TABLE OF CONTENTS

1. CONTEXT OF THE EXERCISE

Date of execution:	29/09/2025	**Start Time:** 8:00 am	**End Time:** 11:00 am
Approximate duration:	3 hours	**Exercise Coordinator:**	Diana Janeth Gómez
Name of Exercise:		VTI Operational Continuity Plan Test Continuity Cycle 2024-2025 – Service continuity test in the event of total non-availability of Onpremise network accounts and clouds linked to Active Directory.	
Place of realization:		The test is run at the remote/face-to-face work sites of the test participants in Ecopetrol Sol y Luna Room Floor 1 Ecopetrol	
Name of the facility or process to be tested:		Process: Science and Technology CT+i / Execution - Transfer and Sustainability of technology / Manage, support and operate technological solutions / Incident Management.	
Proven plan(s):		Active Directory Plan	
Vice presidency:		Science, Technology & Innovation	

General objective of the exercise:

The main objective of the test is to simulate the activities to be carried out when an incident occurs of the deletion of all network accounts in Onpremise/cloud, in order to increase the capacity of the VTI to anticipate and respond to this type of incident.

According to the operational continuity plan, the scenario and strategy to be tested are as follows:

Scenario: ECO-006 Technology Non-Availability
Sub-scenario: SUBECO-006-01 Non-availability of IT applications
Variant: Unavailability of access to network accounts that allow access to Microsoft 365 services (Outlook, SharePoint, Teams and other applications linked to Active Directory)
Included in the VTI Operational Continuity Plan within the framework of the Organizational Resilience cycle for the 2024-2025 term.

SPECIFIC OBJECTIVES (SEE ANNEX 1):

OBJECTIVE	INDICATOR CHECK MEASURE***	LOCATION REMOTE OR SITE ***
Event Identification (Detection)	CHECK	REMOTE
Log incidents arising from monitoring tools	CHECK	REMOTE
Activation of Response and Notification (Alarm)	CHECK	REMOTE
Incident Management Team (EMI) Activation	CHECK	PLACE
Activation of the Business Support Team	CHECK	REMOTE
Human Resources Enlistment	CHECK	REMOTE
Definition and Control of Necessary Resources	CHECK	PLACE
Clarity in Assumed Roles	CHECK	PLACE
Clarity in the activities to be carried out	CHECK	PLACE
Control Response Standard Operating Procedures	CHECK	REMOTE
Analysis of Operational Continuity Impacts	CHECK	REMOTE
Operational Communications towards Continuity (Business Support)	CHECK	REMOTE
Using Documentation and Templates in Command Activation	CHECK	REMOTE
Incident Command activity logging and tracking	CHECK	PLACE
Tests response from SDD and PCO IT service partners.	CHECK	REMOTE

Ensure service restoration		CHECK	PLACE
Disciplines to be verified:	CONTINUITY MANAGEMENT OF INFORMATION TECHNOLOGIES OR CYBERSECURITY.		
Modality for carrying out the exercise:	Table Exercise		

Documents related to the exercise (information inputs):

1. GCC-F-001_Formato_Plan_Del_Ejercicio
2. GCC-F-002_Formato_guión_de_pruebas_y_ejercicios_de_Crisis_y_Continuidad
3. GCC-F-003_Formatos_de_observador_del_ejercicio-test
4. GCC-F-004_Formato_Evaluacion_del_ejercicio
5. GCC-F-005_Informe_del_ejercicio-prueba_V4

Executed Scenario:

Initially, the activities to be carried out when an incident occurs of the deletion of all network accounts in Onpremise/cloud is simulated.
When the service is restored to its normal conditions, TIVIT's Incident Manager confirms the return to normal of the incident.

Premises of the mock test scenario:

- This test is only a theoretical exercise in continuity; does not imply actual deletion of users nor does it affect the service
- There will be no escalation to the Vice Presidency support team, nor to the Business Crisis Committee.
- The PCOs of the allies who solve incidents will not be activated, only the PCO of the Active Directory ally.
- Incident resolution: The guidelines of the incident management practice will be applied according to Ecopetrol's Operation Model for Critical, High and Massive Incidents.
- The test does not contemplate failed activities in the resolution of the incident.

Board 1, Basic Information of the exercise

2. TEAMS PARTICIPATING IN THE EXERCISE

2.1 Agenda of the planned exercise:

The exercise was carried out following the agenda shown below.

Hour	Activity	Estimated time
8:00 AM	1. Report simulated cases to SDD by phone that "indicate that when you try to access the network account in Office 365, a notice comes out indicating that you do not recognize it" for SDD.	2 minutes
8:03 AM	2. Log and/or classify incident in SDD according to its priority level (SM must allow logging in with local accounts)	2 minutes
8:05 AM	3. Ask in the Whatsapp chat of Critical/High/Massive Incidents if there is any failure in the Active Directory due to the number of incident reports that are reaching SDD	2 minutes
8:12 AM	4. Inform the SDD incident manager by phone or chat (WhatsApp) so that he or she can report by phone or chat (WhatsApp) to the first level of support (Allied Incident Manager) according to the escalation matrix of each Service Provider published on the alternate site of the incident practice	7 minutes
8:13 AM	5. The Active Directory Service Leader contacts the TIVIT person on duty for the Active Directory service, in order to detect and confirm the unavailability of the associated network accounts.	3 minutes
8:18 AM	6. Detect and report unavailability of cloud/on-premise network accounts associated with Active Directory	4 minutes
8:21 AM	7. The incident manager of TIVIT PLATAFORMAS must make the first notification, the completion of the template for the first notification in the Ecopetrol WhatsApp incident chat (Incid-Crit/High/Massive) with the template published on the site/Alternate of the incident practice.	6 minutes
8:22 AM	8. The TIVIT incident manager creates and sends a link to the crisis table or crisis room, if necessary, through Meet or Teams and informs the link to enter the Ecopetrol incident chat (Incid-Crit/High/Massive). The incident status update should be per incident practice every 30 min. Define whether progress should be sent in a different time for this situation.	6 minutes
8:28 AM	9. Active Directory Service Leader Ecopetrol requests/activates emergency1 and emergency2 accounts	10 minutes
8:38 AM	10. The ECOPETROL Active Directory Service Leader indicates that the resolution of the incident requires a time greater than the 4 hours of the service RTO	3 minutes
8:42 AM	11. In the Crisis Room, the Active Directory Service Leader ECOPETROL requests the critical contact base for businesses and subsidiaries and allies for the creation of temporary manual accounts	4 minutes
8:46 AM	12. Delivery of the list of critical accounts of Ecopetrol, subsidiaries and allies	5 minutes
8:50 AM	13. Create temporary accounts of critical Ecopetrol users with script	5 minutes
8:47 AM	14. The Active Directory Service Leader requests the SDD Leader to send a service interruption message to the entire community (Ecopetrol and subsidiaries) and activation of IVR.	5 minutes

Hour	Activity	Estimated time
8:50 AM	15. The SDD Indra Incident Manager Verify in conjunction with TIVIT the pre-approved IVR messages about the incident to obtain the VoBo of Ecopetrol Service Management Coordinator	10 minutes
8:53 AM	16. Inform the community of Ecopetrol users and subsidiaries of the unavailability with the pre-approved Active Directory message	5 minutes
8:58 AM	17. SDD uploads the IVR message to the plant and informs the community of Ecopetrol users and subsidiaries of the unavailability with the pre-approved Active Directory message previously approved	6 minutes
9:01 AM	18. Creation of VTI Whatsapp chat on the progress of the solution of the Incident, information for communications with business and subsidiaries	3 minutes
9:03 AM	19. The continuity practice leader performs the analysis and proposes the activation of incident command as defined in the PCO and Governance model for IT Continuity when escalation to incident command is required.	5 minutes
9:08 AM	20. Manager Approves PCO VTI Incident Command Activation	3 minutes
9:11 AM	21. Filling out formats for PCO VTI.	10 minutes
9:14 AM	22.TIVIT Active Directory Domain Controller Administrator informs you of the need to activate Active Directory Backup. Backup Team Requested to Recover Active Directory On-Premise	5 minutes
9:08 AM	23. Create the Backup Request Task in Service Manager for Backups	3 minutes
8:54 AM	24. Delivery by TIVIT backup of the re-established on-premise server and with the drivers, users, data and applications	10 minutes
9:15 AM	25. The active domain controller administrator verifies that the server has the structure and data, users of the directory, according to the protocol of the operation delivered in On premise and initiates On premise synchronization with Cloud	10 minutes
9:45 AM	26. Validation of the synchronization and replication process is performed on Domain controllers and validates the ADConnect, email accounts	10 minutes
9:50 AM	27. Perform analysis of the actions carried out in the cloud to solve the incident, confirm operational service and close incident in the chat of critical/high/massive incidents.	10 minutes
10:05 AM	28. Delete temporary accounts	5 minutes
10:10 AM	29. The TIVIT Incident Manager makes the message about the return to normality of the incident to obtain the VoBo of Ecopetrol Service Management Coordinator	4 minutes
10:16 AM	30. Inform the Ecopetrol user community of the availability of the network accounts associated with the Active Directory and remove IVR message	6 minutes
10:31 AM	31. TIVIT incident closure in SM	5 minutes
10:41 AM	32. Report deactivation of PCO-VTI preventively and return to normality.	5 minutes

