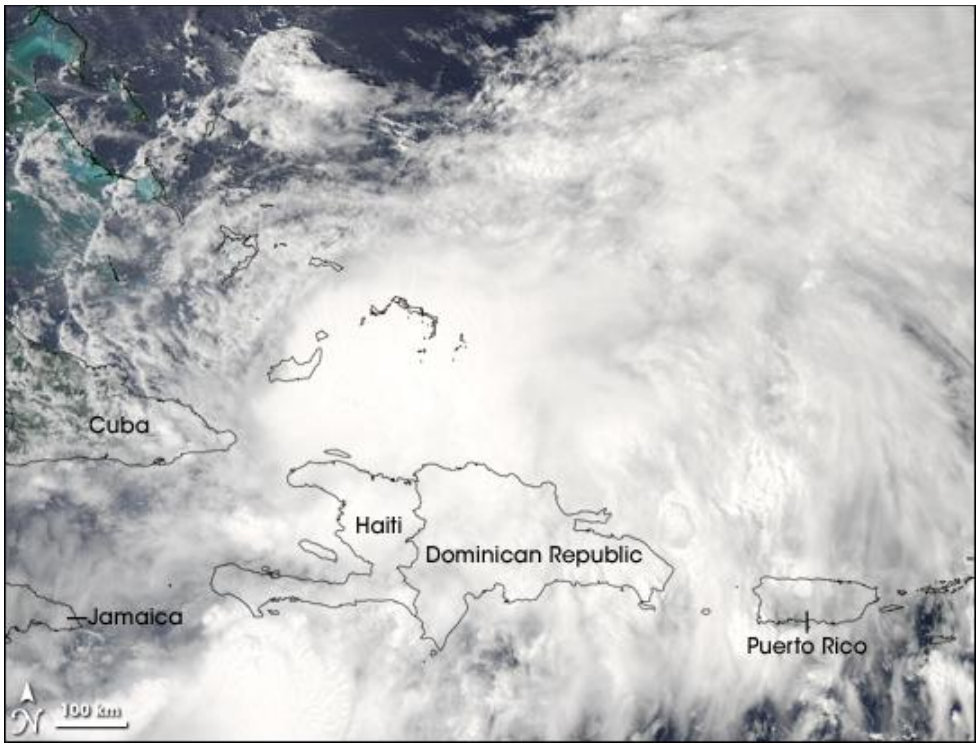


Figure4. Tropical Storm Hanna in 2008 on the north of the island.

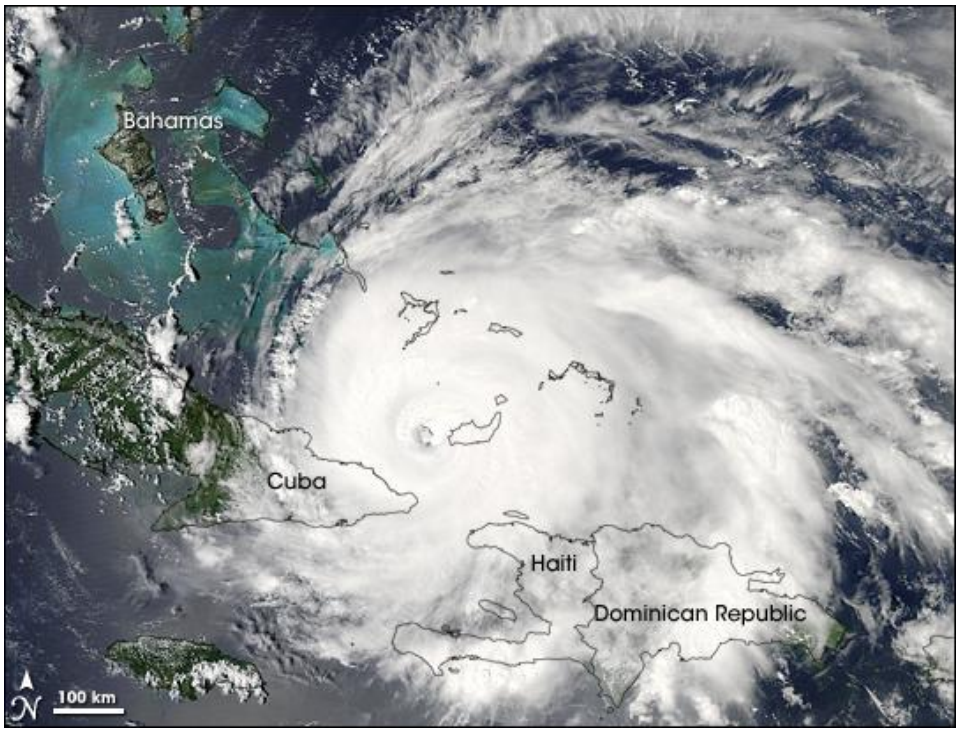


Figure5. Hurricane Ike in 2008 after passing by the north of the island and heading to Cuba.

