TABLE OF CONTENTS

1. OBJETIVE

This document allows readers to understand the key activities that are executed to advance the practice of Digital Technology Continuity within Ecopetrol, as well as the roles responsible for its execution.

The activities are aimed at meeting the objective of the STI Science, Technology and Innovation process. In this sense, the continuity practice seeks to ensure that all services offered by the Vice Presidency of Science, Technology and Innovation have technological recovery strategies, which are tested and thus guarantee rapid recovery and continuous operation of the applications that leverage business processes.

2. GENERAL CONDITIONS

2.1   SCOPE

The Continuity Management practice and this guide that describes it must be applied to all Business services, defined by the Crisis and Continuity area of Ecopetrol, which are operated by the Vice Presidency of Science, Technology and Innovation and the new services that are designed and entered into production.

Consequently, it is applicable to all roles involved in the activities of the "Execution-Transfer and Sustainability of technology" subprocess: such as Service Leaders, Operations Practice Leaders, Digital Leaders (framework or project), Product Owner or Functional Leader, Digital Innovation Studio, and also extends to third-party IT Allies and Auditors of the respective contracts.

2.2   ASSOCIATED DOCUMENTS

The practice is aligned with what is defined within the government of the Crisis and Continuity area of Ecopetrol at the level of strategy, guidelines, definitions, articulated response structure, response teams at each level and the scenarios of loss of business continuity which are found in:

- GCC-G-001 Methodological Guide for the design and execution of exercises and tests.
- GCC-D-001 Business Continuity and Crisis Management Guidelin
- GCC-M-001 ECP Business Continuity Manual

2.3   GENERALITIES

Within ECOPETROL's Comprehensive Management System, there is crisis and continuity management, whose objective is to increase the organization's capacity to prevent, respond and recover from risk scenarios that may generate disruption of critical business functions and/or impact the reputation and compliance with the company's highest strategic objectives.

For the activities included in the practice, the Ecopetrol resilience model is followed:
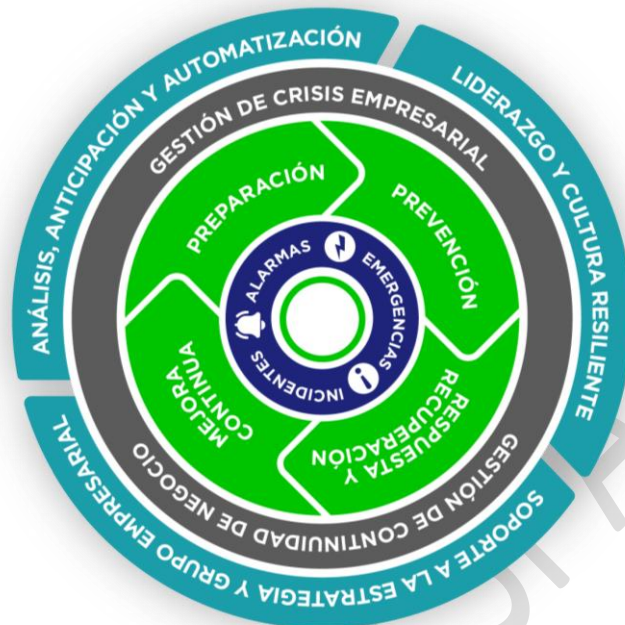
Illustration 1. Ecopetrol Resilience Model

Continuity Management at Ecopetrol is carried out at 3 levels, strategic, tactical and operational as shown below:
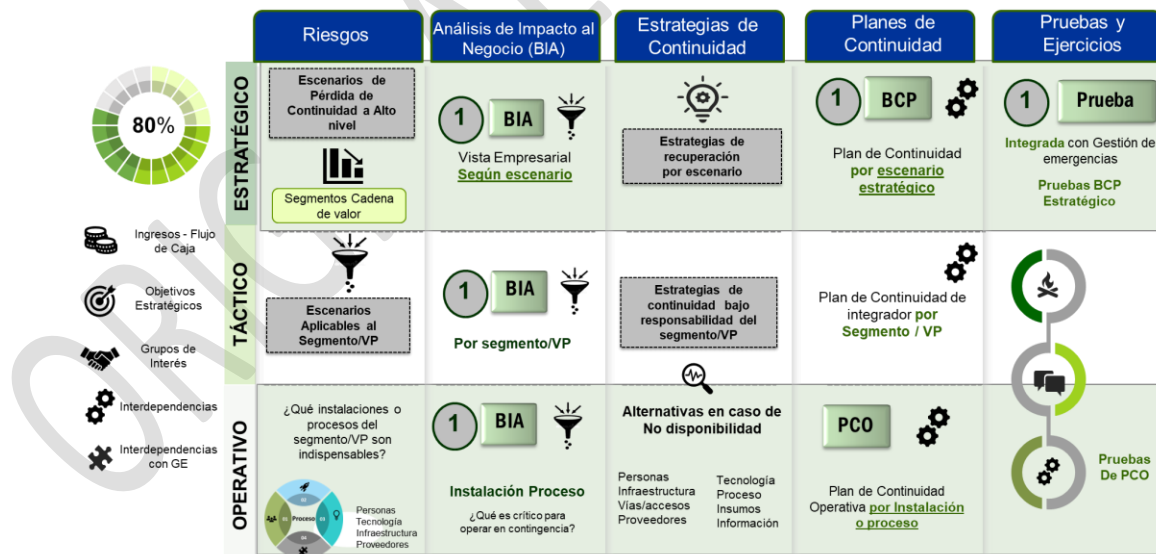