Hour	Activity	Estimated time
10:46 AM	33. Closing of the VTI Operational Continuity Plan Test	5 minutes
10:50 AM	34. Conduct a survey to determine lessons learned from the test result	10 minutes
10:56 AM	35. PCO VTI Test Feedback to Participants	20 minutes

Board 2, Executed fiscal year agenda

2.2 Exercise coordination team:

NAME	SPECIFIC FUNCTION	ROLE IN EXERCISE	LOCATION
Yaneth Munevar Cendales	Digital Infrastructure Manager Incident Commander of the affected service	Responsible for approving the activation of the PCO	Face
Jaime Hernando Malagón Barinas	Overall coordination in resolving the incident EMI Planning Leader Responsibilities under PCO-VTI	General Coordinator of the event	Face
Diana Janeth Gómez Quintero	General planning Operational Continuity Front Responsibilities according to PCO. Coordinate the execution of the test activities, to ensure the validation of the PCO-VTI	Front of Continuity, Trial Service Leader	Face
Ernesto Parra Erazo	General coordination the execution of the test activities executed by Service Ally of service operation and compliance with Incident Management guidelines to ensure compliance with the Service's Operational Continuity Plan.	Service Leader Testing	Face
Wilman Alonso Camargo Duran	General coordination In the execution of the test activities, executed by Service Desk Digital	Service Management Coordinator	Face
Mario Javier López Murcia	Ensure compliance with continuity guidelines of the affected service	Physical Security Management	Remote

NAME	SPECIFIC FUNCTION	ROLE IN EXERCISE	LOCATION
Daniel Alejandro Gonzales Ángel	SDD Indra Service Manager / General Coordination Coordinate the execution of the test activities, to ensure the validation of the service management operation	SDD Indra Service Manager	Remote
If you require more rows please add them***			

Board 3, EXERCISE COORDINATION TEAM.

2.3 Team of exercise participants:

NAME	SPECIFIC FUNCTION	ROLE IN EXERCISE	LOCATION
Yaneth Munevar Cendales	Digital Infrastructure Manager Incident Commander of the affected service	Responsible for approving the activation of the PCO	Face
Jaime Hernando Malagón Barinas	General coordination in the resolution of the incident. EMI Planning Leader Responsibilities under PCO-VTI	General Coordinator of the event	Face
Diana Janeth Gómez Quintero	General planning Operational Continuity Front Responsibilities according to PCO. Coordinate the execution of the test activities, to ensure the validation of the PCO-VTI	Front of Continuity, Trial Service Leader	Face
Ernesto Parra Erazo	General coordination in the execution of the test activities executed by Service Ally of service operation and compliance with Incident Management guidelines to ensure compliance with the Operational Continuity Plan of the service.	Service Leader Testing	Face
Wilman Alonso Camargo Duran	Overall coordination in the execution of test	Service Management Coordinator	Face

NAME	SPECIFIC FUNCTION	ROLE IN EXERCISE	LOCATION
	activities, executed by Service Desk Digital		
Mario Javier López Murcia	Ensure compliance with continuity guidelines of the affected service	Physical Security Management	Remote
Wilson Rueda Gómez	SDD Ecopetrol Leader/ General coordination in the execution of the test activities executed by Digital Service Desk and compliance with Incident Management guidelines	SDD Ecopetrol Leader	Face
Héctor Fabio González	Ensure compliance with incident management guidelines during test execution.	Incident Practice Leader	Face
Edwin David Ramírez Doria	Ensure continuity of the affected application	Backup Service Leader	Remote
Fabian Andrés Gómez García	Ensure continuity of the affected application	Server Service Leader	Remote
Karen Alejandra Martínez Acevedo	Ensure continuity of the affected application	Active Directory Administrator	Face
Tommy Madero Vergara	Ensure continuity of the affected application	Infrastructure	Face
Diana Vélez/ Brayan Mora	Guarantee the registration of the situation presented in the affected service. SDD Service Leader	Service Desk Leader	Remote
Active Directory Administrator Team	Access tests, verification and fidelity tests of data information recovery, ensuring service restoration	Digital Service Desk Agents	Remote
Digital Service Desk Agents	Guarantee the registration of the situation presented in the affected service, Ensure incident logging and attention	Digital Service Desk Agents	Remote
Tatiana Andrea Esponda Ospina	Monitoring of the execution of the test as an observer to ensure the evaluation of the specific elements during	Test Observer	Remote

NAME	SPECIFIC FUNCTION	ROLE IN EXERCISE	LOCATION
	the PCO-VTI test and generate corresponding report		
Uriel Francisco Moreno Rodríguez	Monitoring of the execution of the test as an observer to ensure the evaluation of the specific elements during the PCO-VTI test and generate corresponding report	Test Observer	Face
If you require more rows please add them***			

Board 4, TEAM OF EXERCISE PARTICIPANTS

2.4 External staff participating in the exercise:

NAME	ENTERPRISE	SPECIFIC FUNCTION	ROLE IN EXERCISE	LOCATION
Diana Carolina Vélez	Indra SDD	Notify through WhatsApp chat "Critical, High and Massive Incidents", the message "Drill drill, interruption of service in Active Directory"	SDD Incident Manager	Remote
Carolina Ramírez	TIVIT PLATFORMS	Manage resources and people TIVIT PLATFORM team	TIVIT PLATFORMS Process Manager	Remote
Mauricio Abril	TIVIT PLATFORMS	Allied manager that resolves incidents based on information uploaded to Forms template SharePoint	Practical Incident Manager Ally	Remote
Mario Crispin	TIVIT PLATFORMS	Guarantee continuity of the process and health of the service.	Backup Manager	Remote
If you require more rows please add them***				

Board 5, EXTERNAL STAFF PARTICIPATING IN THE EXERCISE

3. ANALYSIS OF RESULTS

The following information corresponds to the analysis of the results of the exercise, in accordance with the objectives set, based on the strengths and opportunities for improvement identified in the different sources, which will serve to strengthen future tests/exercises.

3.1 Findings of the exercise According to the Observers:

Finding (Strength/Opportunity for Improvement)	Priority	Does it require action to be taken? Yes/NO
(OM) Ensure that all direct and indirect actors are clearly aware of their roles and responsibilities as scripted to respond effectively in a real crisis and complete, clear and timely communication required for decision-making.	Low	Yes
(OM) Perform scenarios with a real scope that can occur in an incident without relying on time constraints	Middle	Yes
(F) High level of technical expertise of the team in the attention of the scenario.	High	Yes
(F) Availability and commitment of personnel during the development of the test.	Low	No
(OM) During the exercise, it became clear that some pre-approved messages were not available for the scenario, despite the fact that the incident guidance states that they should be ready. It is recommended that you review and update pre-approved messages to ensure their availability in future tests and real events.	Middle	Yes
(OM) Being such a critical and high-impact service, it is recommended that drills include absolutely all necessary roles and all those who can intervene in a real incident, without having a time restriction with the drill	Middle	Yes

Board 6, Exercise Findings According to Observers

3.2 Findings of the exercise According to the Facilitators/Coordinator:

Finding (Strength/Opportunity for Improvement)	Priority	Does it require action to be taken? Yes/NO
Identify if it is an identified improvement opportunity or strength and describe it	High Medium Low	otherwise***
(OM) Include in the service's PCO the early integration in the VTI crisis room of the identity, operation partner, Cybersecurity, Cyber defense, and platform teams for root cause analysis, threat isolation and monitoring of suspicious activity and to be in sync with the messages that are reported	High	YES

Finding (Strength/Opportunity for Improvement)	Priority	Does it require action to be taken? Yes/NO
(OM) Incorporate in the service's PCO the contact with the corporate communications team in the presence of news in the media or social networks about the incident and document and take into account the corporate communications protocol that is being formalized and validate the messages with the Crisis Management Center, the Vice Presidency and the Presidency before issuing external communications.	High	YES
(OM) Implement active and permanent monitoring of social networks and media.	Middle	YES
(OM) Include in the service's PCO the obligation to create a case with Microsoft whenever an incident related to Active Directory occurs.	High	YES
(OM) Strengthen the training and definition of Incident guidelines , the use and scope of pre-approved messages, specifying which services apply to mass events.	Middle	YES
(OM) Extend the process of socializing the PCO test into several sessions, in order to identify and link all the necessary roles within the simulation.	Middle	YES
(OM) Document and inventory critical accounts technical accounts in applications to mitigate incident risks in other applications.	High	YES
(OM) Include in the PCO of the service the definition of temporary IPs 10.11.27.*** / 10.11.45.** and cyberark 10.76.184.**, 10.104.**, 10.76.184.***, 10.104.2.** that serves for access by authorized local administrators servers, domain controllers and vCenters. Additionally, take into account the entry of allies from site-to-site VPNs through dedicated channels	High	YES
(OM) Complement this simulated exercise with the technical exercise of periodic Active Directory Technology Recovery Procedure (PRT) testing, including domain controller restoration scenarios, AD Connect synchronization validation, and verification of the availability of critical accounts, in order to ensure the effectiveness of recovery times and minimize risks in a real event.	High	YES

Table 7, Findings of the exercise according to Facilitators/Coordinator of the Exercise.

