Internal Audits for the supervision of Cybersecurity

Aspects

1 Context

2 Guiding Framework

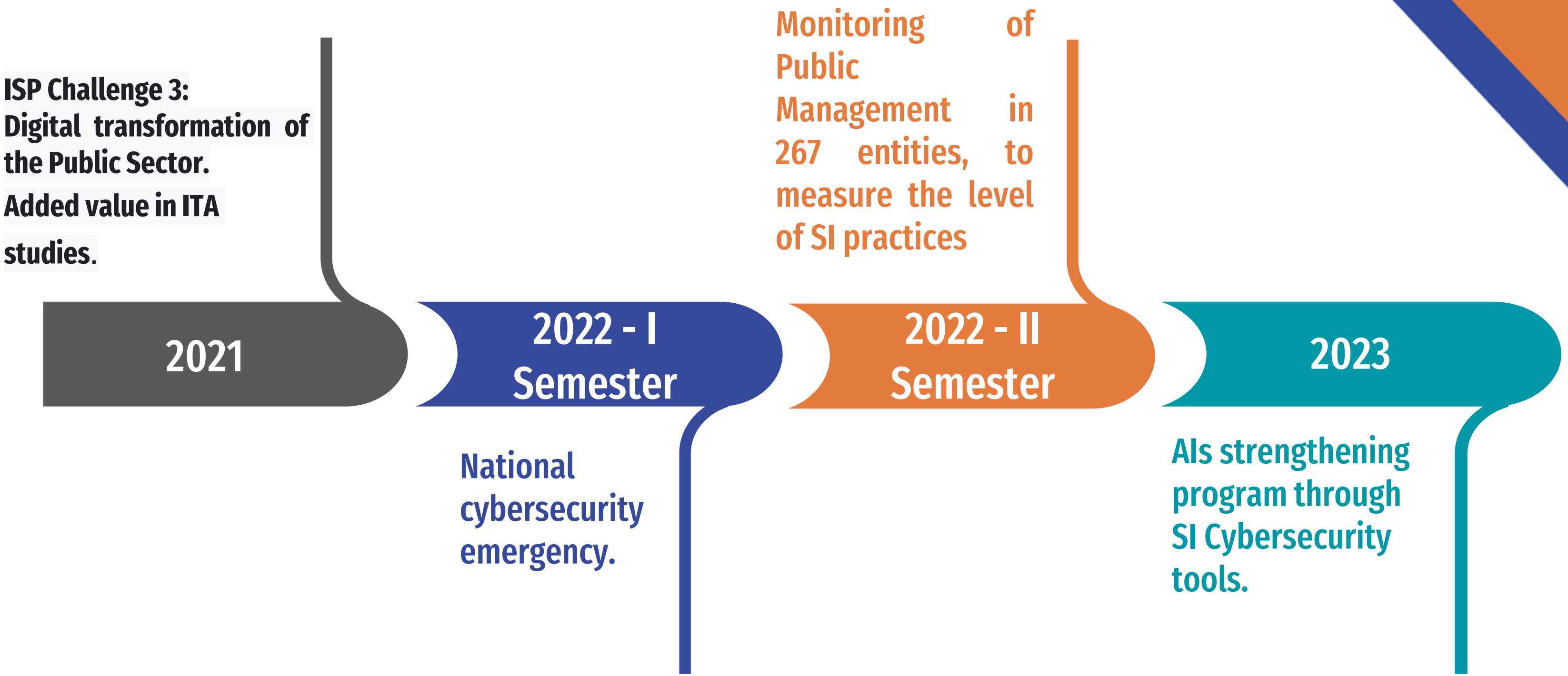
3 Diagnosis

4 Strategy

5 Tools

6 Learning

Context



ISP Challenge 3:
Digital transformation of the Public Sector.
Added value in ITA studies.

2021

2022 - I Semester

National cybersecurity emergency.

Monitoring of Public Management in 267 entities, to measure the level of SI practices

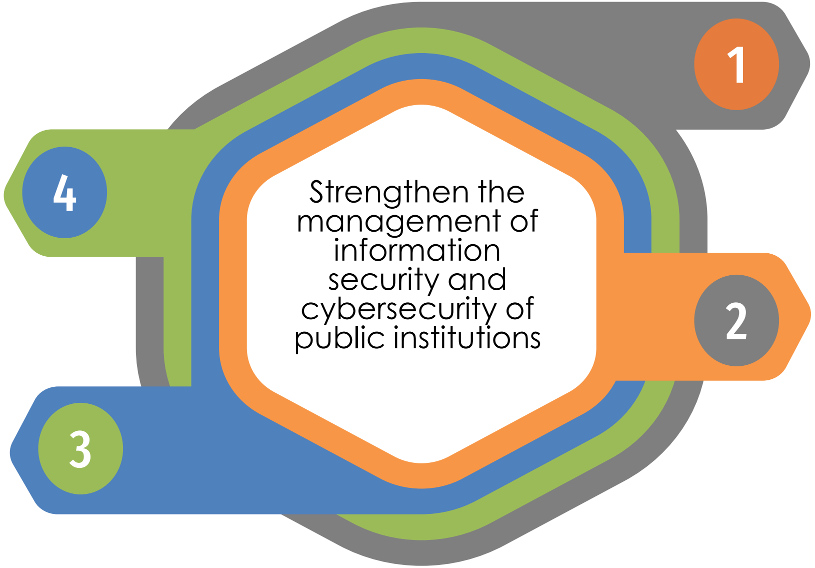
2022 - II Semester

2023

AIs strengthening program through SI Cybersecurity tools.