Illustration 2. Levels of Continuity Management

As part of the Crisis and Continuity strategy, technological continuity is part of business continuity.

The Continuity practice in the Vice Presidency of Science, Technology and Innovation applies to the strategic level (PCE) and operational level (PCO, PRTs and DRPs):

- **Strategic Continuity Plan – PCE:**

The scope of the Strategic Scenario covers the analysis of Scenario 8: "the NON-availability of critical applications and services managed by the VTI in Onpremise, Cloud environments and connectivity services."

In the continuity practice, the responsibility for ensuring compliance was centralized to carry out the analysis, consolidate the strategies and respond to Scenario 8 "Non-availability of critical applications and services managed by the VTI".

The tasks are updating the progress of the plan to close gaps that resulted from this analysis, reporting the status and managing the response to the VDS by the vice president (owner/accountable).

What is related to this strategic level, obeys the definition of a BIA and a **PCE Strategic Continuity Plan** whose accountable is the vice president of the VTI for the mitigation of the risks of Scenario 8.

Ensure preparation and updating of the Strategic Continuity Plan and alternative solutions. And the associated annexes by the VTI. At least one test should be performed annually.

NOTE: For this front, a flow or detail of the activities is not prepared, as it is due to a direct request from the crisis and continuity area, for the delivery and officialization of the information.

- **Operational Continuity Plan of the Vice Presidency – PCO:**

As part of the business continuity cycle that is reviewed annually, the BIA (Business Impact Analysis) analysis is carried out, which allows identifying the critical processes of each business area, analyzing the level of operational and financial impact and estimating recovery times (RTO), in relation to management with the rest of the company at the time of an interruption.

After this analysis, the critical scenarios associated with the identified processes are identified and the magnitude of the operational and financial impact at the time of an interruption is also analyzed, as well as the actions defined to provide continuity to the processes or services identified as critical in the BIA.

Finally, the Operational Continuity Plan is prepared, which also includes the details of the critical processes of the business area, the basic information of the required resources and the recovery times to put the services into operation and therefore the continuity of the business and recover in the shortest time, the normal operation of the service that has been affected, minimizing the negative impact on the other business areas.

- **Technological Recovery Procedures – PRT:**

The objective of the PRT is to ensure the existence and updating of the procedures and the recovery of the applications required by the business processes, prioritizing those defined as critical in all the PCOs of the other business areas and the rest of the services (applications, platforms, infrastructure) operated by the Vice Presidency of Science, Technology and Innovation.

The official repository of all PRTs is the Continuity sharepoint portal:
https://ecopetrol.sharepoint.com/sites/AppNoSAP/Continuidad/SitePages/Bandeja%20Gesti%C3%B3n.aspx#InplviewHash6cd9f2e0-bfb9-4f79-9af6-90844303a77a=ShowInGrid%3DTrue
Where the control and monitoring of the annual test plan is carried out, and the monthly monitoring of the PRT tests.

Disaster Recovery Plan – DRP: Disaster Recovery Plan

The objective of the DRP is to ensure the existence of actions for the activation and return of applications and services in order to provide continuity to critical business processes in the event of disaster events.

The official repository of all DRPs:
https://ecopetrol.sharepoint.com/sites/AppNoSAP/Continuidad/SitePages/Bandeja%20Gesti%C3%B3n.aspx#InplviewHash6cd9f2e0-bfb9-4f79-9af6-90844303a77a=ShowInGrid%3DTrue

3. Development

3.1 ACTIVITIES

Each of the activities and roles of each of the team members are described below.

a. Decision: activate continuity and/or recovery?: this decision is aligned with the crisis declaration made by the Crisis and Continuity area of Ecopetrol and also with the critical priority incident management decision that means that the corresponding PCO alternatives or Technological Recovery strategy must be executed, under at least one of the following conditions:

- There is a high probability or high level of certainty in the materialization of an alarm that compromises the delivery of prioritized critical processes

- The Incident Management practice identifies that:
    o The incident meets

Line	Event	Critical Priority IT Incident Management Plan Trigger
Services/applications and infrastructure	Affectation of a critical priority service.	More than 24 horas

