Information Security Awareness Program

Transportadora de Gas Internacional S.A ESP

January 2022

DOCUMENTO/ ARCHIVO	
Código:	
Nombre Archivo:	Programa de concientización en seguridad de la información
Fecha:	21/01/2022
Versión:	1

REGISTRO DE CAMBIOS			
Versión	**Páginas**	**Fecha Modificación**	**Motivo del cambio**
1	7	07/01/2022	Elaboración del documento

CONTROL DE DOCUMENTOS			
Versión	**PREPARADO**	**REVISADO**	**APROBADO**
1	**Alejando Jiménez** Líder de Seguridad	**Aura M. Pinto** Líder Seguridad	**Lina Montenegro** Gerente de Servicios

Índice

Table Index

None found.

Graphics Index

None found.

1 Objective

Promote a continuous and controlled information security culture, where all members of TGIS.A. ESP, contractors, and third parties understand the importance of it, according to technological advances and emerging threats, and are aware of their responsibility to protect the confidentiality, integrity, and availability of information assets both physically and in cyberspace.

2 Reach

The awareness program is designed to sensitize all members of TGIS.A. ESP, contractors and third parties on computer security and/or cybersecurity in accordance with the provisions of annex 7 number 9.1.18 of the full outsourcing contract for the services provided to Transportadora de Gas Internacional. Likewise, raise awareness among all Indra personnel who are part of the contract.

3 Definitions and Acronyms

3.1 Definitions

N/A.

3.2 Acronyms

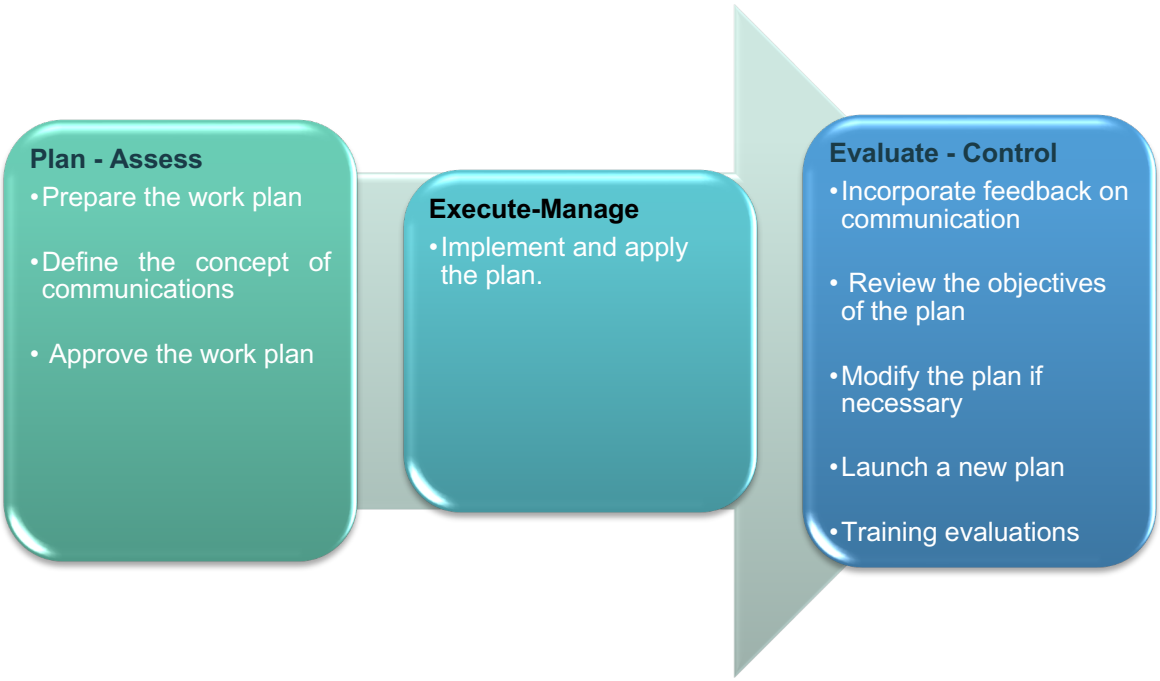
- **TGI:** Transportadora de Gas Internacional S.A ESP