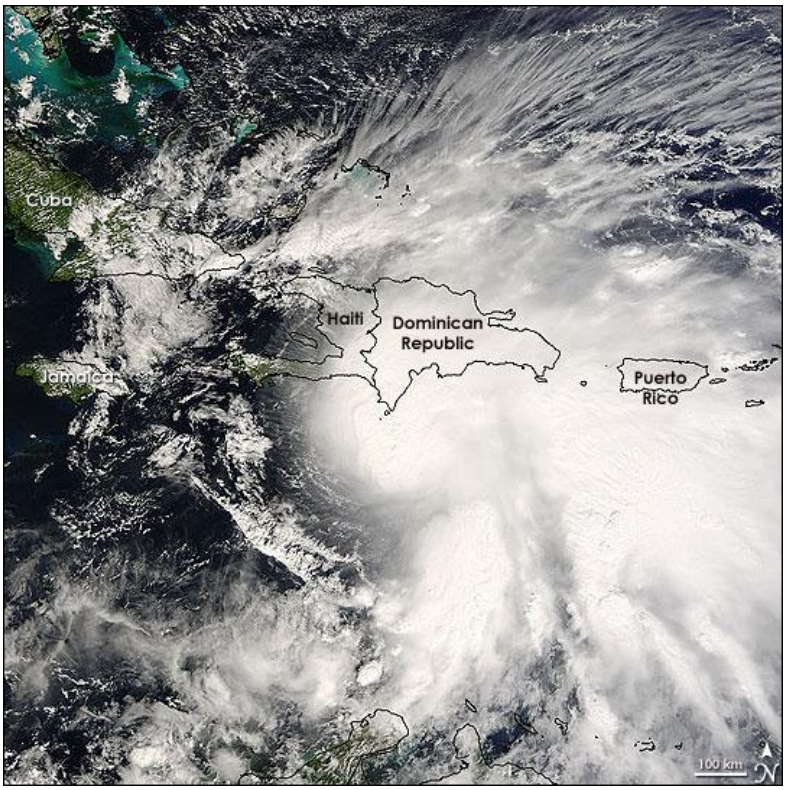


Figure6. Hurricane Noel in 2007 passing south of the island.

Until 1953, hurricanes were officially identified by the sequence of occurrence, nevertheless, people named hurricanes depending on the place of mayor impact or the Saint of that day. After 1953, the National Weather Service started the practice of naming the storms only with female names but in 1979, they began assigning both male and female names. There is a list used to name the hurricanes and these are rotated every six years, but when a hurricane has caused catastrophic damages it name is removed from the list.

The category of a hurricane is determined by the speed that the wind it's able to gain in its circulating movement. The Saffir-Simpson scale is used for hurricanes and it categorizes a storm depending on the intensity of the wind from 1 to 5.

Category one is when winds go from 74 to 95 mph; Category Two with winds from 96 to 110 mph; Category Three from 111 to 130 mph; Category Four from 131 to 155 mph and Category Five are winds greater than 156 mph.

This report will be composed of information tables for each storm, detailing: the date it passed over or near the island, the official name of the storm, the category of the storm when it passed over or near the island, its average wind speed over Dominican territory, the provinces were the center of the storm passed, an image of the territory showing the route track by the storm and the category every certain distance and finally casualties and damages resulted.

20th Century

Date	August 23, 1909
Name	Hurricane #6
Category over/near the island	One
Wind Speed	81 mph
Provinces where eye passed	Peravia, Azua, Baoruco
Route	
Casualty and Damages	No information found.

Date	September 7, 1910
Name	Hurricane #3
Category over/near the island	One
Wind Speed	80 mph
Provinces where eye passed	Pedernales
Route	
Casualty and Damages	No information found.

Date	August 12, 1915
Name	Hurricane #2
Category over/near the island	Two
Wind Speed	103 mph
Provinces where eye passed	None. Passed south of the island
Route	
Casualty and Damages	No information found.

Date	August 22, 1916
Name	Hurricane #5
Category over/near the island	One
Wind Speed	75 mph
Provinces where eye passed	It entered as Hurricane category One in La Altagracia and then turned into a Tropical Storm in the center of the island making a diagonal cross passing by Monte Plata, La Vega, Santiago and exiting through Dajabon to Haiti.
Route	
Casualty and Damages	No information found.

Date	September 10, 1921
Name	Hurricane #3
Category over/near the island	2
Wind Speed	98 mph
Provinces where eye passed	Juan Dolio, Boca Chica, Santo Domingo; Hato Mayor; Las Terrenas, Samana
Route	
Casualty and Damages	No information found.

Date	July 24, 1926
Name	Hurricane #1 (Popular name: Nassau)
Category over/near the island	One
Wind Speed	95 mph
Provinces where eye passed	Hurricane did not make landfall in the island. It passed northeast-north over Bavaro as a category One but when it passed Samana it was already category Two.
Route	
Casualty and Damages	According to the Monthly Weather Review of July 1926 issued by the National Hurricane Center of the National Oceanic and Atmospheric Administration the losses in eastern Santo Domingo the damages were of US$ 3,000,000. [36]