Table 1. Incident Conditions Critical Priority

o The incident affects or has the potential to affect the usual way of operation of the prioritized critical processes, causing the minimum level of operation defined for continuity to be reached.

o The solution to the interruption incident is estimated to be greater than the Recovery Time Objective -RTO defined in the recovery strategies

a. Activate continuity or execute technological recovery strategy: in this activity the PCO of the Vice Presidency of Science, Technology and Innovation is activated to maintain the service or critical processes in operation, as well as execute the corresponding Technological Recovery strategy.

b. Return to normal: this activity must be executed only if the incident practice confirms that the service has been recovered in its initial state, with which the continuity practice returns the services to normal operation.

c. Control and monitor: ensure the results of the Continuity practice and identify opportunities for improvement and implement them. Measure the availability of services.

3.1.a PCO – Operational Continuity Plan

It is the activity in charge of ensuring crisis and continuity guidelines with the objective of developing the BIA of the Vice Presidency, preparing and updating the PCO (Operational Continuity Plan) and carrying out annual tests.

The following is the flow that specifies the step by step to follow to ensure the actions required to keep the BIA and PCO of the Vice Presidency of Science, Technology and Innovation updated.
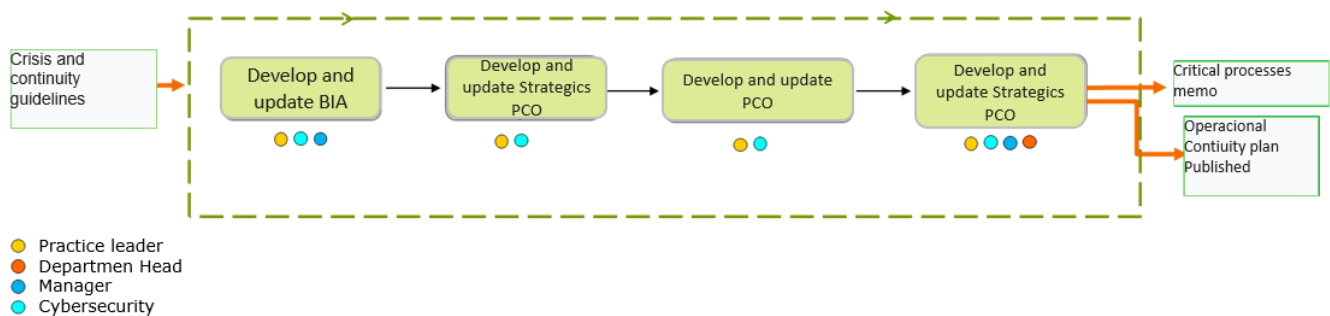

Ilustración 3. Flujo Plan Continuidad Operativa

3.1.b PRTs – Technological Recovery Procedures

It is the activity in charge of:

- Ensure the development and updating of technological recovery procedures by the projects (new services) and the operation (updating existing ones). According to PRT policies defined in this guide. See Annex 1
- The planning, execution and monitoring of testing of recovery procedures, as well as ensuring the reporting of results and corrective or improvement actions
- Recovery of the service, applications and/or infrastruc
- Backup policies are implemented according to the requirements of each project, for example: the backup of Kactus systems is not the same as that of the Video Game Chat, the retentions and priorities are different.
- If there is a backup for certain components that can be redeployed, you would go the redeploy route rather than the backup route, because it is sometimes slower, according to each scenario.
- It is necessary to validate according to the solution and the scenarios, if the backup is still valid, or if the backup is the second option, because backups may be being made to backups that are not required. For example, in a digital position there must be backups that have a backup, and it was decided that it would be better to deploy and mount the application.
- Generation of reports on results and improvement actions of the PRT, establishing formal feedback on the results and restoration times, which must be sent to the Crisis and Continuity team, to articulate this information in the Business Impact Analysis – BIA.
- The frequency of backup restoration tests is included in the annual PRT tests, in accordance with disaster events and unavailability of applications and services.
- Critical IT applications are prioritized for the annual PRT testing program.

The recovery strategy and procedure, as well as the report of each test, is recorded on the official site of the PRTs, which is the [sharepoint del portal de continuidad](#).

The scope of this test is technical in nature, for this reason the functional test is optional, at the discretion of the functional leader.