3.3 Exercise findings based on Participants' assessment and feedback

Evaluation result of the exercise focus application

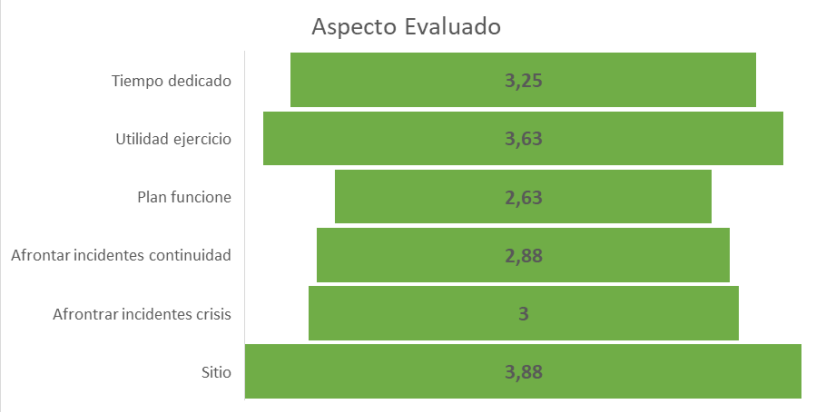


Figure 1, Exercise evaluation statistics.

Evaluated Aspect	Average
Time Spent	3,25
Profit for the year	3,63
Plan Works	2,63
Dealing with incidents continuity	2,88
Coping with crisis incidents	3
Place	3,88

Results of the evaluation of the logistic focus exercise

Evaluated Aspect	YES	NO
4. Script	6	6
2. Scope	3	4
7. Roles and Team	8	5
1. Objectives	1	5
3. Scenario	7	5
5. Communications	6	4
6. Time	1	8

Figure 2, Exercise evaluation statistics.

Finding (Strength/Opportunity for Improvement)	Priority	Does it require action to be taken? Yes/NO
(OM) Include in the guidelines the performance of at least one drill per year for this critical service where the entire team, roles and activities are involved, as well as document response alternatives. Due to criticality and the number of actors involved, additional socialization sessions with leaders (PODs) and allies should be scheduled to ensure alignment and effectiveness in the execution of the exercise.	Loud	Yes
(OM) Use the alternate communication tool in the same exercise	Low	NO
(OM) to carry out training of the entire technical team that could be in a real incident (There are 7 and the test was attended by only one person).	Middle	Yes
(OM) Strengthen the training and definition of guidelines for the Digital Service Desk, so that it is clearly established in which cases the IVR must be activated, the level of approval to send the unavailability message and timely communicate the type of failure presented.	Middle	Yes

Table 8, Exercise Findings Based on Assessment and Feedback

4. EVALUATION

4.1 Evaluation of compliance with the specific objectives of the exercise.

Specific Objectives	Perception of Compliance			
	Compliment	Partially fulfilled	Not fulfilled	Remarks
Event Identification (Detection)	X			
Log incidents arising from monitoring tools	X			
Activation of Response and Notification (Alarm)	X			
Incident Management Team (EMI) Activation	X			
Activation of the Business Support Team	X			
Human Resources Enlistment	X			
Definition and Control of Necessary Resources	X			
Clarity in Assumed Roles	X			
Clarity in the activities to be carried out	X			
Control Response Standard Operating Procedures	X			
Analysis of Operational Continuity Impacts	X			
Operational Communications towards Continuity (Business Support)	X			
Using Documentation and Templates in Command Activation	X			
Incident Command activity logging and tracking	X			
PCO testing of SDDs and IT service partners.	X			
Ensure service restoration	X			

Table 9, Evaluation of compliance with the specific objectives of the exercise.

4.2 Summary of the findings to be managed as a result of the exercise/test.

No.	Finding (Strength/Opportunity for Improvement)	Action to be Executed	Priority	Responsible	Start date	End Date
1	(OM) Ensure that all direct and indirect actors are clearly aware of their roles and responsibilities as scripted to respond effectively in a real crisis.	Conduct training with the entire team	Middle	Karen Martínez and Carolina Ramírez	10-10-2025	31-11-2025
2	(OM) Extend the execution scenario in critical IT service testing	Extend test scenario to real-world scenarios	Middle	Diana Janeth Gómez	10-10-2025	30-05-2026
4	(OM) During the exercise, it became clear that some pre-approved messages were not available for the scenario, despite the fact that the incident guidance states that they should be ready. It is recommended that you review and update pre-approved messages to ensure their availability in future tests and real events.	Validate pre-approved messages from massive incidents and ensure their availability	Middle	Héctor Fabio Gonzales López/Aliados	07/10/2025	31/12/2025
6	(OM) Being such a critical and high-impact service, it is recommended that drills include absolutely all necessary roles and all those who can intervene in a real	Involve all roles involved in the exercise	Middle	Diana Janeth Gómez	10-10-2025	30-09-2026

No.	Finding (Strength/Opportunity for Improvement)	Action to be Executed	Priority	Responsible	Start date	End Date
	incident, without having a time restriction with the drill					
7	(OM) Include in the service's PCO the early integration in the VTI crisis room of the identity, operation partner, Cybersecurity, Cyber defense, and platform teams for root cause analysis, threat isolation and monitoring of suspicious activity and to be in sync with the messages that are reported	Integrate all the required equipment into the crisis room	Middle	Ernesto Parra	07/10/2025	31/12/2025
8	(OM) Incorporate in the service's PCO the contact with the corporate communications team in the presence of news in the media or social networks about the incident and document and take into account the corporate communications protocol that is being formalized and validate the messages with the Crisis Management Center, the Vice Presidency and the Presidency before issuing external communications.	Incorporate into the Service PCO	Middle	Ernesto Parra/External communications	10-10-2025	30-05-2026

No.	Finding (Strength/Opportunity for Improvement)	Action to be Executed	Priority	Responsible	Start date	End Date
9	(OM) Implement active and permanent monitoring of social networks and media.	Supervise	Middle	Ernesto Parra/External Communications Team	10-10-2025	30-03-2026
10	(OM) Include in the service's PCO the obligation to create a case with Microsoft whenever an incident related to Active Directory occurs.	Include in the PCO of the service	Middle	Ernesto Parra / Diana Janeth Gomez	10-10-2025	30-03-2026
11	(OM) Strengthen the training and definition of Incident guidelines, the use and scope of pre-approved messages, specifying which services apply to mass events.	*Conduct training*	Middle	Héctor Fabio Gonzales López/Aliados	07/10/2025	31/12/2025
12	(OM) Extend the process of socializing the PCO test into several sessions, in order to identify and link all the necessary roles within the simulation.	*Conduct training*	Middle	Karen Martínez	10-10-2025	30-10-2026
13	(OM) Document and inventory critical accounts technical accounts in applications to mitigate incident risks in other applications.	*Conduct training*	*Middle*	Ernesto Parra/Fabian	06/10/2025	31/10/2025
14	(OM) Include in the guidelines the performance of at	Simulation Execution 2025	High	Ernesto Parra	10-10-2025	30-03-2026

No.	Finding (Strength/Opportunity for Improvement)	Action to be Executed	Priority	Responsible	Start date	End Date
	least one drill per year for this critical service where the entire team, roles and activities are involved, as well as document response alternatives. Due to criticality and the number of actors involved, additional socialization sessions with leaders (PODs) and allies should be scheduled to ensure alignment and effectiveness in the execution of the exercise.					
15	(OM) Use the alternate communication tool in the same exercise	Use alternative communication tools for future exercises to	Middle	Diana Janeth Gómez	10-10-2025	30-05-2026
16	(OM) to carry out training of the entire technical team that could be in a real incident (There are 7 and the test was attended by only one person).	Conduct training	High	Héctor Fabio Gonzales López /Allies	10-10-2025	30-12-2025
	(OM) Strengthen the training and definition of guidelines for the Digital Service Desk, so that it is clearly established in which cases the IVR must be	Generate training	Middle	Héctor Fabio Gonzales López /Allies	10-10-2025	30-12-2025

No.	Finding (Strength/Opportunity for Improvement)	Action to be Executed	Priority	Responsible	Start date	End Date
	activated, the level of approval to send the unavailability message and timely communicate the type of failure presented.					
	(OM) Extend the process of socializing the PCO test into several sessions, in order to identify and link all the necessary roles within the simulation.		Middle	Diana Janeth Gómez	10-10-2025	30-05-2026
	(OM) Identify and control technical accounts to include them in the list of critical accounts to mitigate risks of incidents with applications.	Control technical accounts	Middle	Ernesto Parra / Diana Janeth Gómez	10-10-2025	30-12-2025
	(OM) Include in the PCO of the service the definition of temporary IPs 10.11.27.*** / 10.11.45.** and cyberark 10.76.184.**, 10.104.**, 10.76.184.***, 10.104.2.** that serves for access by authorized local administrators servers, domain controllers and vCenters. Additionally, take into account the entry of allies from	Include authorized local IPS addresses in PCO Train partners on site-to-site VPN login	Middle	Ernesto Parra/ Fabian Gómez/Diana Janeth Gómez	10-10-2025	30-12-2025

