1. OBJECT

Guarantee attention to security incidents that compromise the confidentiality, integrity, and availability of the information of Transportadora de Gas Internacional S.A. ESP. This procedure establishes the necessary actions to guarantee the identification, analysis, containment, eradication, and subsequent actions that are required to carry out timely attention to information security incidents that arise and thus minimize the risk of theft or leak. of information.

2. REACH

Incident management begins its cycle when the information security incident is identified and recorded and ends when the service is resolved and restored. The management of information security incidents deals with all those events that involve or may affect the confidentiality, integrity, and/or availability of the services provided to Transportadora de Gas Internacional S.A. ESP.

3. DEFINITION OF TERMS

3.1 RISK ACCEPTANCE: The informed decision to take a particular risk.

3.2 ACTIVE: Any element that has value for the organization and that the following is considered for Information Security Risk Management: networks, hardware, information, location, personnel, business processes and activities, software, and organizational structure.

3.3 THREAT: Potential cause of the unwanted incident, which may result in damage to the system or the Organization.

3.4 ANOMALY: Deviation or discrepancy from a rule or usage. (RAE).

3.5 SERVICE LEVEL AGREEMENTS: It is an agreement between an IT service provider and a customer. The SLA (Service Level Agreement) describes the IT service, documents the service level goals, and specifies the responsibilities of the IT service provider and the customer. A single SLA can cover multiple IT services or multiple clients.

3.6 CAUSES: The reason why an event happens, and its identification depends on the experience level of the environment and the elements involved.

3.7 CONFIDENTIALITY: Ownership of information that prevents it from being disclosed to unauthorized individuals, entities, or processes.

3.8 CONSEQUENCES: Result of the event that can be certain or uncertain and have positive or negative effects for the entity and that can be expressed in qualitative or quantitative terms. An initial consequence may have a greater impact considering the secondary effects.

3.9 AVAILABILITY: Information being accessible and usable at the request of an authorized entity.

3.10 EVENT: A significant status change for the issue of a configuration item or IT service. The term “event” is also used as an alert or notification created by an IT service, configuration item, or monitoring tool. Events typically require action by IT operations staff and often lead to the logging of Security Incidents.

3.11 INCIDENT RESPONSE GROUP (GRI): It refers to the specialized group that is formed to attend to security incidents. This group will be confirmed by the TGI Security Officer, Indra's security leader, i-CSOC specialists, and all those people who are required (by any of the three parties) to solve the security incident. The GRI is coordinated by Indra's security leader.

3.12 IMPACT: The impact and urgency are used to calculate priority. The impact is based on the level of the business impact of the problem.

3.13 INCIDENT: Event that is not part of the standard operation and functioning of a service and that can cause an interruption or reduction in its quality.

3.14 SECURITY INCIDENT: Security events generated in the operation and functioning of the services that affect the integrity, confidentiality, and/or availability of the information.

3.15 INTEGRITY: Accuracy and completeness of information.

3.16 ISO27001:2013: ISO/IEC 27001:2013, *Information security management systems — Requirements*

3.17 MSPI: Information Security and Privacy Model-MSPI

3.18 MONITORING: Ongoing verification, supervision, critical observation, or determination of status to identify changes from the required or expected level of performance.

3.19 PRIORITY: It is based on impact and urgency, and is used to identify the time required to execute the actions that must be taken in an Incident.

3.20 **ASSET OWNER:** Person or position that administers, authorizes the use, regulates or manages the information asset. The asset owner approves the required level of protection against confidentiality, integrity and availability. Person or position that administers, authorizes the use, regulates, or manages the information asset. The asset owner approves the required level of protection against confidentiality, integrity, and availability.

3.21 **PROBLEM:** Repetitive or high-impact security incidents and the causes that originate them are unknown. Failures in configuration elements that intervene in the provision of the service are also considered security incidents.

3.22 **RECORD:** A document that contains the result or other type of output from a process or activity. Records are evidence that an activity took place, and could be in paper or electronic format.

3.23 **RISK:** Effect of uncertainty on objectives. An effect is a deviation from what is expected, be it positive, negative, or both. The objectives can have different aspects (economic, image, environmental) and can be applied at different levels (strategic, operational, or the entire organization).

3.24 **URGENCY:** Indicates how pressing the issue is to the recipient of the service. Urgency and impact are used to calculate priority.

3.25 **VULNERABILITY:** Weakness identified on an asset that can be exploited by a threat to affect the confidentiality, integrity, and/or availability of information.