PRTs in Operation:
The following flow shows the detail to guarantee the updating of the PRTs and their activation when required:
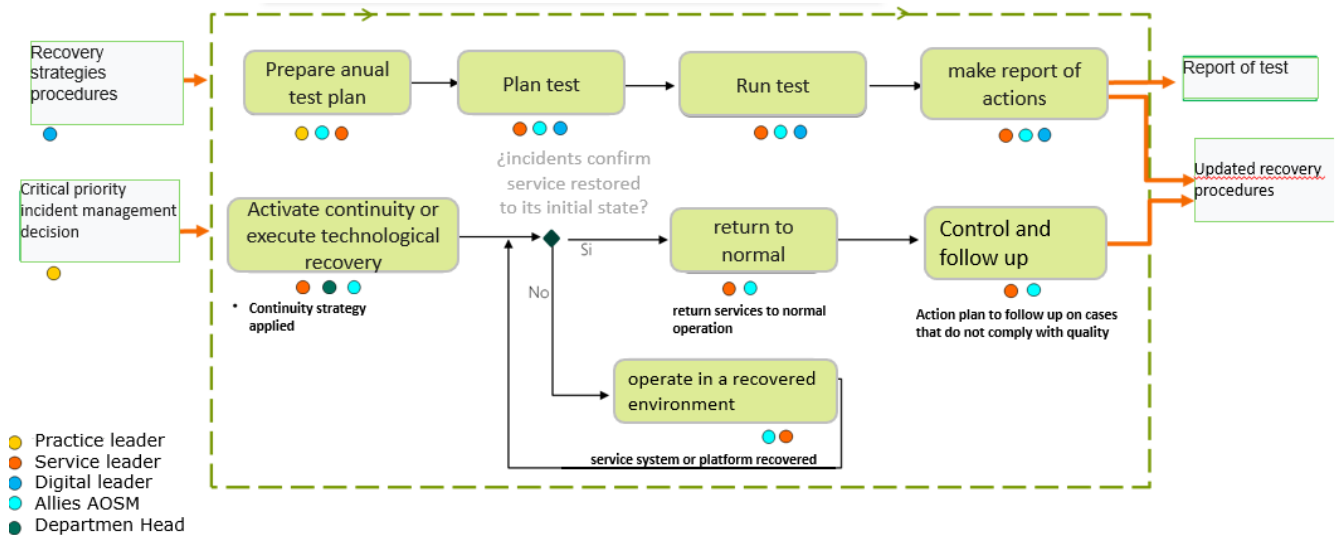
Illustration 4. Technological Recovery Procedure Flow

Note:
- Only prioritized or critical applications BCM (Critical for business continuity) have an RTO and RPO defined by the businesses, in their annual BIA exercises. For other applications that are not critical for business continuity, the RTO time is the result of the last test. And the RPO according to the backup policy

PRTs in Projects:
When receiving PRTs from projects, the following must be taken into account:
In Azure Devops it is acceptable to have PRTs while the project finalizes delivery to the operation and the operation at that time can incorporate the PRT in the portal and in the next annual PRT testing cycle.

Before starting the continuity process, the application service must be registered in the UCMDB, ASSET MANAGER and Asset Management

If the solution is not SaaS
Define and document Technology Recovery Strategy and Procedure (PRT).
The solution is required to have a continuity strategy and technological recovery procedure, so that users of the application service can perceive shorter times of unavailability of a solution/application consistent with the business process

These are the IT continuity requirements that need to be managed prior **to the solution going into production**:
1. Fill out the Backup Record (reviewed and approved by the Backup Leader) and upload the support email generated with the approval of the Backup policy to the site defined by the transition practice.
2. Determine the steps to follow to recover the solution/application/platform.

3. Register the continuity strategy on the official SharePoint site of the continuity portal and the steps to follow to recover the application service.
4. Schedule a PRT test on the official sharepoint site of the continuity portal.
5. Perform the test with the Partner that receives in operation (*), after executing the test, document the results with the evidence in the same PRT on the official sharepoint site of the continuity portal, filling out all the information, and request the approval of the PRT by the same means to the service leader.
   o Remember that those responsible for defining the expected RTO and RPO indicators are those defined by the Businesses with support from the Crisis and Continuity Area and those obtained are the result of the tests with the Allies, the calculation carried out in RTO and RPO obtained is the sum of the times of the activities executed, recorded in the continuity portal.
6. Check if the business has PAO, provide that information if it exists. If you do not have documentation that it does not exist.
7. The information must be completed at the site defined by the transition practice, in the format and/or repository defined by the practice.
8. The project notifies through the site defined by the transition practice, with a tag (@) to the service leader with a copy to the Continuity practice leader, the upload of the information with the approval of the PRT (Continuity Portal URL where the approval was) by the service leader, and the ID of this PBI (#) for validation. Specifically in the site defined by the transition practice in the NON-FUNCTIONAL REQUIREMENTS - Continuity item, include the approval url in the PRT report by the service leader located on the official sharepoint site of the continuity portal for transversal knowledge of the teams.
9. The project leader notifies the VoBo through the site defined by the transition practice, with a tag (@) to the practice leader, with a copy to the service leader.
10. The practice leader notifies the closure of the PBI (#) through the site defined by the transition practice.