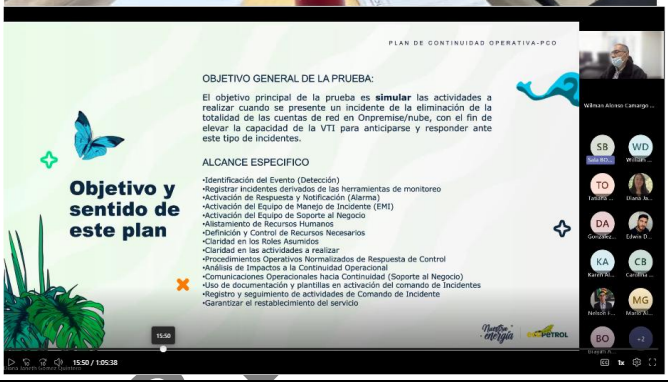
No.	Finding (Strength/Opportunity for Improvement)	Action to be Executed	Priority	Responsible	Start date	End Date
	site-to-site VPNs through dedicated channels					
	(OM) Complement this simulated exercise with the technical exercise of the periodic tests of the Technology Recovery Procedure (PRT) of the Active Directory, which include scenarios of restoration of domain controllers, validation of AD Connect synchronization and verification of the availability of critical accounts, in order to ensure the effectiveness of recovery times and minimize risks in the event of a real event.	PRT 2025 Test Run	Middle	Ernesto Parra /Allies	10-10-2025	31-12-2025

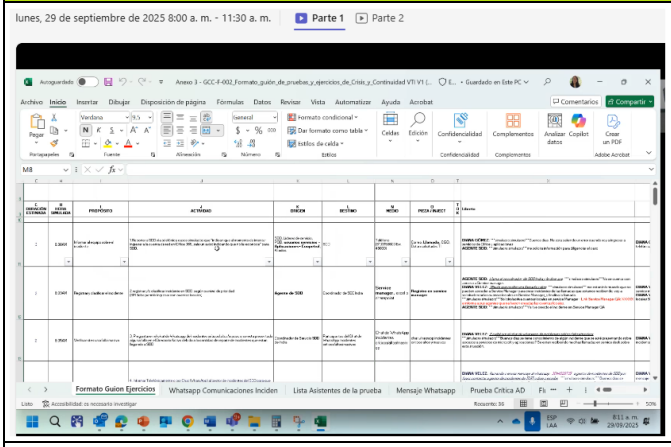
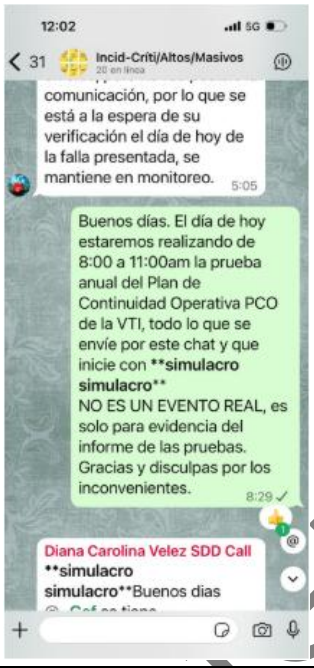
Table 10, Summary of the findings to be managed as a result of the exercise/test.

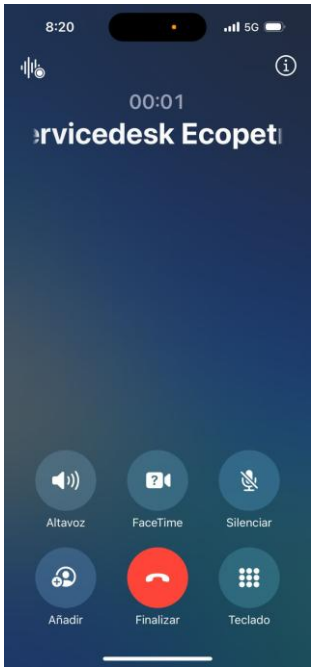
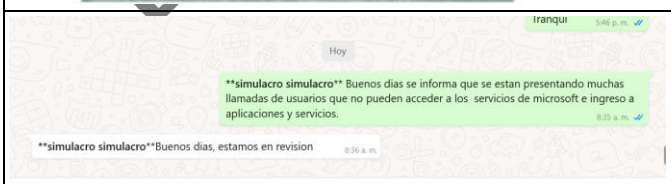
4.3 Other important considerations of the exercise:

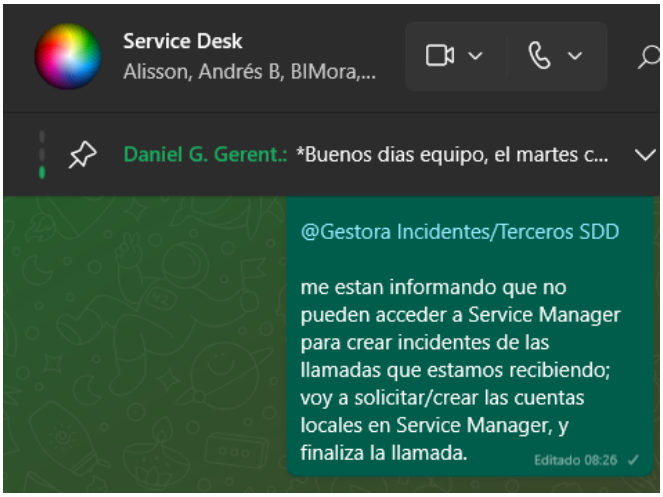
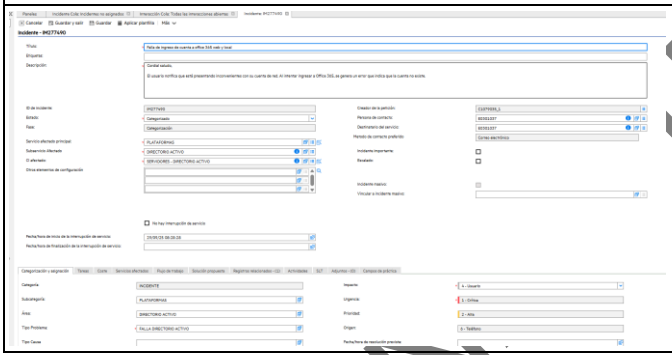
In the development of the exercise, the importance of the active participation of all actors was highlighted, which allowed validating the level of preparation, the commitment of the areas and the ability to react under pressure in real time. Likewise, in the PCO-VTI test, it is concluded that the proposed objective was achieved in accordance with the methodology defined by the Crisis and Continuity area, the PCO of the VTI and the previous planning. The effectiveness of the alternative implemented to address this type of scenario was verified, highlighting the timely management of the event by the VTI staff, the Active Directory Service and the allied managers involved.

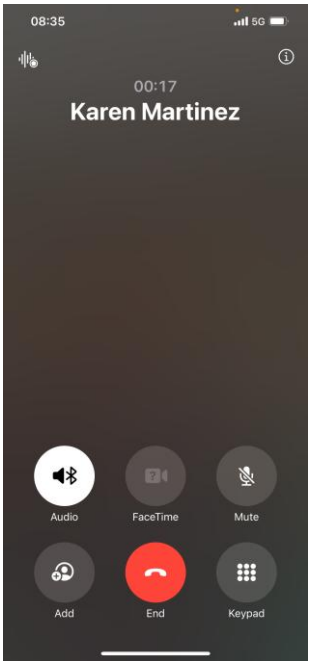
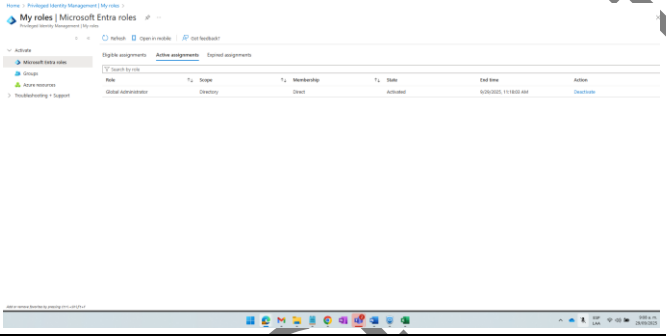
4.4 Photographic Record

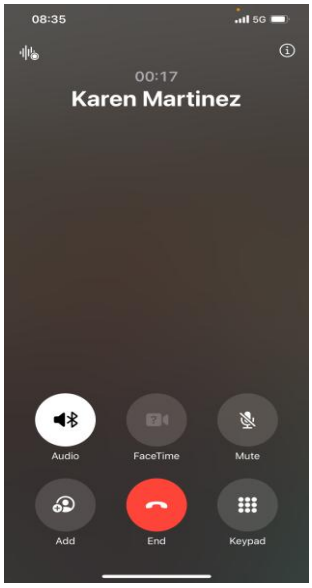
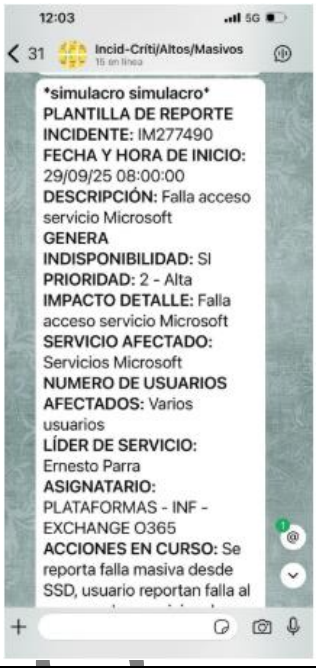
Photographic Record Photograph Description	
 	*Explanation of the scope of the test, premises of the simulated test scenario.*