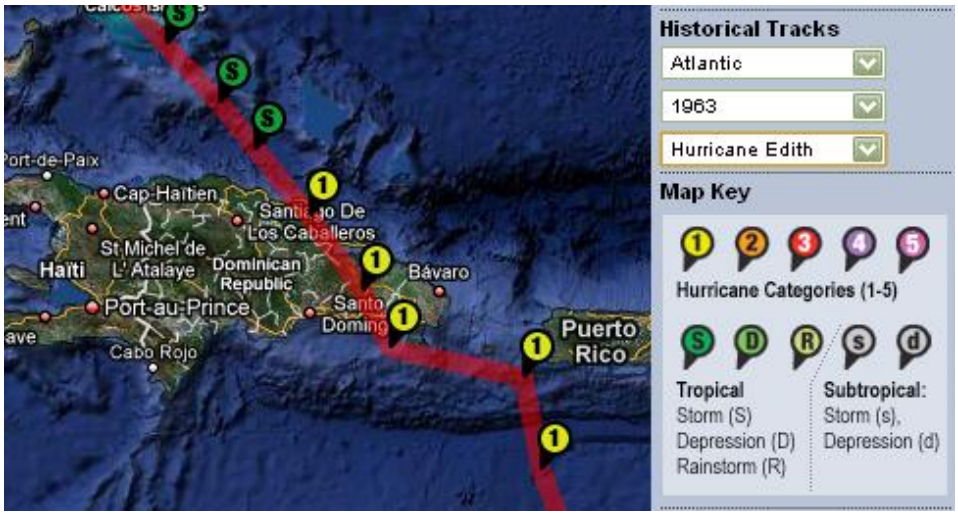
Date	September 14, 1928
Name	Hurricane #4 (Popular name: Okeechobee)
Category over/near the island	Four
Wind Speed	155 mph
Provinces where eye passed	No landfall on the island. The hurricane passed north and northeast of the island as category 4 hurricane.
Route	
Casualty and Damages	No information found.

Date	September 3, 1930
Name	Hurricane #2 (Popular name: San Zenon)
Category over/near the island	Four
Wind Speed	150 mph
Provinces where eye passed	Distrito Nacional, Santo Domingo; San Cristobal; San José de Ocoa; San Juan. Thanks to the mountains of the Dominican terrain the hurricane was weakened to a Tropical Storm, it exits through Elias Pina.
Route	
Casualty and Damages	This hurricane is known as the fifth deadliest of the Atlantic basin. It caused mayor destruction of the capital city, 20 miles wide of destruction. The airport was blown away. The rainfall flooded the Ozama River which inundated more the city. There is no official number of the deaths, from the estimation some sources state 2000 deaths while others up to 8000. The winds downed all communications inside of the city, trees were uprooted and crops destroyed. [37] It passed 5 hours and a half since it struck Santo Domingo as a category 4 hurricane and then weakened to a Tropical Storm and during those hours it destroyed houses, the communication systems were totally disrupted, bridges were wrecked and roads turned impassable. Telegraph lines simply vanished. The district of Nueva Villa, Duarte and San Carlos were complete destroyed. [38]

Date	September 27, 1932
Name	Hurricane #7 (Popular name: San Ciprian)
Category over/near the island	One
Wind Speed	92 mph
Provinces where eye passed	Isla Saona which belongs to the Dominican Republic. But it didn't make a landfall in the island it passed south and when it reached Barahona it was already a Tropical Storm.
Route	
Casualty and Damages	There were high wind and heavy rain but the damage was limited to crops. There were no fatalities. [39]

Date	September 22, 1949
Name	Hurricane #9
Category over/near the island	One
Wind Speed	75 mph
Provinces where eye passed	It made a landfall on San Cristobal as a category 1, and then passed over Azua, Baoruco but by the time it exited through Independencia it weakened to a Tropical Storm.
Route	
Casualty and Damages	15 lives were lost and the damages sum up to $12,000. [40]

Date	October 17, 1955
Name	Hurricane Katie
Category over/near the island	It approached to the island as a hurricane category Three but on landfall it turned into a Tropical Storm.
Wind Speed	115 mph while approaching the island and then it decrease to 69 mph on landfall
Provinces where eye passed	Pedernales, Independencia, San Juan, Santiago Rodriguez and it exited through Puerto Plata.
Route	
Casualty and Damages	Pedernales was badly damaged because of the high winds of hurricanes while it was approaching the shore. There were 7 deaths and an estimated damage of $200,000. [41]

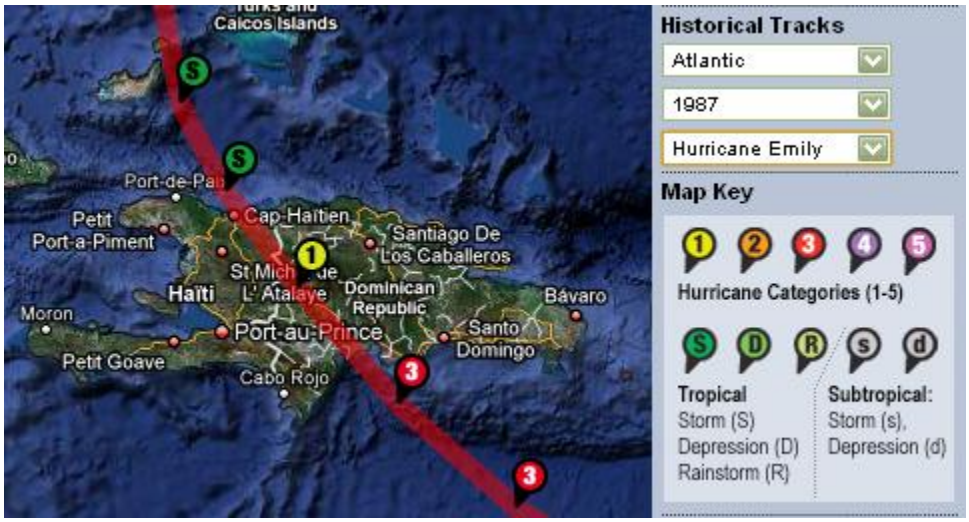
Date	September 27, 1963
Name	Edith
Category over/near the island	One
Wind Speed	75 mph
Provinces where eye passed	San Pedro de Macorís, Hato Mayor, Samana
Route	
Casualty and Damages	According to the Monthly Report the damage was minor but the strong winds and the heavy rain, caused $400,000 damage. [42]