4. DEVELOPMENT OF ACTIVITIES

ACTIVITY WHAT	HOW/WHERE	RESPONS. WHO	CHECKPOINTS	REGISTRATION
4.1 Anomaly report	All workers, contractors, lawyers, interns, SENA trainees, control entities, and other third parties that have access to or use any TGI information asset must report any anomaly related to the issues described within the guidelines and policies of the MSPI.	Employee, contractor, lawyer, trainee, SENA apprentice, control entities, and other third parties that have access or use of any TGI information asset.	Policy and guidelines documents	Report of IT events in the Service Desk tool
4.2 Service Desk	The Service Desk validates whether the reported anomaly classifies as an information security event, in which case it must be registered as such and assigned to the Information Security Incident Response Team. (i-CSOC). If the event is classified as an information security incident, go to point 4.4. Otherwise, go to activity 4.3.	Service Desk Analyst	Policy and guidelines documents P-ADI-022 Service desk	Report of IT events in the Service Desk tool
4.3 Classification as an IT requirement	If the anomaly is not classified as an information security event, the Service Desk analyst who received the case records it in the request management tool as a normal IT requirement. This procedure ends.	Service Desk Analyst	Policy and guidelines documents	Report of IT events in the Service Desk tool
4.4 Assess the incident	When a security incident is received from the Service Desk or a Security Event is reported by security monitoring tools, i-CSOC analysts must analyze the incident to assess whether it is associated with security issues or belongs to other IT outsourcing services. Additionally, the affected services, the impact, and the scope of the incident must be determined to establish the impact and urgency of attention to it.	i-CSOC Analyst		N/A

ACTIVITY WHAT	HOW/WHERE	RESPONS. WHO	CHECKPOINTS	REGISTRATION
4.5 Validate if it is a False Positive	If it is a false positive, go to activity 4.6. If it is not a false positive, go to activity 4.7.	i-CSOC Analyst		N/A
4.6 Document the incident as a false positive	If the initial report is a false positive, the incident is documented and activity 4.28 is passed.	i-CSOC Analyst		Documented in Service Manager
4.7 Is it a security incident?	If it is a security incident, go to activity 4.8. If it is not a security incident, go to activity 4.29	i-CSOC Analyst		
4.8 Is it registered in the service desk tool?	If it is registered, go to activity 4.10. If it is not registered, go to activity 4.9.	i-CSOC Analyst		
4.9 Request registration by the Service Desk	If the incident has been detected by the i-CSOC security monitoring tools, the Service Desk is requested to generate the security incident and assign it to the i-CSOC.	i-CSOC Analyst	P-ADI-022 Service desk	Case registered in the Service Desk tool
4.10 Analyze and define the root cause	An analysis of the incident is carried out with the information available to establish the causes that are originating it.	i-CSOC Specialist		
4.11 Can it be fixed?	If the specialist can solve the incident, go to activity 4.12. If the specialist cannot solve the incident, go to activity 4.14	i-CSOC Specialist		
4.12 Define and implement containment/ Eradication actions	The Specialist establishes the necessary actions to solve the incident. It is important to assess the risks before the implementation of the actions and the rollback process in case they do not work. When the actions to be implemented require modification in the configuration of the platforms, the respective emergency change control must be generated and submitted to the change committee for approval. It is also important to take into account that, if an initial solution is not evident, containment activities must be carried out while the incident is analyzed in depth.	i-CSOC Specialist	P-ADI-020 Information technology change management	Emergency change control
4.13 Is the Solution effective?	If the solution is effective, go to activity 4.23 If the solution is not effective, go to activity 4.14.	i-CSOC Specialist		

ACTIVITY WHAT	HOW/WHERE	RESPONS. WHO	CHECKPOINTS	REGISTRATION
4.14 Notify IT Outsourcing Security Lead	If the activities carried out to remedy the incident are not effective, the IT outsourcing security leader is notified to assess the situation and, if necessary, convene the Incident Response Group.	i-CSOC Specialist		
4.15 Convene the Incident Response Group	If the implemented solution is not effective, it is escalated to the Security Incident Response Group. The GRI will be made up of the TGI Security Officer, the IT outsourcing security leader, i-CSOC and/or IT outsourcing specialists, and affected service providers; among others, to jointly seek a definitive solution to the reported incident. The conformation of the GRI will be conditioned to the type of security incident to be solved.	IT Outsourcing Security Leader		Meeting format Minutes of Conclusions
4.16 Investigate and Diagnose	The GRI verifies the actions carried out, and a more specialized root cause analysis establishes an action plan to be implemented.	Incident Response Group		
4.17 Contain and Eradicate	The GRI implements the actions to eradicate the incident. The risks must be taken into account in the implementation of the actions and the rollback process in case it does not work. When the actions to be implemented require modification in the configuration of the platforms, the respective emergency change control must be generated and submitted to the Change Committee for approval.	Incident Response Group	P-ADI-020 Information technology change management	Emergency change control
4.18 Is the Solution effective?	If the solution is effective, go to activity 4.23. If the solution is not effective, go to activity 4.19.	Incident Response Group		
4.19 Is it required to activate the DRP?	If it is required to activate the DRP, go to activity 4.20. If it is not required to activate the DRP, go to activity 4.16.	Incident Response Group		
4.20 DRP activation approved?	If activation is required, go to activity 4.21 If activation is not required, go to activity 4.23	TGI IT Director		
4.21 Request to activate DRP-affected service	If the DRP of the affected service is authorized to be activated, the continuity manager will be contacted so that the actions to activate this plan can be coordinated through that agency.	Security Incident Response Group		Meeting format Minutes of conclusions
4.22	Activate the DRP	DRP TGI Leader	Disaster Recovery Plan	Minutes / Statement of the decision