Photographic Record Photograph Description	
	*Explanation of the context of the script, and the execution of the script begins at 8:11 am.*
	*The Leader of the Continuity practice informs in the WhatsApp chat of (Incid-Criti/Altos/Masivos), informing that the operational continuity plan of the Vice Presidency of Science, Technology and Innovation is being carried out with the message "Simulation Drill that is NOT A REAL EVENT, it is only for evidence of the report of the tests.* *Thank you and apologies for the inconvenience."*

Photographic Record Photograph Description	
	*The Leader of the Continuity practice Report simulated cases to SDD by phone that "indicate that when you try to access the network account in Office 365, a notice comes out indicating that you do not recognize it" for SDD.*
	*Start the Incident Manager of the digital Service desk of the partner Indra, sending a message in the WhatsApp chat of Critical, High and Massive Incidents consulting about the incident reporting on the lack of access to Microsoft services and applications.*
	*The Incident Manager of the digital Service desk of the partner Indra report by Chat (WhatsApp) to the first level of support (Allied Incident Manager) according to the escalation matrix of each Service Provider*

Photographic Record Photograph Description	
	published on the alternate site of the incident practice
	*The Incident Manager of the digital Service desk of the partner Indra informs by Chat (WhatsApp) that they cannot enter Service Manager proceed to activate the local accounts to record and classify the incident*
	*Once logged in with the local accounts, the incident is registered and/or classified with IM277490*

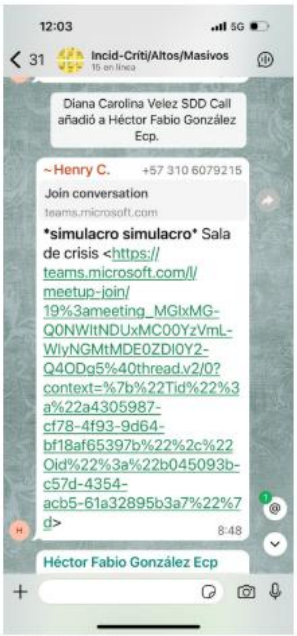
Photographic Record Photograph Description	
	*Ecopetrol's Active Directory Service Leader establishes communication with the TIVIT person on duty for the Active Directory service, in order to detect and confirm the unavailability of the associated network accounts.*
	*The TIVIT Domain Controller Administrator, as shift manager, validates the unavailability of the Active Directory service and confirms that the associated email accounts are not operational. Subsequently, it establishes communication with Ecopetrol's Active Board Service Leader to report the situation and coordinate the corresponding actions*

Photographic Record Photograph Description	
	*Detect and report unavailability of cloud/on-premise network accounts associated with Active Directory*
	*The incident manager of TIVIT PLATAFORMAS makes the first notification, the completion of the template for the first notification in Ecopetrol's WhatsApp incident chat (Incid-Crit/High/Massive)*

Photographic Record Photograph Description	
	*Conversation between Eng. Jaime Malagón, Head of the Platforms and Connectivity Department (Planning Leader) and the Service Leader of the Active Directory of Ecopetrol, about the incident and the first actions.*

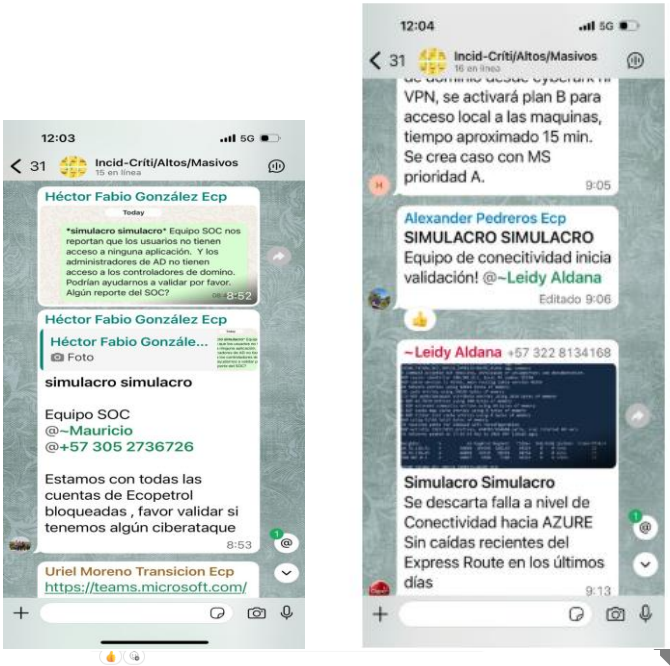
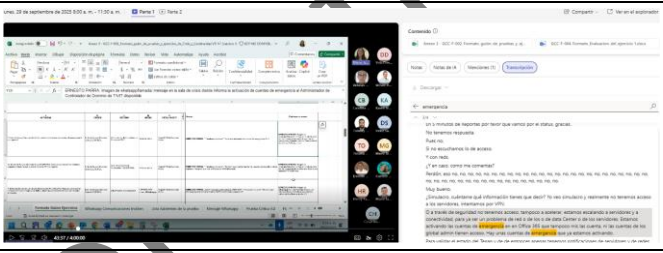
Photographic Record

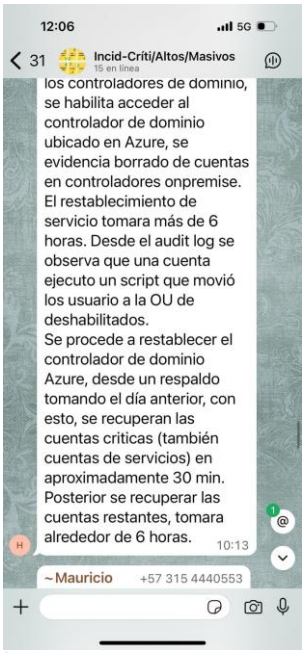
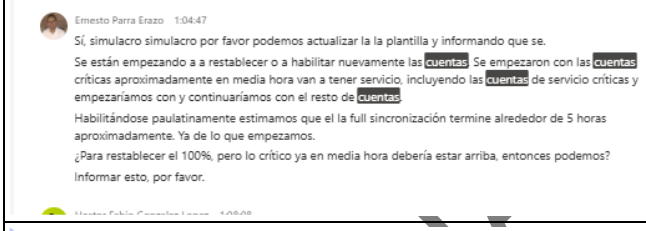
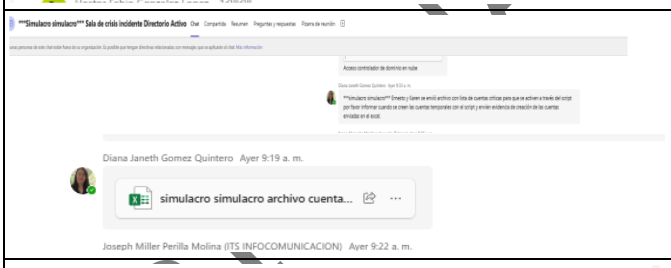
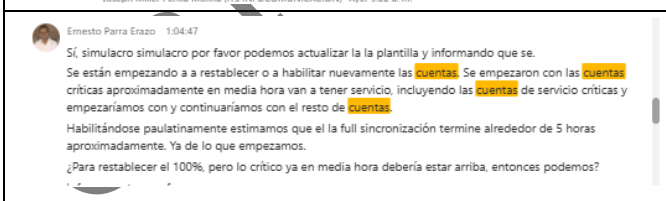
Photograph Description

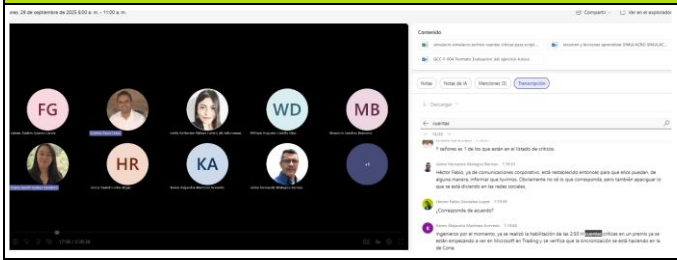
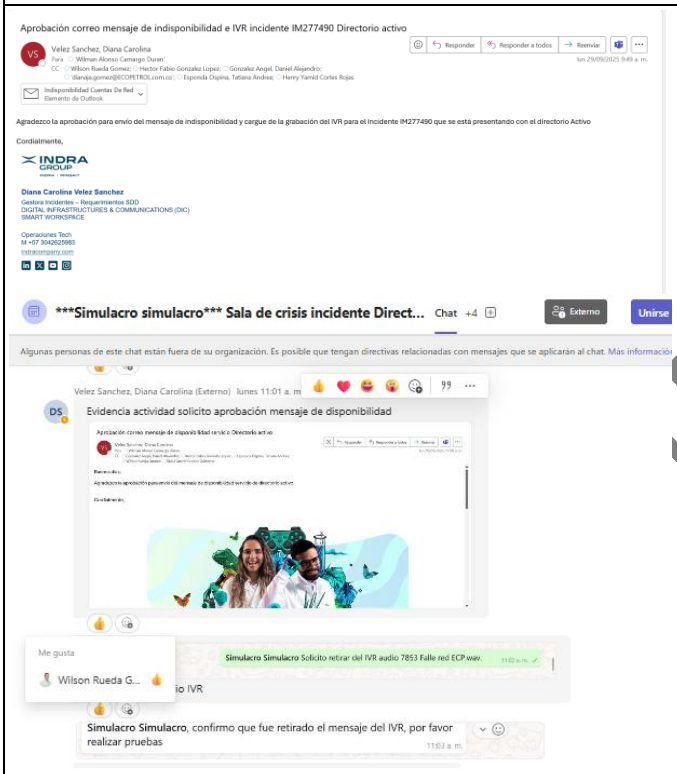
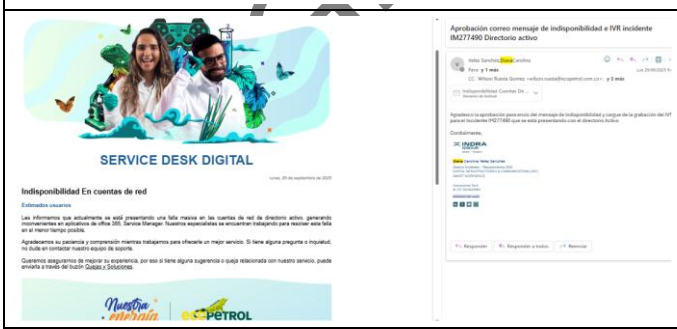