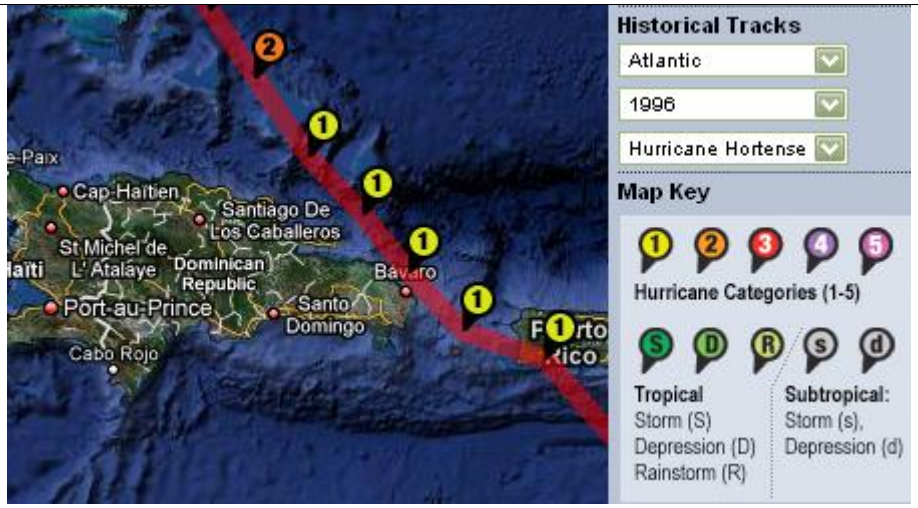
Date	September 29, 1966
Name	Hurricane Inez
Category over/near the island	Four
Wind Speed	138 mph
Provinces where eye passed	Pedernales
Route	
Casualty and Damages	Crop damages, which affect the economy. The town of Oviedo in Pedernales was totally destroyed there were 100 deaths. [43]

Date	September 11, 1967
Name	Hurricane Beulah
Category over/near the island	One
Wind Speed	86 mph
Provinces where eye passed	Pedernales
Route	
Casualty and Damages	Two lives were lost and because of the high winds and the torrential rains wreaking havoc among the sugar cane and coffee crops. [44]

Date	September 17, 1975
Name	Hurricane Eloise
Category over/near the island	It approach the island as a category 4 hurricane and near shore it turn into a Tropical Storm
Wind Speed	69 mph
Provinces where eye passed	Puerto Plata, Monte Cristi
Route	
Casualty and Damages	Torrential rains and winds. Communications were cut off; the electricity company cut all power off fearing for electrocutions because of numerous wires fell. Telephone service was sporadic. [45]

Date	August 31, 1979
Name	Hurricane David
Category over/near the island	Five
Wind Speed	173 mph
Provinces where eye passed	San Cristobal, Monsenor Nouel, La Vega, San Juan and exited though Elias Pina as a Category Three Hurricane.
Route	
Casualty and Damages	It caused torrential rainfall, resulting in extreme river flooding; roads were damaged or destroyed especially in Jarabacoa, San Cristobal and Bani. Over 2000 deaths because of river floods. A church and a school used as shelter were swept away in Padre las Casas. Damages exceed the 1 billion U.S. dollars and approximately 200,000 were left homeless. [46]

Date	September 22, 1987
Name	Hurricane Emily
Category over/near the island	Three
Wind Speed	121 mph
Provinces where eye passed	Impacted as a category 3 hurricane Azua; San Juan and then exited through Elias Pina as a category One
Route	
Casualty and Damages	The flooding cause widespread mudslides. Total deaths were 3. The damages were as high as US$25 million in the farming industry. 5000 people were forced to evacuate their homes. [47]

Date	September 10, 1996
Name	Hurricane Hortense
Category over/near the island	One
Wind Speed	75 mph
Provinces where eye passed	There was no landfall. It passed by the east and northeast coast of the island.
Route	
Casualty and Damages	There people died and 21 were reported missing. A school and church were destroyed as effect of the wind and tree falls, many houses were damaged and several electricity poles went down. Roads were blocked because of the excessive raining and storm surge. [48]

Date	September 22, 1998
Name	Hurricane Georges
Category over/near the island	Three
Wind Speed	121 mph
Provinces where eye passed	Bayahibe, La Altagracia, Juan Dolio, Santo Domingo, San Cristobal, La Vega, Azua, San Juan and exited through Elias Pina.
Route	
Casualty and Damages	It produced copious rains resulting deadly flash floods, mud slides and storm surge. 185,000 where left homeless and 100,000 people remained in shelters through mid October as electricity and water service remain out in most of the country. 380 deaths. [49] Various bridges were destroyed, 90% crops destroyed and estimated damages over $1 billion. [50]

21th Century

Entering the 20th century, things all spring around the changes of century, the end of the world, etc., but Mother Nature kept reacting to the changes of climatology and storms continued to form. In the year 2000, two storms were formed that passed near the island but that didn't caused mayor effects, there was Debby which turned from category One to Tropical Storm over the north of the island and then Helene, which passed south and was only a Tropical Storm with light effects.