ISP: Institutional Strategic Plan
ITA: Information Technology Audits
SI: System Information

Guiding framework



Strengthen the management of information security and cybersecurity of public institutions

1 Develop and share agile, adaptable and simple tools to audit information security with an emphasis on cybersecurity

2 Create an impact of awareness about the importance that AIs have in reasonably ensuring the continuity of your entity's services.

3 Use and apply the developed tools

4 02/05/2023 to 30/10/2023

Initial diagnostic

1. Studies carried out by the Internal Audits, period 2021-2023

2. Training level and staff with certifications.

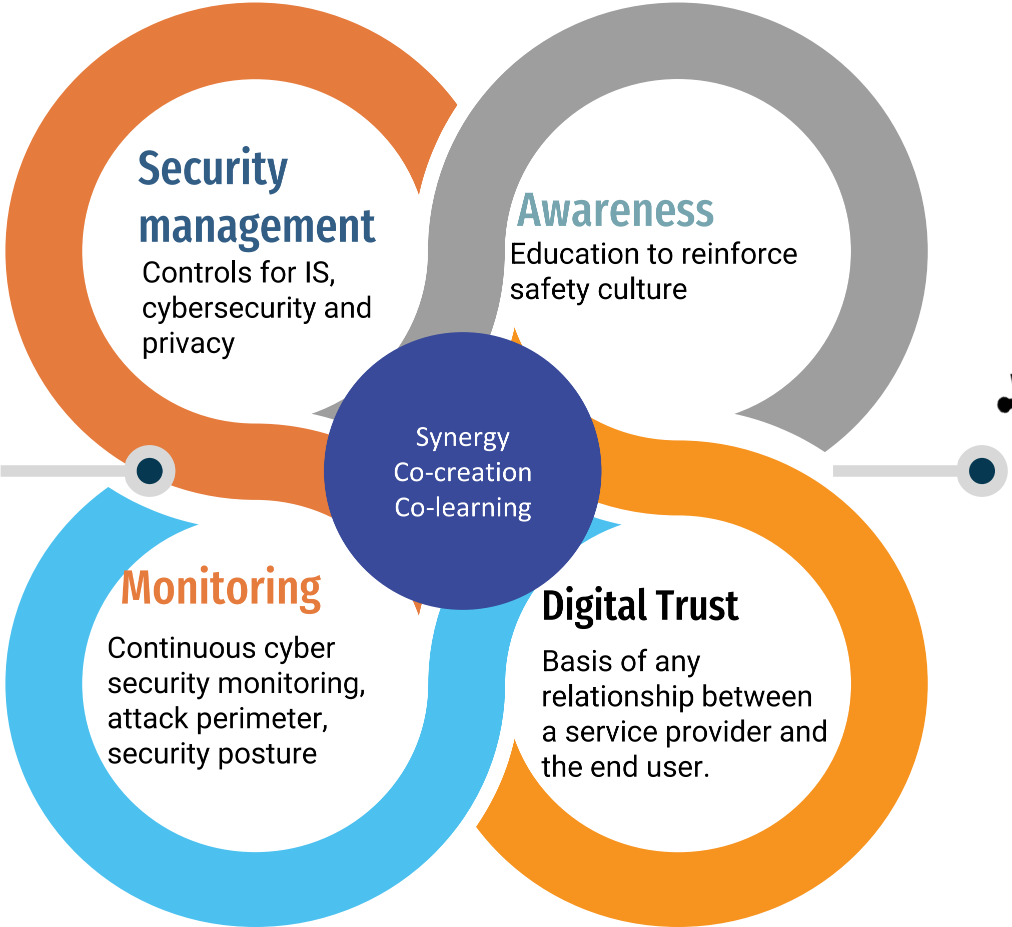
3.Support in tools and best practice frameworks.

ice
SEGURO SOCIAL
COSTA RICA
PODER JUDICIAL
República de Costa Rica
mep
Ministerio de Educación Pública
BP
PRO PATRIA NOSTRA SANGUIS NOSTER
ALAJUELA

Strategy

Internal Audit Units

CGR



Security management

Controls for IS, cybersecurity and privacy

Awareness

Education to reinforce safety culture

Synergy
Co-creation
Co-learning

Monitoring

Continuous cyber security monitoring, attack perimeter, security posture

Digital Trust

Basis of any relationship between a service provider and the end user.