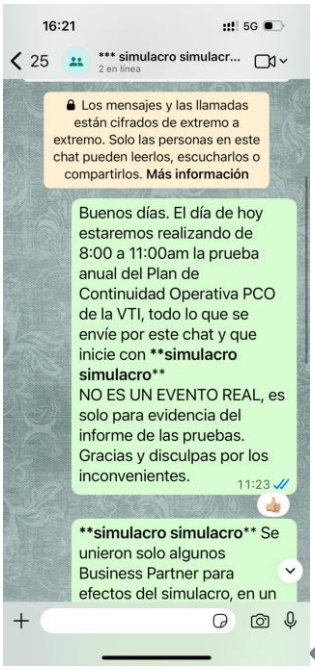
TIVIT's Incident Manager proceeds to create an incident attention room in Teams/Meet without prior scheduling of the agenda, sharing the invitation through Ecopetrol's WhatsApp chat (Incid-Crit/High/Massive). Once the crisis room is enabled, the call to the corresponding team begins immediately, beginning the inquiry into the status of the incident.

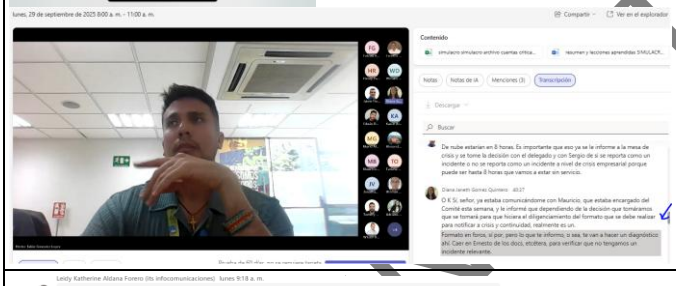
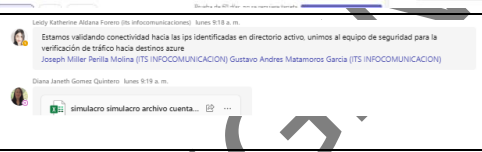
During the development of the session, it is established that the update of the status of the incident must be carried out in accordance with the defined practice.

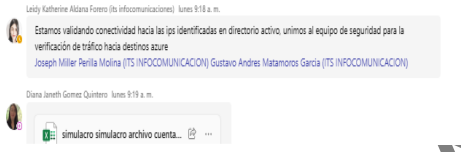
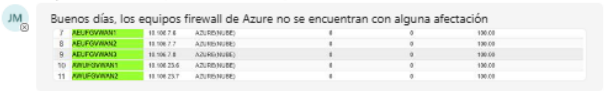
Photographic Record Photograph Description	
	*Inside the Situation Room, different hypotheses are raised and analyzed about the cause of the incident, including the possibility of a cyberattack. As part of the technical validation, the status of the Active Directory server is reviewed and connectivity to the corresponding IP address is confirmed, without evidence of degradation, high response times or latency problems.* *Additionally, it is established that, if required, traffic to a specific destination in Azure will be identified with the support of the Security team. At the same time, a case is registered with Microsoft to have specialized support in the investigation and resolution of the incident.*
	*Ecopetrol's Active Directory Service Leader requests the activation of emergency accounts to TIVIT's Domain Controller Administrator*

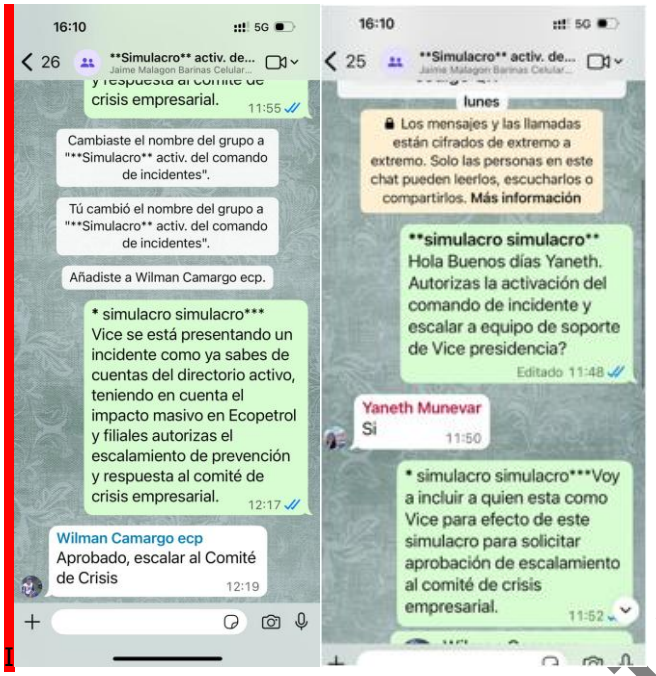
Photographic Record Photograph Description	
 	*In the Situation Room, the Service Leader of ECOPETROL's Active Directory indicates that the solution of the incident requires a time greater than the 4 hours of the service RTO and requests to update the template to the TIVIT PLATFORMS incident manager and notify in Ecopetrol's WhatsApp incident chat (Incid-Crit/High/Massive) with the respective progress.* *Additionally, it requests the critical contact base for businesses and subsidiaries and partners for the creation of temporary manual accounts.* *And requests the activation of the unavailability message*
	*The Leader of the Ecopetrol continuity practice delivers the list of critical accounts of Ecopetrol, subsidiaries and allies to begin reinstatement of the accounts through script.*
	*Proceed to create the accounts of critical Ecopetrol users* *The TIVIT Active Directory Domain Controller Administrator initiates the process of resetting and enabling Active Directory accounts, prioritizing critical accounts and essential service accounts.*

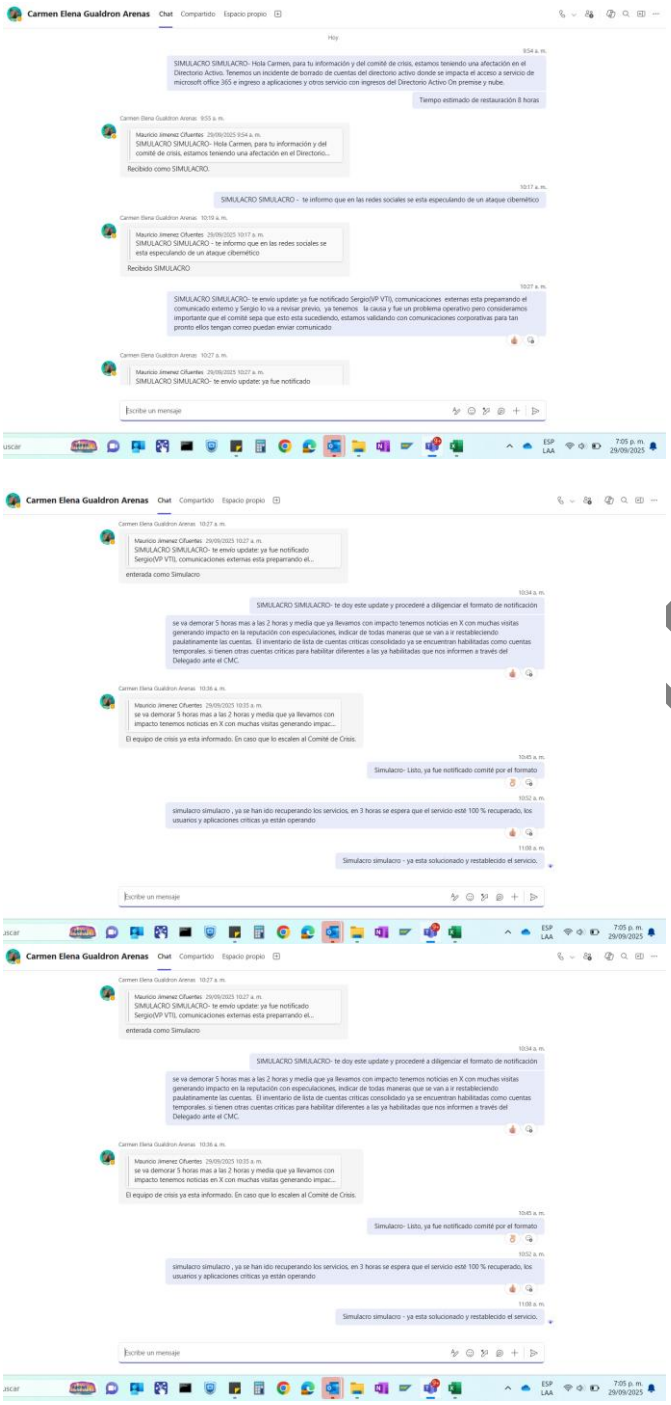
Photographic Record Photograph Description	
	*and notifies that these will be available in approximately 30 minutes. And subsequently, it will continue progressively with the rest of the user accounts.*
	*ECOPETROL's Active Directory Service Leader requested the SDD Leader to send the service interruption message to the entire community and activate the IVR, while SDD Indra's Incident Manager, in conjunction with ECOPETROL's Active Directory Service Leader, verified the pre-approved IVR messages related to the incident and obtained the VoBo from Ecopetrol's SDD Leader (according to the level of approval described in the incident guide).*
	*The respective notification of Unavailability of the service is made*