Note:
- (*) If an Partner that receives in operation has not been defined, the test is carried out only by the project team.
- Keep in mind that the PRT test is executed in a QA environment or another environment other than PRD.
- Approval of the PRT test report is the service leader.
- Name the stage in the pipeline with PRT. DO NOT name it as PRODUCTION.

In case the solution is SaaS
1. It is required that the contractual documentation of the service level agreements be uploaded from the site defined by the transition practice to know what it includes about backup, continuity or technological recovery plan.
2. The project notifies through the site defined by the transition practice, compliance with the above described with a tag (@) to the service leader for validation and approval in the Wiki with a copy to the leader of the continuity practice.
3. The service leader must give the VoBo through the site defined by the transition practice, with a tag (@) to the project with a copy to the practice leader.
4. The practice leader performs the closure of the PBI (#) through the site defined by the transition practice

3.1.c Disaster Recovery Plan (DRP)

DRPs in Proyects:
When DRPs are received by projects, the following must be taken into account:

Before starting the continuity process, the application service must be registered in the UCMDB, ASSET MANAGER and Asset Management

If the solution is not SaaS

- For DRP´s take in account the following:

DR implementation applies only to solutions defined as BCP,
Define and document Disaster Recovery Strategy and Procedure (DRP). The solution is required to have a technological recovery strategy and procedure in the event of a disaster, so that users of the application service can perceive shorter times of unavailability of a solution/application consistent with the business process.
These are the IT continuity requirements that need to be managed prior to receipt of the DR operation of the solution:

1. Register the Backup Record (reviewed and approved by Backup Leader), and upload support email generated with the approval of the Backup policy to the site defined by the transition practice.
2. Register on the official SharePoint site of the continuity portal, the continuity strategy and the steps to follow to activate/return the application service with viable activation scenarios.
3. Schedule DR test on the official continuity portal sharepoint site.
4. Perform the test with the Partner that receives in operation (*), business of the critical process and service leader, after the final test/validation has been executed, document the results with the evidence in the same DRP on the official sharepoint site of the continuity portal, filling out all the information, and request the approval of the DRP by the same means to the service leader
   a. Remember that those responsible for the definition of the expected RTO and RPO indicators are those defined by the Businesses with the support of the Crisis and Continuity Area and those obtained are the result of the tests with the Allies, the calculation carried out in RTO and RPO obtained is the sum of the times of the activities executed, registered on the official sharepoint site of the continuity portal.
5. The project notifies through the site defined by the transition practice, with a tag (@) to the service leader, to the business leader with a copy to the leader of the Continuity practice, the upload of the information with the approval of the DRP (Continuity Portal URL where the approval was) by the service leader, and the ID of this PBI (#) for validation. Specifically in the Wiki in the NON-FUNCTIONAL REQUIREMENTS item - Continuity, include the approval url in the DRP report by the service leader located on the official sharepoint site of the cross-team continuity portal.
6. The project leader notifies through the site defined by the transition practice the fulfillment of the above described by requesting the VoBo, with a tag (@) to the practice leader, with a copy to the service leader
7. Delivery of the DRP activation template and return of the DRP to PRD template approved by the service leader.
8. The practice leader notifies the closure of the PBI (#) by the site defined by the transition practice.

Note:
- Approval of DRP test report is done by service leader.
- The PRT test is executed in a QA environment or another environment other than PRD.
- Name the stage in the pipeline with DRP. DO NOT name it as PRODUCTION or PRT

In case the solution is SaaS
1. It is required to upload to the site defined by the transition practice, the contractual documentation of the service level agreements that includes the continuity strategy or DRP disaster recovery plan and that includes that it has a DRP Disaster Recovery and that there is a commitment to carry out at least one open test with other integrations that are required to ensure the continuity of the business process.
2. Delivery of the DRP activation template and return of the DRP to PRD
3. The project notifies through the site defined by the transition practice, compliance with the above described with a tag (@) to the service leader for validation and approval in the Wiki with a copy to the leader of the continuity practice.
4. The service leader must give the VoBo through the site defined by the transition practice, with a tag (@) to the project with a copy to the practice leader
5. The practice leader performs the PBI closure (#) for the site defined by the transition practice.

