LatinoInsurance

Contingency Plan

Contents

1. Introduction

This document provides an overview of the LatinoInsurance Contingency Plan and shows the strategies and actions used to ensure the viability and reliability of its technological infrastructure in the face of any kind of crisis, thus ensuring the adequate level of services it offers. your platform.

2. Evaluation

LatinoInsurance's Contingency Plan addresses classified threats through a process of identifying frequent incidents and adverse conditions that can generate significant impacts.

Among its objectives it includes the protection of the operational capacity of the services' technology platform and of protecting and responding successfully through mitigation activities.

The following threats have been identified:

- Public disturbances and / or violence in the Data Center.
- Massive absenteeism due to pandemics.
- Cybernetic Attacks.
- Fire Damage.
- Severe weather and natural disasters.
- Destruction of the Data Center Operating Platform Service.
- Terrorist attack.

According to the classification of the threat, the IT department will take the necessary measures for the immediate restoration of the services maintained by the technological platform.

3. Planning

The following activities have been defined::

- Weekly Backup of the Databases in the cloud and locally, which are synchronized immediately.

Data Base	Frequency	Backup Servers
Main Database Online	Weekly	Production Online Local Server
Logical Doc Database	Weekly	Production Online Local Server
Main Database - Backup Server	Weekly	Production Online Local Server

- Backup of the Source Code is done weekly both locally and online.

- Backup of key Financial Information files is done weekly both locally and online.

- Preventive maintenance of the Servers according to the Service Provider guidelines and planning.

4. Execution

In the event of a disaster and after carrying out the pertinent evaluations, the following actions will be carried out which will allow the service to be restored as quickly as possible

- Redirection to the Backup Server in the Cloud in case the Main Server fails (+/- 4 hours).

- If for any reason the two available servers fail (Main and Backup Servers), a new server will be set up with an available provider and all the services necessary to host the web application and its respective database (+/- 24 hours) will be enabled .

- Redirect web.latinoinsurance.com path to the IP of the new Server (+/- 4 hours in parallel with the setup of the new server).

- Restoration of the last database backup (+/- 8 hours).

- Installation of the Web Application and all of the services needed for the application to work at 100% (+/- 2 hours)

- Testing of the functionalities and data of the Web Application with the collaboration of the Financial Analysis department. (+/- 4 hours).

Threat Level	Action	Time
Low	1. Database update and Web Application restoration	+/- 8 horas
Medium	1. Main to Backup Server routing. 2. Database restoration 3. DNS routing	+/- 24 horas
High	1. Buy a new server 2. Database restoration and installation of Web Application. 3. DNS Routing 4. Web and Database testing	+/- 48 horas

5. Recovery

LatinoInsurance has a team of experienced professionals dedicated to responding to any threat, thus giving the possibility that all the services offered remain operational 100% after a disaster. The services will be restored in the shortest possible amount of time depending on the analysis carried out previously. .

Latinoinsurance has the necessary infrastructure so that in the case of any eventuality we can respond to our clients in the shortest possible time.