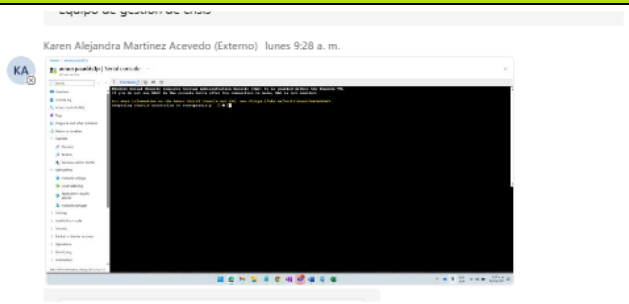
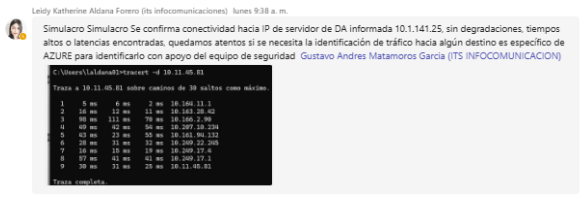
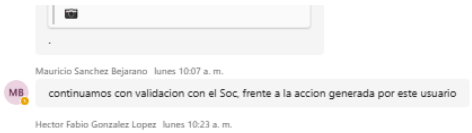
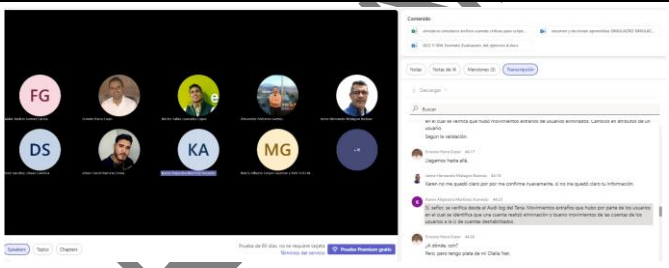
Photographic Record Photograph Description	
	*The IVR message was uploaded to the messaging plant, so that, when communicating to the established line, users are informed in a timely manner about the existence of an incident that affects the Active Directory (AD) service and immediately know the situation without the need to escalate additional queries.*
	*The leader of Ecopetrol's continuity practice creates VTI's Whatsapp chat on the progress of the Incident solution, information for communications with business and subsidiaries*

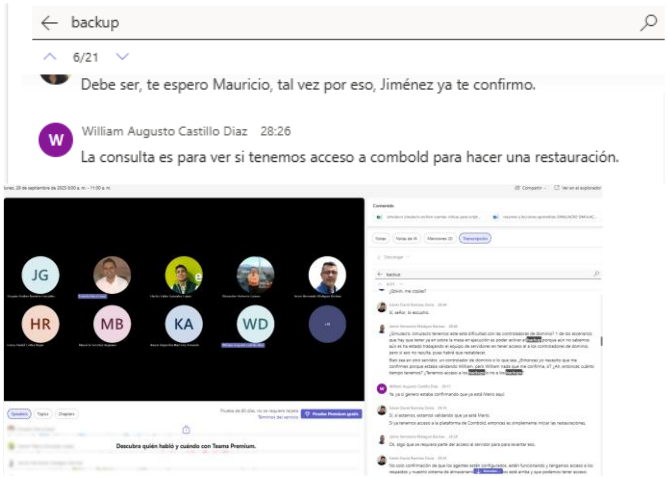
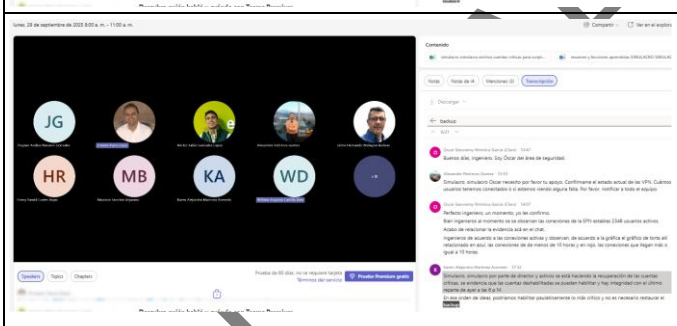
Photographic Record Photograph Description	
	*Ecopetrol's continuity practice leader performs the analysis and proposes the activation of incident command as defined in the PCO and Governance model for IT Continuity when escalation to incident command is required.*
	
	*Eng. Leidy Katherine Aldana Forero performs connectivity validation to AZURE to rule out recent outages of the Express Route in recent days.*

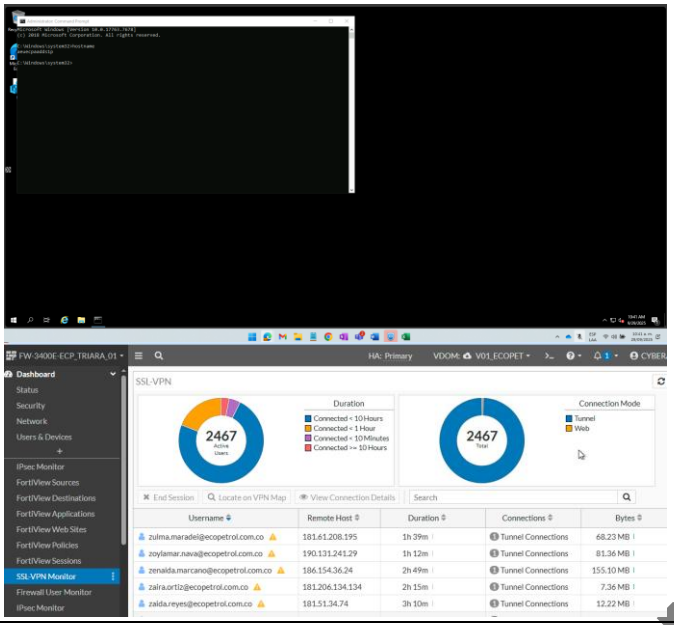
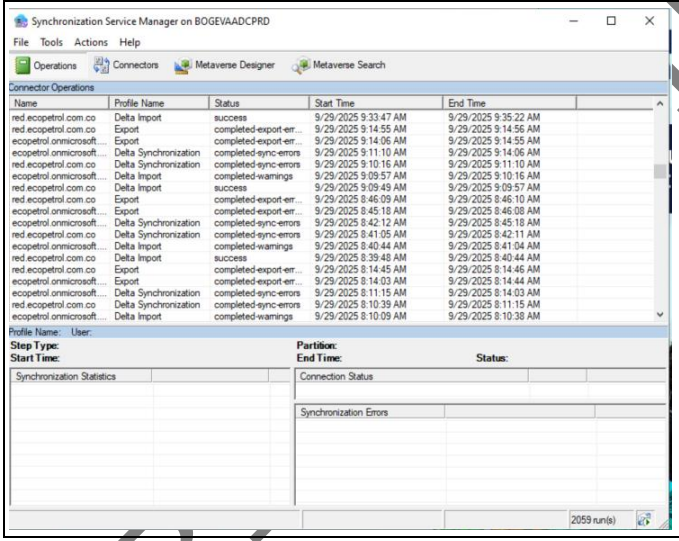
Photographic Record Photograph Description	
	*Eng. Fabian Andrés Gómez performs server validation upstairs with Ms, while the servers are accessed.*
	*Eng. Leidy Katherine Aldana Forero requests to join the security team for the verification of traffic to Azure destinations Eng. Joseph Miller Perilla Molina (ITS INFOCOMUNICACION) Gustavo Andrés Matamoros García (ITS INFOCOMUNICACION)*
	*Eng. Joseph Miller Perilla Molina (ITS INFOCOMUNICACION) Gustavo Andrés Matamoros García (ITS INFOCOMUNICACION) confirm that the Firewall equipment is not affected*
	Mr. Jaime Malagón, Head of the Platforms and Connectivity Department (Planning Leader), Requests the Service Leader of the Active Board of Directors of ECOPETROL to evaluate the root cause in order to take appropriate actions in the case