The following is the flow that shows the existence of Recovery Procedures for the entry of new services into the operation, through the Transition practice:
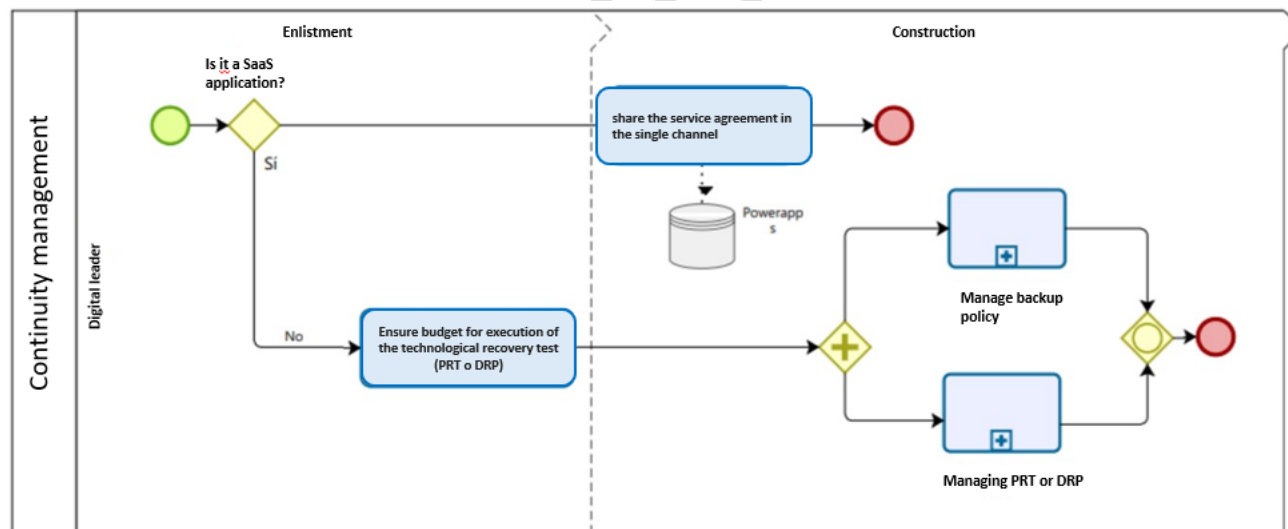

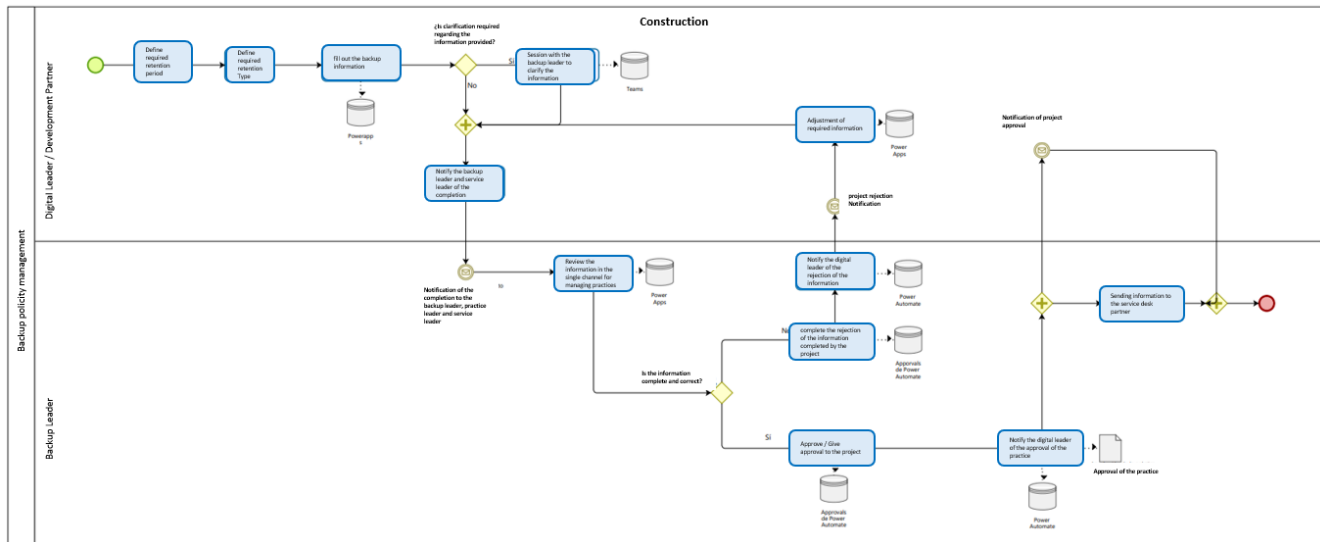**Illustration 5. Flow Practice Transition Procedure Continuity**

