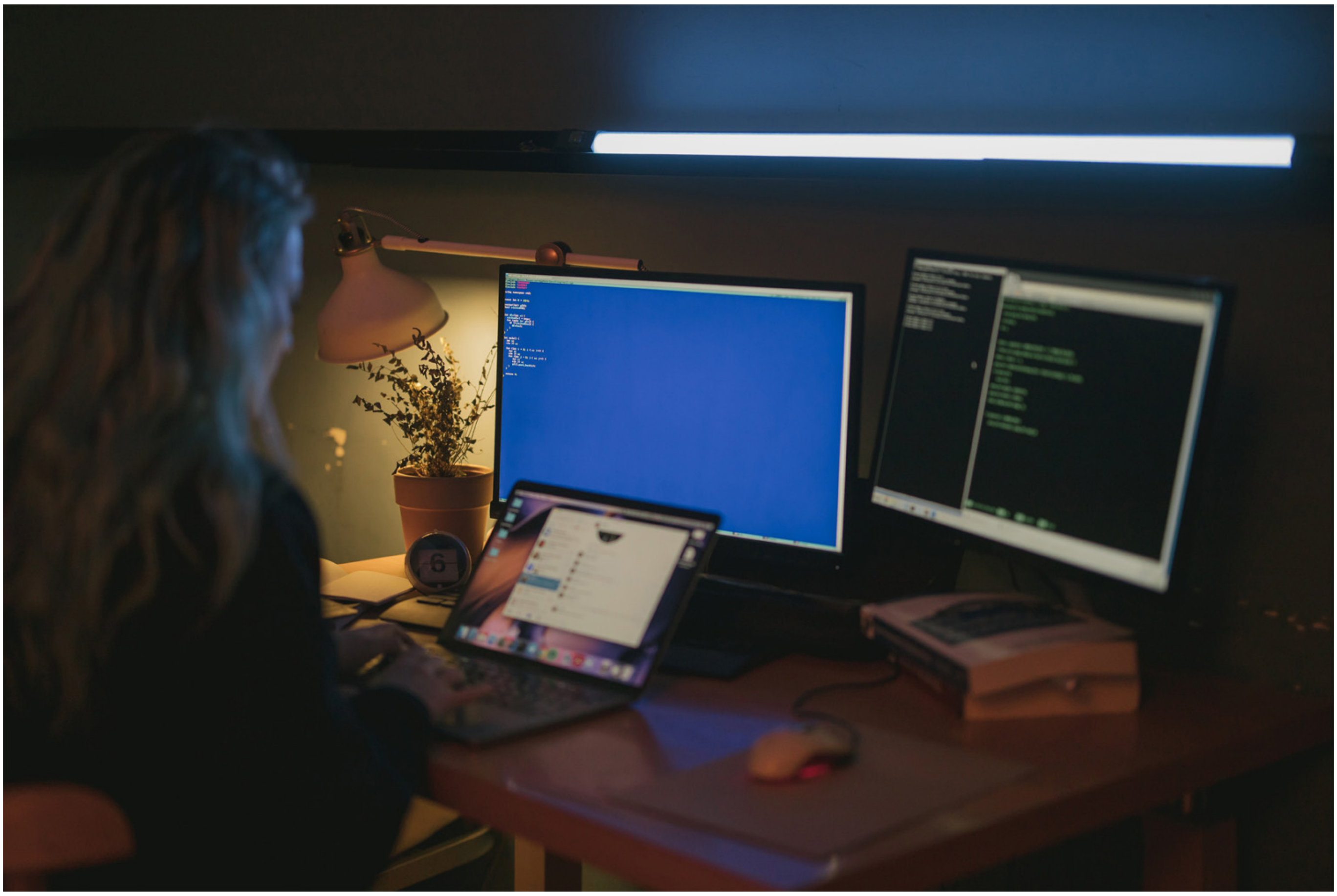
Given the publication of the LGPD and the large amount of data that companies have and handle, the existence of **data contingency plans** is of paramount importance.

In this sense, this text aims to structure and present adequate data contingency plans for your company, as well as the advantages of its use.

WHAT ARE DATA CONTINGENCY PLANS?



A data contingency plan is a set of detailed actions that will be implemented in the event of an unexpected event to reduce the impact and prevent data loss.

This plan has three elements, which are:

- Data backup plan
- Disaster recovery plan
- Emergency operation plan

Below, the main characteristics of each of these elements will be presented.

BACKUP OF DATA

The secure backup of all your data should be in a secure location such as a virtual data room (VDR).

Virtual storage media provide greater security for digital documents and limit access to only those authorized to view them.

They are used extensively for business transactions, including M&A, banking, and investment.

In this sense, interested parties can securely access documents at specific times, from any platform, and anywhere in the world with an internet connection.

In short, a VDR is used whenever someone needs to securely store information and make it available to a limited group of people.

In this way, your company will have reliable and accessible data backups at any time, and, in addition, with information from all departments of the company.

DISASTER RECOVERY

Once you've reviewed what it takes to make a **safe backup** and ensure your company's data is protected, it's time to plan exactly how to restore it in the event of a disaster.

Ideally, your critical data and systems should be identified and prioritized, such as sensitive personal data or confidential company information.

In that case, this data must be recovered first for its proper protection.

EMERGENCY OPERATION

Ultimately, this is where the two plans for data backup and disaster recovery come together.

In other words, the emergency operation consists of forming a general plan that allows the company to deal with attacks or data loss.

HOW DO CONTINGENCY PLANS OF CONFIGURATION OCCUR?

For configuration, each team member must have a specific task in case of an emergency.

In this sense, to guarantee the plan's success, all details must be explained, such as the order of restoration, who is responsible for each stage, and all the actors involved.

In addition to the configuration, you will need to set priorities for the order to restore systems and delegate which team members have the authority to view, change, recover and **restore data.**

Therefore, any changes to your business must be accounted for, such as new hardware, software, personnel changes, and new locations, among other factors.

These practices presented above will allow the plan to work better once well documented and regularly adopted, and data will be increasingly protected.

Generally speaking, these are the main points about **data contingency** plans. Keep following our blog and follow our Instagram for more content.