ACTIVITY WHAT	HOW/WHERE	RESPONS. WHO	CHECKPOINTS	REGISTRATION
4.23 Restore Normal Operation	Once the incident has been resolved, and if contingency and/or recovery activities (DRP) have been carried out, the affected services are restored to normal operation.	Incident Response Group		
4.24 Is an investigation of the incident necessary?	Once the incident has been resolved, the GRI will determine whether it is necessary to carry out an investigation that may lead to forensic analysis.	Incident Response Group		Meeting format / Minutes of conclusions
4.25 Execute evidence collection procedure	The evidence collection procedure is executed to start the investigation and/or forensic analysis. POST / TICKET TRACEABILITY	i-CSOC Specialist	P-ADI-034 Collection of digital evidence	F-ADI-066 Forensic Evidence Extraction F-ADI-068 Chain of Custody Label Continuity Record
4.26 Generate the Report	Details of the incident and remedial actions are presented as part of the monthly information security management report.	i-CSOC Specialist		Monthly Security Management Report
4.27 Document the Incident	The actions taken to mitigate the security incident are documented in the management tool. If an investigation of the security incident was generated, the respective Report must be attached to the ticket in the service desk tool.	i-CSOC Analyst	F-ADI-071 Information Security Incident Report	Documentation of the incident in the management tool
4.28 Change incident status to Resolved	The status of the incident is changed to "resolved", indicating that its management has been completed and it has been completely resolved. This procedure ends.	Analyst i-CSOC		
4.29 Return the event to the service desk process.	If the assigned incident is not security but belongs to one of the IT outsourcing operation services, the incident will be redirected so that it is managed by the corresponding attention group. This procedure ends.	Analyst i-CSOC		Service Desk Procedure

NOTE:
It is the responsibility of each worker, contractor, lawyer, trainee, SENA apprentice, control entities, and other third parties that have access or use of any information asset of TGI S.A. ESP, to timely report as an information security event any type of non-compliance detected with the guidelines and procedures of the company's MSPI, as well as any anomaly that could be considered as the basis of an information security incident.

When information security incidents or events occur, they must be reported promptly, per what is defined in this procedure.

For all incidents, they must be registered in the IT service management tool, they must be categorized, and their impact analyzed and escalated to provide a solution.

Security incidents must be documented and classified according to the activities defined in this procedure.

When an incident occurs, it must be reported following the escalation matrix. The Security leader will decide whether to convene or not the incident response group.

During the analysis of the reported security incidents, it must be identified which ones will be escalated and contact the authorities, consulting the Contacts with Authorities and Interest Groups procedure, if the situation warrants it.

All events that are identified through monitoring and review of event records that put the integrity, availability, or confidentiality of any information asset at risk, must be reported under this procedure.

In cases where it is necessary to collect and preserve the evidence of the investigations carried out during the analysis of an information security incident, this activity must be carried out following what is indicated in the P-ADI- procedure 034 Collection of Digital Evidence.

Observed or suspected information security weaknesses in the information systems or services of TGI S.A. ESP., that affect the confidentiality, integrity, or availability of the information, under this procedure, must be reported on time.

REFERENCED DOCUMENTS

- I-ADI-027 Contacto con autoridades y grupos de interés. (Contact with authorities and interest groups)
- P-ADI-020 Gestión de cambios de tecnología de información. (Information technology change management)
- P-ADI-022 Mesa de servicio. (Service Desk)
- P-ADI-034 Recolección de evidencia digital. (Digital Evidence Collection)

ANNEXES

F-ADI-071 Reporte Incidentes de Seguridad de la Información

Elaboró: VTR / María J. Carrillo P.
Revisó: VTR / Maria J. Carrillo P.
Aprobó: VTR / / Edwin J. Alvarez J.

Produced by: VTR / María J. Carrillo P.
Reviewed: VTR / Maria J. Carrillo P.
Approved: VTR / / Edwin J. Alvarez J.