Illustration 6. Practice Transition Procedure Flow Continuity - Backups
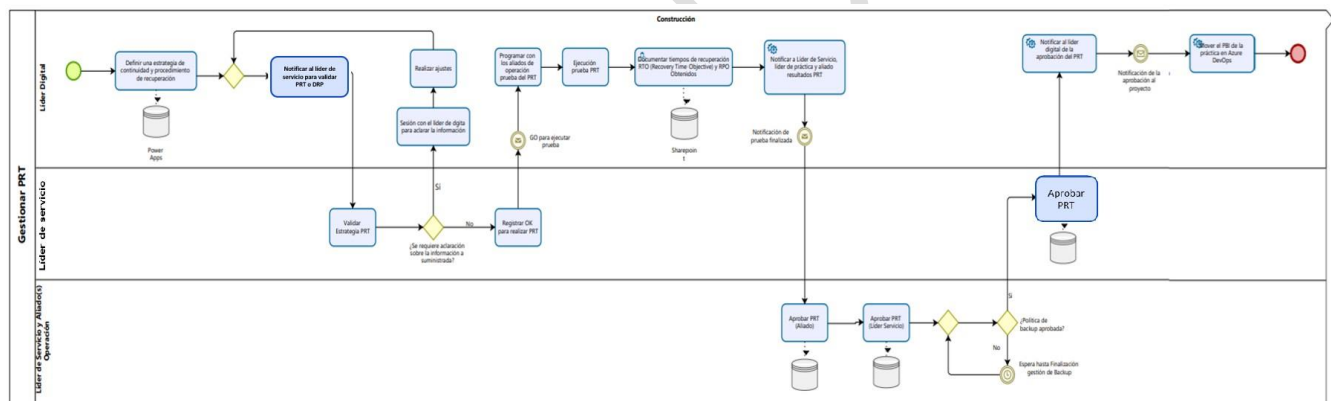

Illustration 7. Flow Practice Transition Procedure Continuity

3.2 RASCI of activities

The following table clarifies the assignment of responsibilities for each relevant activity and decision using the RASCI matrix: **R**esponsible, **A**ccountable, **S**upport, **C**onsulted and **I**nformed.
- Responsible (**R**esponsible): person assigned with the responsibility of doing the task
- Approver (**A**ccountable): person who makes the final decision and is ultimately responsible for executing the task.
- **S**upport: person who supports the person responsible in the execution of the task.
- **C**onsulted: person who is consulted before making a decision or executing an action
- **I**nformed: person who is informed of a decision or action that has been taken or executed, respectively.

3.2.a PCO – Operational Continuity Plan

Actividad	Responsible	Accountable	Supportive	Consulted	Informed
Develop/Update the BIA	Defined leader for critical process	Critical process manager	Practice leader (Continued)	Managers	Managers Department
Develop/Update Estrategic of PCO	Defined leader for critical process	Managers Department	Practice leader (Continued)	Service leader	Manager
Develop/Update of PCO	Defined leader for critical process	Critical process manager	Practice leader (Continued)		Managers Department
Perform tests PCO	Defined leader for critical process		Practice leader • (Continued) • Service leader	Not Applicable	Manager

Table 2. RASCI – Operational Continuity Plan

3.2.b PRTs – Technological Recovery Procedures

Actividad	Responsible	Accountable	Supportive	Consulted	Informed
Prepare Annual Testing Plan	Partner	Practice leader (Continued)		Service leader	Service leader
Plan Tests	Partner	Service leader / Digital leader	Partners		Partners
Run the test	Partner	Service leader / Digital leader	Partners		Partners
Perform Report/Actions	Partner	Service leader / Digital leader	Partners		Partners
Run Recovery Procedure	Managers Department / Service leader	Managers Department	Partner		Business
Operate in recovered environment	Partner	Service leader			
Return to normal	Partner	Service leader			
Control and Monitor	Partner	Service leader			User

Table 3. RASCI – Technological Recovery Procedures

3.2.c DRP - Disaster Recovery Plan

Actividad	Responsible	Accountable	Supportive	Consulted	Informed
Prepare Annual Testing Plan	Partner	Practice leader (Continued)		Service leader	Service leader
Prepare/maintain DRP activation template and return of DRP to PRD	Partner / Digital leader	Service leader	Partners	Practice leader (Continued)	
Drill planning / Testing	Partner / Digital leader	Service leader / Digital leader	Partners		Practice leader (Continued)
Run Mock/Test - DRP Activation	Partner / Digital leader	Service leader / Digital leader	Partners		Partners
Operate in DRP environment	Functional leader / Business responsible	Service leader / Digital leader			
Return mock/test - Return DRP to productive	Partner / Digital leader	Service leader / Digital leader	Partners		Partners
Perform Report/Actions	Partner / Digital leader	Service leader / Digital leader	Partners		Partners
Control and Monitor	Partner	Service leader			User

Table 4. RASCI – Disaster Recovery Plan

3.3   METHODOLOGY

3.3.a Generalities

In order to ensure that the test plans of the defined recovery procedures work as defined in the service design, they must be tested at least once a year, for which the following considerations must be taken:

- The plans are the responsibility of the service leaders with the support of each Partner.
- All applications/services in charge (SaaS and Stand alone are excluded) must have a PRT and a schedule for testing in the continuity portal.
- All plans are consolidated by the practice leader for comprehensive tracking using the sharepoint of continuity portal site available for tracking and controlling evidence.
- Review of monthly reports from Allies in conjunction with service leaders and corresponding auditors.
- Alignment of the integration of the tests of the components managed by the different Allies

This planning is locate don the site sharepoint of continuity portal.