Date	Augusto 23, 2000
Name	Hurricane Debby
Category over/near the island	It headed from Puerto Rico as a Category One, but it decreased to a Tropical Storm on its way here.
Wind Speed	69 mph
Provinces where eye passed	No landfall. Passed north of the island.
Route	
Casualty and Damages	The damages to the island were moderate to light; the major effect was storm surge and waves which caused some damages to the houses near shore, some others by damage by the wind gusts. [51]

The following years, 2001 and 2002, were good years since no storm passed too close to the island nor originated strong rains or effects. But in 2003, three Tropical Storms were near Dominican Republic; the ninth storm that was formed only was a Tropical Depression, that's

why it has no name, and it disintegrated on the south of the island. Then there was Mindy, a Tropical Storm that was originated on the east of the island and then passed northeast. And the last one was Odette that crossed diagonally from the southwest to the north center of the Dominican Republic.

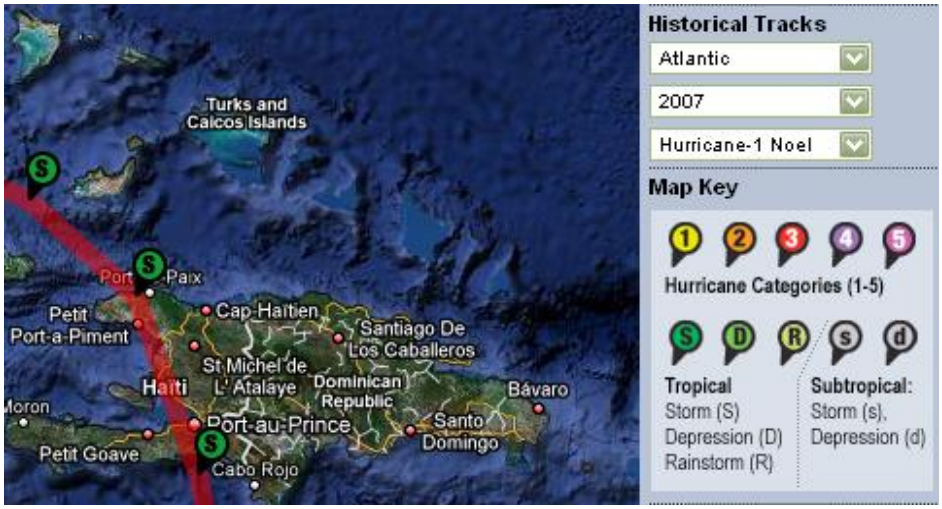
Date	December 06, 2003
Name	Hurricane Odette
Category over/near the island	Tropical Storm. This is the first storm record in December.
Wind Speed	52 mph
Provinces where eye passed	Pedernales, Barahona, Azuza, La Vega, Hermanas Mirabal, Espaillat.
Route	
Casualty and Damages	In total 8 life were lost and 14 injured most from the mud slides and the flash floods. Various trees were uprooted and downed. Power lines fell and there were damaged to buildings, bridges and large areas of agriculture. [52]

In the year 2004 one hurricane category one passed over the shore of the island from the east to the north, making several landfalls.

Date	September 16, 2004
Name	Hurricane Jeanne
Category over/near the island	One
Wind Speed	81 mph
Provinces where eye passed	It entered as a category One hurricane over Punta Cana, La Romana, El Seibo, by the time it reached Samana it turned into a Tropical Storm, Nagua, Moca, and Puerto Plata.
Route	
Casualty and Damages	Torrential rains and tropical storms force winds across the island. [53]

In 2005 only one Tropical Storm passed the island, Alpha, and then 2006 was a light season as no storm neither got too near the island nor passed over it. The year 2007 wasn't as calm, it had the Hurricane Dean that passed south of the island as a category Four hurricane producing intensive rain and winds on the south and also Hurricane Noel that made landfall on Haiti still as a Tropical Strom producing vast rain on the whole west side. Rarely in December a Tropical Storm was formed were called Olga, which passed the island from east to west and the effects big since the floor was saturated of rain from the previous storm a month ago.