4 Reference Documents

- N/A

5 Strategy

The phases of the defined strategy (Plan - Assess, Execute - Manage and Evaluate - Control) and the activities considered are presented below:



5.1 Plan – Assess

For this phase, the following activities will be considered:

5.1.1. Prepare the Work Plan

In order to carry out any information security plan, the work team must review the criteria and topics to be shared within the target audience, for this the following phase activities must be carried out:

- Review the policies and guidelines defined within the organizations as the central axis of awareness.
- Carry out a preliminary survey of information to analyze the most common problems and incidents that arise in information security issues.
- Analyze current trends used by attackers.
- Develop and define the proposal of the awareness plan based on the result of the analysis of the previous points.

5.1.2. Define the Concept of Communications

Communications are a key aspect of awareness programs. Effective communications planning is of decisive importance to obtain the expected results. Program managers must use the necessary resources to ensure that the people involved in or affected by the program receive the necessary information (ie the message) at the right time and in the right way. In accordance with the above, it is proposed to carry out the socialization using different means such as: email messages, contests and awards ceremonies, messages on company screens, publication of news on the intranet, training in good practices aligned with the regulations and security model, and infographics among others.

5.1.3. Approve the Awareness Plan

Once the awareness plan has been defined, it will be presented to TGI Security and Communications and also to Organizational Change Management for its dissemination and to

generate approval, taking into account that it is aligned with the good practices defined by TGI and in accordance with the contract.

5.2 Execute – Manage

Once the plan has been prepared and approved and taken into account the necessary considerations for its implementation with the appropriate resources, it will be executed to obtain the expected results. The publication will be made to TGI officials and within Indra and will be escalated to Organizational Change Management so that its publication can be managed.

The dissemination will be carried out monthly, dealing with different topics during each month, taking into account the results obtained from the analysis carried out in the monthly preparation phase.

For the proposed work plan, the following media will be used as a basis for dissemination and remembrance: email messages, videos, contests and awards ceremonies, messages on company screens, publication of news on the intranet, and others that are considered relevant. An information security and cybersecurity day will be included in this plan once a year.

5.3 Evaluate – Control

5.3.1. Incorporate feedback on communication

Feedback received on the delivery of planned communications needs to be reviewed to consider ways to improve and make communications more effective in the future.

5.3.2. Review Plan Objectives

The plan objectives should be reviewed given the results from the point of view of effectiveness. What has the team achieved? Have the recommendations materialized? If the objectives have not been achieved, what must be done to achieve the desired results? Or, is it necessary to modify the objectives?

5.3.3. Plan Effectiveness

The verification of the plan's effectiveness is accomplished through its result in delivering the pieces each month and strengthening what has been taught through the reports of security incidents by TGI officials carried out through the service desk. Training is also included annually within the program in different areas, and at the end of the session, an evaluation of knowledge and training is made.

5.3.4. Modify the Plan if Necessary

The experiences obtained and the progress in the way that computer attacks are carried out since the implementation of the plan offer knowledge and ideas to make the necessary modifications in order to achieve better results. If necessary, the activities and tasks carried out should be modified. The key is to make changes without losing sight of the goals and objectives of the plan.

5.3.5. Launch a New Plan

If modifications are made to the plan based on the conclusions drawn, the next step is to reactivate it and carry out the tasks described in the Execute - Manage phase. This step provides a unique opportunity to follow up on other topics or reinforce those included in earlier stages.

5.3.6. Follow Up

Biweekly monitoring will be carried out through security monitoring sessions, where the status of design and delivery of messages by email, videos, contests, awards ceremony, messages on company screens, or news publications on the intranet will be reported. And it will remain as support in the follow-up minutes.

6 Activities

The awareness plan is proposed taking into account the problems evidenced in the initial phase of information gathering and according to the current trends of this year.

7 Annexes

1. Cronograma de concientización 2022.xls