3.3.b Follow up

Premises that must be taken into account for monitoring:

- The continuity practice leader convenes the follow-up sessions.
- Hold monthly sessions with each Partner responsible for applications, services and infrastructure.
- The participation of the corresponding service leaders and interveners is required.
- Each Partner must present evidence of compliance with the plan, reports and sending the above information to service leaders, all in the same continuity portal.
- In the event of a contractual breach that affects what is defined by this practice, the situation will be escalated in particular to the Coordinator and Head of the respective Department.

3.3.c Measurement

The information and/or metrics with which the practice will be monitored are:

• Test coverage and effectiveness: this metric identifies the coverage of the tests carried out on all applications for business continuity. Regarding effectiveness, the number of successful tests and/or with improvement actions is measured with respect to the number of tests on the applications subject to measurement.

4. CONTINGENCIAS

Not Applicable

5. EXHIBIT

Exhibit 1 – Policies for PRTs and DRPs.

VERSIONS LIST

Previous Document			
Version	**Date** **dd/mm/yyyy**	**Code and title of document**	**Changes**
1	03/11/2020	T&I-G-020	Initial document
2	23/12/2022	T&I-G-020	Update of the document, due to adjustment to the CT+I process and document alignment.
1	27/06/2023	CTI-G-003	Update of the CT+i Document with the Open Text Guide base
2	11/09/2023	CTI-G-003	Update for improvements and new practice guidelines
New Document CT+i			
Version	**Date** **dd/mm/yyyy**	**Changes**	
3	30/07/2024	Update of the DRP document, PBI update of the continuity practice on PRTs and DRPs. and information backups in PRTs and DRPs.	

For more information go to:

Author(s):
Diana Janeth Gomez Quintero
E-mail: dianaja.gomez@ecopetrol.com.co
Dependence: Service Transition Coordination
Digital Quality Department
Cluster Management 5th Industrial Revolution

Electronically reviewed by:	Electronically approved by:
Paula Marcela Cardona Osorio Service Transition Coordinator Identity document No. 30.238.602 Vice Presidency of Science, Technology and Innovation	**Carolina Santos Cabrera** Digital Quality Department (e) Identity document No. 52.712.860 Vice Presidency of Science, Technology and Innovation

*Document signed electronically, in accordance with the provisions of **Decree 2364 of 2012**, through which article 7 of Law 527 of 1999 is regulated, on the electronic signature and other provisions are dictated.*
*To verify compliance with this mechanism, the system generates an **electronic report that shows the traceability of the review and approval actions** by those responsible. If you need to verify this information, request said report from Service Desk*

Exhibit 1. Definitions for PRTs y DRPs

They must meet the following minimum requirements and standard guidelines:
- Have the required level of detail in the description of the strategy and activities.
- Ensure in the strategy that all activities have a person in charge, the name of the role is accepted (server administrator, database administrator, application support, etc.), given that at the time of the test it must be updated to the names of those who perform the test / simulation.

- Completeness in filling out all the fields defined for the documentation of the results report
- Be updated, with detailed and complete information, in the official repository.
- Carry out timely registration of changes, without waiting for the next cycle to do so.
- For cases in which the technological recovery times (RTO and RPO) obtained during the test exceed the times agreed by the businesses, an analysis must be carried out and documented on the causes that generate the differences between these times; and include the evidence of this analysis in the PRT or DRP.
- The time taken by functional leaders to perform the functionality test (when applicable) should be excluded from the RTO times.
- The description field of service components, complement by application with the following message: "To know the service components, please refer to the UCMDB in the CI: SERVICE MANAGER CLOUD Universal CMDB (https://aeuecpaucmdb2p.red.ecopetrol.com.co:8443/ucmdb-ui).
- It is required to update all models of the services/applications in charge in the UCMDB with all its components.
- Validate the consistency of the RPO obtained against the test start data and the date of the last backup, in order to ensure the quality of the PRT.
- Guarantee that the tests are executed considering all the defined activities, in order to achieve the measurement of RTO times, in accordance with the reality of the process and identify failure situations that have not been previously detected.
- The participation of functional leaders in the PRT tests is at the discretion of each functional leader.
- Define action plans and lessons learned.
- Document the risks and controls associated with each test.
- Define risks and controls (defined transversal or others).
- Identify monthly those tests / drills, for which failures have occurred consecutively (months and/or years) in the execution of the tests, in order to remedy the failure situations or improve the defined activities and allow the Organization to guarantee that in the event of an interruption, the business process can continue.
- Ensure that the activities executed with respect to those planned are complete.
- Carry out a feedback exercise to service leaders and the crisis and continuity area of the results of the tests / drills, so that the businesses and the crisis area take the corresponding actions and/or adjustments in the definitions.
- Approve or reject according to compliance with the previous guidelines.