Date	August 18, 2007
Name	Hurricane Dean
Category over/near the island	Four
Wind Speed	144 mph
Provinces where eye passed	No landfall. It passed south of the island.
Route	
Casualty and Damages	Heavy rain, streets flooded, rough waves and 6 deaths. Media reported the destruction of some poor homes. [54]

Date	October 29, 2007
Name	Hurricane Noel
Category over/near the island	Tropical Storm
Wind Speed	52 mph
Provinces where eye passed	No direct landfall over Dominican Republic. It made landfall in Haiti, on the west of the Dominican Republic.
Route	
Casualty and Damages	Torrential rains produced loss of life, 87 totals in Dominican Republic. 78,000 people were in shelters over two weeks, 15,000 home were damage, 6,000 destroyed. Mudslides and floods also washed away several bridges. The losses reported were of $77.7 million. [55] For two hours the entire island was without power and two days later, one third of the island remained without electricity. [56]

Date	December 11, 2007
Name	Tropical Storm Olga
Category over/near the island	Tropical Storm
Wind Speed	57 mph
Provinces where eye passed	La Altagracia, El Seibo, Hato Mayor, Monte Plata, Monsenor Nouel, La Vega, Santiago, San Juan and exited through Elias Pina.
Route	
Casualty and Damages	One of the reasons these Tropical Storm was so dangerous was because a month ago the island was impacted by Noel and the ground was still saturated by the rain. It was also out of season. It caused torrential rainfall, mudslides and flooding of the Yaque River, 22 deaths, 12,000 homes damage, of these 370 destroyed. [57] A deadly side effect was that the authorities release the flood gates of the Tavera dam in Santiago and that caused major damage.

2008 was a very active hurricane season and despite the fact that no hurricane made a landfall in Dominican Republic the rains and winds caused floods that damage great parts of the island. There was Tropical Storm Fay in August 15, then Hurricane Gustav in August 26, followed by Hurricane Hanna in September 3 and last Hurricane Ike that passed north of the island on September 6.

Date	August 15, 2008
Name	Tropical Strom Fay
Category over/near the island	Tropical Storm
Wind Speed	46 mph
Provinces where eye passed	Santo Domingo, Azua, San Juan, Elias Pina
Route	
Casualty and Damages	This storm officially formed over the Dominican Republic and it prepared the terrain to worsen the effects of posterior storms that passed by later that year. Damage was primary caused by rainfall-induced floods that affected residential structure. There was reported 2400 affected or destroyed homes because of the wind and flood water. Five deaths in Dominican Republic. [58]

Date	August 26, 2008
Name	Hurricane Gustav
Category over/near the island	One
Wind Speed	86 mph
Provinces where eye passed	No landfall on the island. It landed on Haiti, on the west side of the Dominican Republic.
Route	
Casualty and Damages	Eight people died in a mudslide triggered by heavy rain in Santo Domingo, two ladies died after rocks fell over their house the six children were drag to the river on the side of the road. [59] [60] Gustav caused significant property damages, but no monetary damage figures are available.

The year 2009 was a light year in general, the amount of storms formed was less than usual and none of the few affected the Dominican Republic.

Conclusions

The Atlantic basin is very active and as an island in the Caribbean the odds of not being affected by hurricanes exist in a minor way. The effects of hurricanes used to be more dangerous before because people weren't well educated on what to do during the past of a hurricane and edifications used to be weaker.

About the effect of Hurricanes in the Dominican Republic it can be said that the mountain terrain of the island helps to diminish, up to some point, the intensity of these storms because the rotation speed and strength is reduced while passing those parts of the island. They weaken and decrease wind speed, though reducing category.

General effects due to hurricanes are the saturation of the ground that produces landfalls, also crops get damaged and because of this the economy is affected. Another effect is the overgrowth of the rivers and this affect the people that live near the shore of rivers and seas. The strength of a river can also affect bridges and leave communities excommunicated. Winds can be very dangerous affecting electricity/telecommunication poles and trees that may fall over properties, houses, roads, bridges.

The hurricane period for each year is from June to November, but statistically the month of major activity for the Dominican Republic is September, were 14 out of the 27 storms occurred in this month.

Over this analysis we can infer that against the hurricane threats that Dominican Republic is exposed to, regular backup decisions are sufficient because what they affect more aren't technology services but rather agriculture industry and poor constructed residences. There is still a percentage of opportunities that a storm can affect the telecommunications and electricity for what redundancy and backup must be considered.

14 Bibliography

[1] Terremark Worldwide Inc. (2007, May 2). *General Information: NAP del Caribe.* Retrieved March 2009, from Lacnic Documents: http://lacnic.net/documentos/naps/naps_del_caribe.pdf

[2] Terremark Worldwide, Inc. (2008, December 30). *Terremark - Investors - Press Release*. Retrieved March 2009, from Terremark.com/Investors: http://phx.corporate-ir.net/phoenix.zhtml?c=120545&p=irol-newsArticle&ID=1239728&highlight=

[3] Business Wire. (2007, March 27). *Telecommunications in the Dominican Republic is One of the Fastest Growing and Most Competitive Sectors of the Economy.* Retrieved March 2009, from BNET: http://findarticles.com/p/articles/mi_m0EIN/is_2007_March_27/ai_n18768132/

[4] Listín Diario. (2009, February 16). *ADOZONA News: Call centers para trabajar.* Retrieved March 31, 2009, from ADOZONA Website: http://www.adozona.org/esp/noticiasdet.asp?codid=1145

[5] El Nuevo Diario. (2006, April 21). *30 mil empleos aportarán empresas de Call Centers para 2007.* Retrieved March 31, 2009, from El Nuevo Diario Website: http://elnuevodiario.com.do/app/article.aspx?id=20827

