AGBI

ATIVOS REAIS

INTERNAL CONTROLS MANUAL

POLICIES & INTERNAL STANDARDS

BUSINESS CONTINUITY PLAN

General Principles - Objective

The purpose of this Business Continuity Plan (BCP) is to establish responsibilities, actions, and procedures to enable the recovery of the company's data, communication, and network environment in the event of an unexpected outage. The plan is structured to meet the following objectives:

a) Recover the structure of the physical network of the company within acceptable parameters (especially term) for the business and defined by this document;

b) Retrieve the applications and data used by the company within acceptable (especially term) parameters for the business and defined in this document;

c) Retrieve the company's communication structure within acceptable parameters (especially deadline) for the business and defined by this document; and

d) Mitigate business impact in terms of monetary losses and operational interference.

To achieve this goal, this document has been structured in three parts, namely:

1) Identification of the person responsible for the BCP and its responsibilities
2) Infrastructure planning and procedures to enable the BCP
3) Post-out recovery procedures in case of an unexpected event

Identification of Those Responsible for the Business Continuity Plan

The Business Continuity Plan is under the responsibility of the AGBI Executive Committee. Among its responsibilities are:

a) Promote communications and TI structure planning to enable rapid business re-establishment in the event of disruption or disaster

b) Contact with service providers to recover data and infrastructure;

c) Leadership with the AGBI Real Assets team to meet the procedures identified in this policy.

Infrastructure planning and procedures to enable the BCP

The effectiveness of the AGBI Business Continuity Plan depends not only on the guidelines outlined in this plan, but also in regard of the company's internal policies, in particular the Home Office Policy. In order to define a safe and easily recoverable environment, AGBI has put in place a data security policy, in addition to a policy for the use of IT and communication resources, which establish the procedures to be followed by its collaborators in relation to the company's information and its infrastructure, in addition to defining the necessary bases for business continuity in case of unscheduled interruptions or disasters. The procedures serve their purpose both for remote work (home office) and face-to-face and, consequently, facilitate the transition from one to the other without prejudice to the data, information security and productivity of the manager.

In addition, to enable a BCP that allows AGBI to protect its business information and re-establish working conditions efficiently and quickly after a partial or permanent interruption event, it was planned infrastructure and IT services to allow data and communication recovery in a brief period, either in the AGBI office or on a remote website.

A *Cold-site Contingency strategy was* adopted from which the company could move to an environment with minimal infrastructure and telecommunications resources and people operating from notebooks made available by the company. There is also a Home Office Policy that already provides for minimum procedures and requirements for the performance of company functions remotely without prejudice. In addition, a series of standard operating procedures (POP) have been established under the Home Office Policy to improve the quality of virtual communication, ranging from labeling on audio and video links to best practices in sending documents and files.

File Server: We have our database stored locally on two mirrored servers. The local back-up is done daily and can be recovered in few hours (a file can be recovered in few minutes) by the system administrator, and the remote backup can be recovered within a maximum of 24 hours after the request of the system administrator. In this way, in case there is disaster in our facilities we are fully able to continue activities in any other location immediately. Remote storage eliminates problems associated with natural events that could affect sites in the same location.

Email Server: AGBI has chosen to hire an enterprise-class cloud email server provided by Microsoft through its Office 365 E3 packages product. This service, in addition to relying on high availability with a 99.9% service time guarantee, benefits from Microsoft's datacenter infrastructure, server redundancy, *and enterprise-class compliance and* security policies. Because it is based on a cloud server, in case of impossibility of using the AGBI office, the service could be easily reestablished on a remote site through webmail or by configuring new computers for access to the server. In addition, several network redundancy storage procedures were adopted using the Microsoft OneDrive program, cloud file storage, to facilitate the remote operation of AGBI collaborators.

Communication: We use Vivo's corporate-level voice and data services, as well as redundancy of vivo's corporate data service and cellular lines for the team.