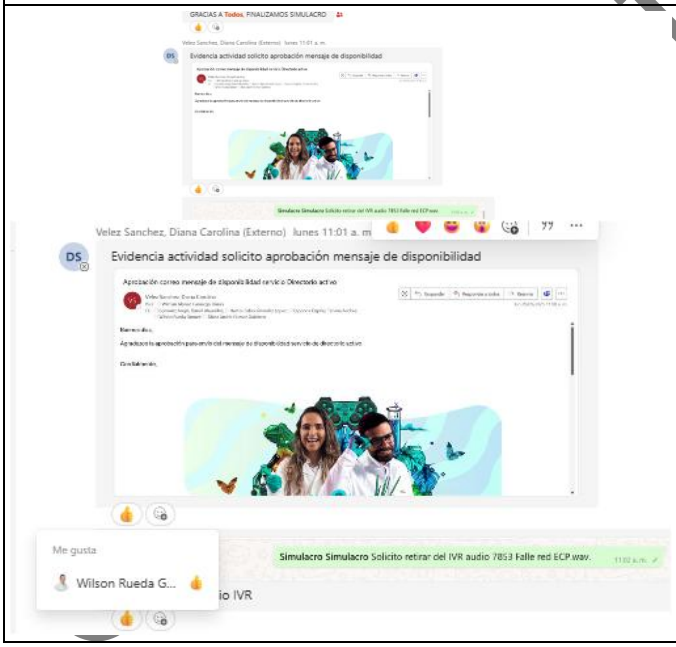
Photographic Record Photograph Description	
	*Confirmation of the approval of the activation of the PCO VTI incident command and approval of who was fulfilling the role of Vice President for information escalation to the committee, although it was not planned to escalate to this level due to the situation presented during the drill, it was decided to escalate to the crisis committee.*
	*Conversation between Eng. Jaime Malagón, Head of the Platforms and Connectivity Department (Planner Leader) and Eng. Yaneth Munévar, informing him of the status of the incident and the progress and actions taken*

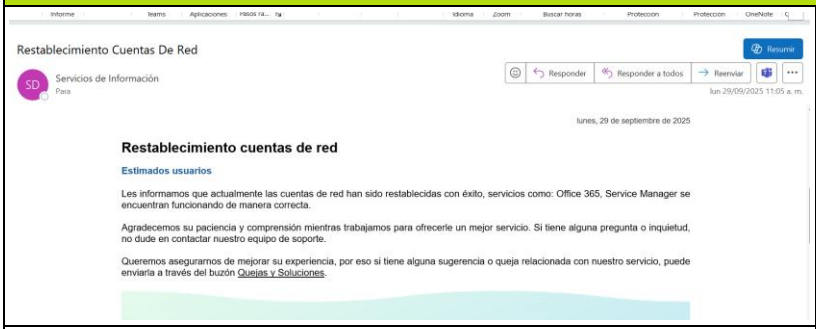
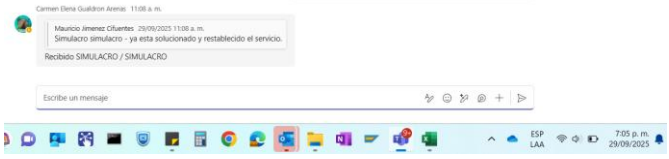
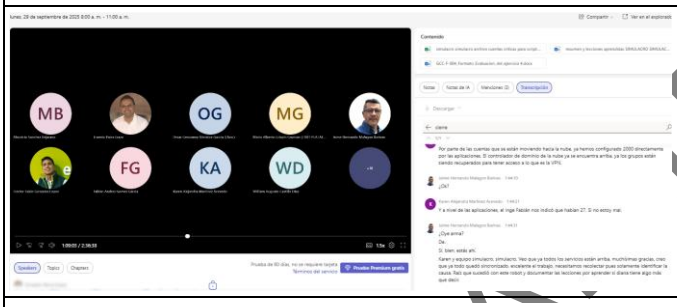
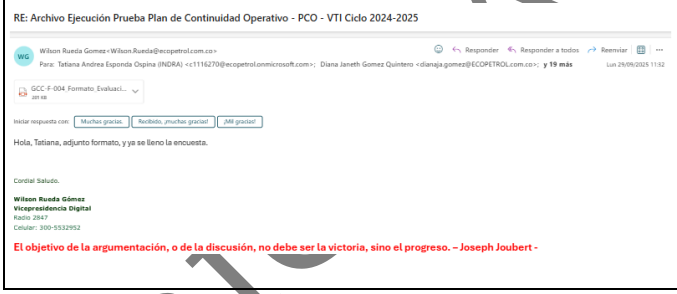
Photographic Record Photograph Description	
	*Communications made during the drill in the role of VTI representative in the crisis committee.*

Photographic Record Photograph Description	
	*TIVIT Active Directory Domain Controller Manager reports that it gains access to the cloud domain controller*
	*Eng. Leidy Katherine Aldana Forero confirms connectivity to the IP informed*
	*Mr. Mauricio Sanchez proceeds to make the respective validations with the SOC, in the face of the action generated by this user*
	*Eng. Hector Fabio Gonzales proceeds to join Eng. Diego Alejandro Rodríguez Rodríguez on the communications side to validate reputational impact and give context on the situation of the incident.*
	*The TIVIT Active Directory Domain Controller Administrator identifies and notifies the root cause where it was verified that through the audit logs of the Tenant system, unusual movements by a User were presented. In particular, it was identified that one account executed the transfer of several user accounts to the "Disabled Accounts" Organizational Unit, which generated the temporary unavailability of these accounts.*

Photographic Record Photograph Description	
 No activar Backup	*During the exercise, TIVIT's Active Directory Domain Controller Administrator initially informed the need to activate Active Directory Backup and requested the Backup Team to recover on-premise. However, it was evident that such restoration was not necessary, since the recovery of critical accounts was being executed from Active Directory.* *Likewise, it was verified that the disabled accounts could be enabled and that there was integrity with the last backup made the day before at 6:00 p.m. Consequently, it was determined that it is possible to gradually enable critical accounts without requiring a full backup restore.*
	*Due to the operational decision made during the year, a new strategy was defined that made restoring from backup unnecessary. As a result, it was not necessary to generate the backup request task in Service Manager for the Backups team, nor to create or delete temporary accounts, since the restored accounts corresponded to the primary accounts and not temporary accounts.*

Photographic Record Photograph Description	
	*The previous activity was replaced by the TIVIT Active Directory Domain Controller Administrator performed the Permissions Verification and confirmed that the person responsible for the operation had domain administrator privileges to perform enablement. Subsequently, I perform the Enablement in AD OnPremise by accessing Active Directory Users and Computers (ADUC) and located the disabled accounts within the corresponding OU, once located, proceeds to enable the critical accounts and their properties (password, groups, expiration policies) were reviewed.*
	*Validation of the synchronization and replication process of Domain controllers and validation of ADConnect, email accounts*

Photographic Record Photograph Description	
	*Perform analysis of the actions taken in the cloud to solve the incident, Confirm operational service and close incident in the chat of critical/high/massive incidents.*
	*The TIVIT Incident Manager makes the message about the return to normality of the incident and obtained the VoBo from Ecopetrol's SDD Leader (according to the level of approval described in the incident guide).*

Photographic Record Photograph Description	
	*The Indra Incident Manager proceeds to inform the Ecopetrol user community of the availability of the network accounts associated with the Active Directory and remove IVR messages from the communications equipment plant*
	TIVIT incident closure in SM
	*Report deactivation of PCO-VTI preventively and return to normality.*
	*Closing of the VTI Operational Continuity Plan Test*
	*The corresponding survey was carried out to identify lessons learned derived from the result of the test, in accordance with the GCC-F-004_Formato_Evaluacion_del_ejercicio format.*

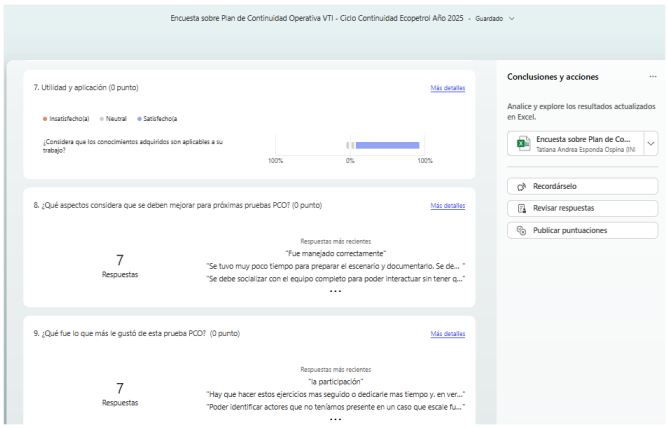
Photographic Record Photograph Description	
	*The PCO-VTI test feedback session was held for the participants, in order to review results, findings and opportunity for improvement focused on socialization of the exercise through a Microsoft Forms form.*

Table 11, Photographic record of the exercise,

5. ANNEXES

1. Annex 1. GCC-F-001_Formato_Plan_Del_Ejercicio
2. Annex 2. GCC-F-002_Formato_guión_de_pruebas_y_ejercicios_de_Crisis_y_Continuidad
3. Annex 3. GCC-F-003_Formatos_de_observador_del_ejercicio-test
4. Annex 4. GCC-F-004_Formato_Evaluacion_del_ejercicio
5. Annex 5. GCC-F-005_Informe_del_ejercicio-prueba_V4

Electronically reviewed by:	Electronically approved by:
JAIME HERNANDO MALAGÓN BARINAS **Head of Platforms and Connectivity Department** **Citizenship Card No. 11.185.568** **Vice-Presidency of Science, Technology and Innovation**	**YANETH MUNEVAR CENDALES** **Digital Infrastructure Manager** **Citizenship Card No.52.492.372** **Vice-Presidency of Science, Technology and Innovation**
Electronically signed document, in accordance with the provisions of Decree 2364 of 2012, which regulates Article 7 of Law 527 of 1999, on electronic signatures and other provisions are issued. *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 such a report from Service Desk.*	