[6] CEI-RD. (2008, April 24). *CEI-RD News: El CEI-RD busca impulsar sector de Call Center*. Retrieved March 31, 2009, from CEI-RD Website: http://www.cei-rd.gov.do/leer_noticia.asp?id=301

[7] Javier, J. (2008, May 13). *El Diario Libre: Call Centers generan 25 mil empleos directos en el país.* Retrieved March 31, 2009, from El Diario Libre Website: http://www.diariolibre.com/noticias_det.php?id=16069

[8] CEI-RD. (n.d.). *Investment Brochures: Invest in DR, Call Contact Centers.* Retrieved April 15, 2009, from CEI RD Website: http://www.cei-rd.gov.do/download/brochures/call-center.pdf

[9] Saleem, K., Deng, Y., Chen, S.-C., Hristidis, V., Li, T., & Luis, S. (2008). Towards a Business Continuity Information Network for Rapid Disaster Recovery. *The Proceedings of the 9th Annual International Digital Government Research Conference*, (pp. 107-116). Montreal.

[10] Landry, B., & Koger, S. (2006). Dispelling 10 Common Disaster Recovery Myths: Lessons Learned from Hurricane Katrina and other Disasters. *ACM Journel , 6* (4).

[11] DR1. (n.d.). *Weather: Hurricanes in the Dominican Republic*. Retrieved April 15, 2009, from DR1 Website: http://dr1.com/weather/hurricanes.shtml

[12] de Champeaux, D., Lea, D., & Faure, P. (1993). Chapter 13: Domain Analysis. In *Object-Oriented System Development.* Addison Wesley.

[13] Hooper, J. W., & Chester, R. O. (1991). *Software Reuse: Guidelines and Methods.* New york and London: Plenum press.

[14] DeBaud, J.-M., Moopen, B., & Rugaber, S. (1994). Domain Analysis and Reverse Engineering. *International Conference on Software Maintenance, 1994. Proceedings.* (pp. 326-355). Victoria,BC: IEEE.

[15] Oldfield, P. (2002). *AP-M.* Retrieved March 2009, from http://www.aptprocess.com: http://www.aptprocess.com/whitepapers/DomainModelling.pdf

[16] Answers Corporation. (n.d.). *Plate tectonics: Definitions from Answers.com*. Retrieved October 19, 2009, from Answers.com Web site: http://www.answers.com/topic/plate-tectonics

[17] Schiesser, R. (2002, Juanuary 11). *Steps to Developing an Effective Disaster-Recovery Process.* Retrieved February 15, 2010, from InformIT: IT Disaster at the Movie Studio: http://www.informit.com/articles/article.aspx?p=24909&seqNum=3

[18] Carl Bradbury, M. (2007, November 20). *Continuity Journal.* Retrieved February 18, 2010, from The IT Disaster Recovery Plan: http://www.continuitycentral.com/feature0524.htm

[19] Segura, R. (2008). Conference dictated about Energy in the Dominican Republic.

[20] Montan, F. (2003, October 20). *The energetic drama [El drama energetico].* Retrieved October 14, 2009, from Ahora Magazine: http://www.ahora.com.do/Edicion1328/SECCIONES/actualidad4.html

[21] Rosso, A. (2008, June 2). *La falta de Institucionalidad es causa de la crisis energetica.* Retrieved October 14, 2009, from Hoy Digital: http://www.hoy.com.do/economia/2008/6/2/92030/La-falta-de-institucionalidad-es-causa-de-la-crisis-energetica

[22] Hewitt Associates. (2007). *Dominican Republic Offshoring Attractiveness Strategy Report, Part 1.* Hewitt Associates.

[23] Encyclopedia Britannica. (2009). *Dominican Republic :: The land -- Britannica Online Encyclopedia.* Retrieved October 14, 2009, from Britannica Online Encyclopedia: http://www.britannica.com/EBchecked/topic/168728/Dominican-Republic/54427/The-land

[24] Franklin, J. L. (2008). *Tropical Cyclone Report Hurricane Dean.* National Hurricane Center.

[25] Geological Society of America. (1999). Penrose Conference: Margenes de Placas Tectónicas en Transición de Subducción a Fallamiento Transcurrente. *Dominican Republic.* Puerto Plata: Asociación Dominicana de Mitigación de Desastres.

[26] O'Reilly Pérez M. Sc, H. (2002). *¿Es posible que ocurra un sismo catastrofico en Republica Dominicana?* Santo Domingo: Presidente de SODOSISMICA.

[27] Dominican Today. (2009, February 26). *11 Dominicans nabbed so far in US$100M Internal Revenue fraud.* Retrieved February 15, 2010, from Dominican Today: http://www.dominicantoday.com/dr/local/2009/2/26/31219/11-Dominicans-nabbed-so-far-in-US100M-Internal-Revenue-fraud

[28] Diario Libre. (2010). El pais cuenta con plan de contingencia para terremotos. *Diario Libre* , 8.

[29] Morreale, T. (2008, May 12). Incident Handling for SMEs. *SANS-InfoSec Reading Room* . SANS Institute.