Given the profile of managed funds (few assets, investments in closed companies, typically 1-3 investments per year per fund, etc.), no elevated risk of lack of continuity for the business has been identified. The most important point in the event of a possible outage would be to restore the databases (containing the analysis and management information of the pipeline investments and invested assets of the funds, reports and management controls, etc.) and the basic infrastructure for day-to-day operation of a *fund focused on private equity* (computers / notebooks, basic telephony network and basic infrastructure to access data stored on servers and website).

Current Infrastructure of AGBI Real Assets

a) 7 HP desktop computers and two notebooks;

b) No break for power contingency for local computers;

c) Network infrastructure connected to Vivo's 100 mega link;

d) Telefonica's telephone network with ten individual lines and twenty extensions;

e) Remote servers with unlimited storage capacity increased as we need to incrementally. These servers back up the data of individual users daily and this data can be retrieved from any computer by accessing the internet through properly validated login and password;

f) Microsoft email system, containing security system and antivirus infrastructure. In addition, we have anti-virus systems on our individual computers;

g) Windows and Microsoft Office packages on your company’s computers, including Microsoft OneDrive.

Company Infrastructure and Services Recovery Procedures

AGBI has a simple and effective contingency and business continuity plan, to ensure that in case of any type of incident that makes it impossible to enter, travel to the company's office or that implies the evacuation of the site, all collaborators can continue their activities, following the following flow:

1. If there is any type of event that makes it impossible to access the office, it was established that Ms. Josefa and Ms. Dilaine, the first collaborators to arrive/attempt to access the office, contact Mr. Gustavo. If you need to evacuate the office, partners Gustavo and Luciano will take your notebooks and Mrs. Dilaine and Mr. Diogo will take the other two existing notebooks in the company to the contingency environment, if the situation allows you to go to transport, so that everyone can work quickly and follow in the best way performing their activities;

2. Upon receiving the incident alert or facing the evacuation situation, Mr. Gustavo will inform (Link/WhatsApp) collaborators who are not in the office to trigger the contingency plan;

3. Each collaborator will be informed about the time when he/she must move to the contingency environment and if the move is not immediate, the collaborator must return/remain in his/her home and work in a home office;

4. The third IT team is triggered together with the company's collaborator team in item 2, and will adopt the procedures below:

   4.2 Automatic response configuration of emails, for all collaborators with the following message "At the moment the AGBI team is unable to access some information and may have some problem receiving this message via email and receiving calls on their phones in the office. Please contact the partner Mr. Gustavo Fonseca at: (11) 99246-0733";

   4.3 Displacement to the place established as a contingency environment, to assist in accessing the information of the existing backup files, on a physical external disk that is in the possession of Mr. Gustavo and that will contain the backup and, at least, the last week of company activity;

4.4 Regardless of the incident derailing access to the office indefinitely, the IT team will provide a server that will be made available in the contingency environment, for the return of the backup return also made in the cloud using the Microsoft Azure Backup service, which we have the retention for 12 months, with daily full backups, because it is a solution integrated into the server operating system, this backup is only used in extreme situations.

5. When collaborators are in the contingency environment, notebooks or processing resources will be made available to key people in order to restore as soon as possible the flow of analysis, reports and information inside and outside the company, if no availability of notebooks for everyone to work or if the transportation of existing notebooks in the office has not been possible, the acquisition of new notebooks can be made possible in 24-48 hours;

6. Use of corporate mobile phones until the reestablishment of landlines or disclosure of new contingency contact numbers;

7. Resumption of e-mail communications by configuring the e-mail server on new computers or access via webmail. Because it is a remote service, access to e-mail through corporate smartphones should not be impaired in case of problems affecting the AGBI office;

8. Activation of the secondary internet link in case of service failure in vivo's primary link;

9. Once access to the office is reestablished, the IT team will copy the changed files in the execution of the contingency plan, and synchronize them within the AGBI server, all necessary checks to ensure the integrity of the data will be verified, the communiqué previously configured in each collaborator's email will be disabled, and AGBI goes into normal operation.