[30] SANS Institute. (n.d.). *Sans Institute Best Practices*. Retrieved 03 01, 2010, from SANS InfoSec Reading Room - Best Practices: http://www.sans.org/reading_room/whitepapers/bestprac/

[31] WhatIs. (2009). *SearchSecurity: Security Glossary*. Retrieved April 15, 2009, from TechTarget Corporate Website: http://searchsecurity.techtarget.com/glossary/0,294242,sid14,00.html

[32] Indotel. (2009). *About us: Indotel*. Retrieved April 15, 2009, from Indotel Website: http://www.indotel.gob.do/conoce-al-indotel/

[33] CEI-RD. (2009). *About us: CEI-RD*. Retrieved April 15, 2009, from CEI-RD Website: http://www.cei-rd.gov.do/index.asp

[34] Contact Center Association. (n.d.). *About us: Contact Center Association*. Retrieved April 15, 2009, from Contact Center Association Website: http://acc-rd.org/

[35] PNI Call Center. (2008). *Services*. Retrieved December 1, 2009, from Inbound Offshore Contactl Center: http://www.pnicallcenter.com/inbound-call-center.html

[36] National Hurricane Center. (1926). *Monthly Weather Review.* http://docs.lib.noaa.gov/rescue/mwr/054/mwr-054-07-0312.pdf: National Oceanic and Atmospheric Administration.

[37] Hartwell, E. (1930). *The Santo Domingo Hurricane of September 1 to 5, 1930.* San Juan, Puerto Rico: Weather Bureau .

[38] The Associated Press. (1930, September 4). Hurricane takes tremendous toll in Island City. *Sheboygan Journal* , p. 23.

[39] The Lowell Newspaper. (1932, September 29). Storm heading for island of Jamaica. *Lowell Sun* , p. 32.

[40] Zoch, R. T. (1949). *North Atlantic Hurricanes and Tropical Disturbances of 1949.* Washington, D.C.: Weather Bureau.

[41] Dunn, G., Davis, W., & Moore, P. (1955). *Hurricanes of 1955.* Miami: Weather Bureau Office.

[42] Dunn, G. (1963). *The hurricane season of 1963.* Miami: U.S. Weather Bureau Office.

[43] History. (1966, September 24). *Hurricane Inez batters Carribean*. Retrieved December 12, 2009, from History Disaster: http://www.history.com/this-day-in-history.do?action=Article&id=50847

[44] National Oceanic and Atmospheric Administration. (1967). *Hurricane Beulah. Preliminary Report with Advisories and Bulletins Issued.* Silver Spring: Weather Bureau.

[45] Daily Capital News. (1975, September 18). Hurricane Eloise slams Dominican. *Daily Capital News* , p. 13.

[46] Hebert, P. (1979). *Atlantic Hurricane Season of 1979.* Miami: National Hurrican Center.

[47] Case, R., & Gerrish, H. (1988). *Annual Summary Altlantic Hurricane Season of 1987.* Miami: National Hurricane Center.

[48] Avila, L. A. (1996). *Preliminary Report Hurricane Hortense.* Miami: Nationa Hurricane Center.

[49] Guiney, J. L. (1999). *Preliminary Report Hurricanes Georges.* Miami: National Hurricane Center.

[50] National Climate Data. (1999, April 12). *Georges Pummels Caribbean, Florida Keys, and U.S. Gulf Coast*. Retrieved December 13, 2009, from NCDC: Hurricane Georges - Satallite Images: http://lwf.ncdc.noaa.gov/oa/reports/georges/georges.html

[51] Pasch, R. J. (2000). *Tropical Cyclone Report.* Miami: National Hurricane Center.

[52] Franklin, J. L. (2003). *Tropical Cyclone Report Tropical Strom Odette.* Miami: Natioanl Hurricane Center.

[53] Lawrence, M. B., & Cobb, H. D. (2004). *Tropical Cyclone Report.* Miami: National Hurricane Center.

[54] Franklin, J. L. (2008). *tropical Cyclone Report Hurricane Dean.* Miami: National Hurricane Center.

[55] Brown, D. P. (2007). *Trpical Cyclone Report Hurricane Noel.* Miami: National Hurricane Center.

[56] Riddel, K., & Flinn, R. (2007, November 1). *Storm Noel Becomes Hurricane, Heads Away From Bahamas.* Retrieved December 13, 2009, from Bloomberg: http://www.bloomberg.com/apps/news?pid=20601086&sid=aczqilI1fiq4&refer=latin_america

[57] Mainelli, M. (2008). *Tropical Cyclone Report tropical Storm Olga.* Miami: National Hurricane Center.

[58] Stewart, S. R., & Beven II, J. L. (2009). *Tropical Cyclone Report Tropical Storm Fay.* Miami: National Hurricane Center.

[59] CNN. (2008, August 28). *Gustav blamed for 22 deaths as it batters the Carribean.* Retrieved December 13, 2009, from CNN World: http://www.cnn.com/2008/WORLD/weather/08/27/gustav/

[60] News paper 7 dias. (2008, August 27). *Aumenta a 23 el numero de muertos en Haiti y Rep. Dom. por "Gustav".* Retrieved December 13, 2009, from Periodico 7 dias: http://www.7dias.com.do/app/article.aspx?id=31078