Tools.

Developed tools

Evaluation of the Information Security Management System

Tool based on the ISO standard 27001:2023

Cybersecurity level assessment

Tool based on the NIST Cybersecurity Framework (NIST CSF)

Digital trust, awareness and awareness

Formulation of the essential elements and demonstration of a campaign

SGSI evaluation tool

Aim:

- Determine whether the institution's security management reasonably complies with the applicable regulatory framework.

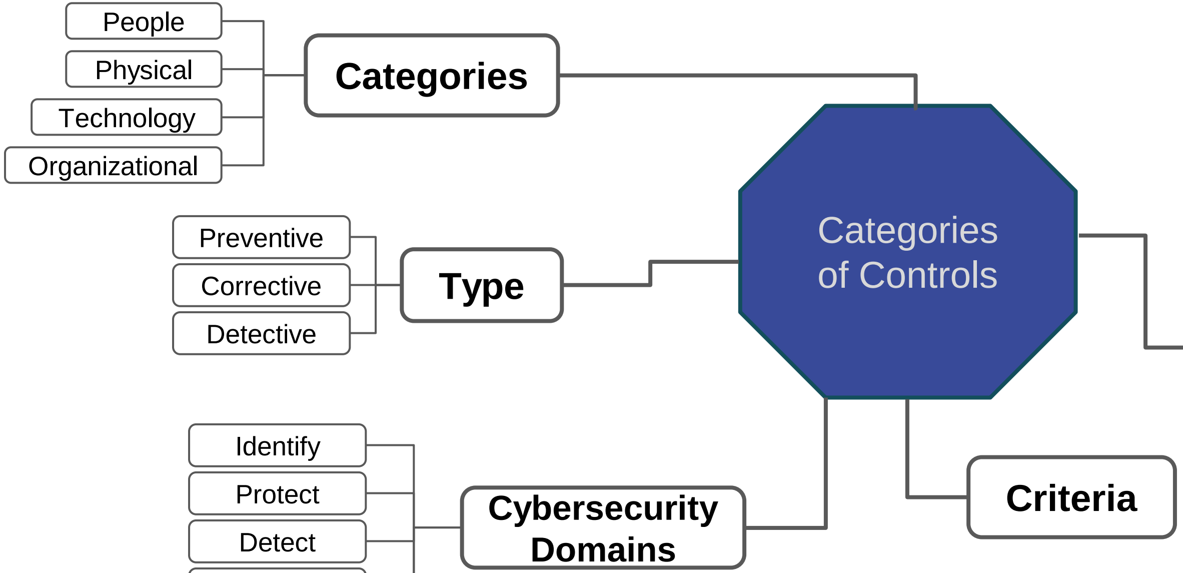
Detail:

- This tool takes the structure of ISO 27001:2023 to develop a compliance questionnaire.

Approach:

- Categorization of controls by themes and attributes is used to provide a detailed understanding of how controls influence risk management and information security.

ISMS evaluation tool



Categories of Controls

Categories

People

Physical

Technology

Organizational

Type

Preventive

Corrective

Detective

Cybersecurity Domains

Identify

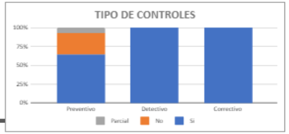
Protect

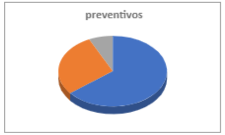
Detect

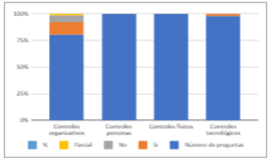
Respond

Recover

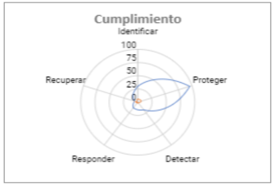
Criteria







detectivos



correctivos

Tool for evaluating the level of cybersecurity

Aim:

- Determine whether the institution's current level of cybersecurity allows it to reasonably comply with the applicable regulatory framework and the objectives established by the institution.

Detail:

- This tool uses the NIST Framework (checklist version 1.1) with the purpose of detecting deficiencies in the current cybersecurity risk management strategy. Its function is to provide management with crucial information for the formulation of an action plan aimed at continuous improvement.

Approach:

- The Framework structure, which includes Function, Categorization, and Subcategorization of controls, is used to provide a detailed understanding of the level at which the institution is during the self-assessment.

Tool for evaluating the level of cybersecurity

Framework		
Functions		
	Identify	Categories Subcategories Activities
	Protect	
	Detect	
	Respond	
	Recover	

Levels
1- Partial
2- Risk Informed
3- Repeatable
4- Adaptive

Digital trust, awareness and awareness

Aim:

- Raise awareness of the importance of digital trust
- Provide guidance on how to run a cybersecurity awareness campaign, with limited or no budget.

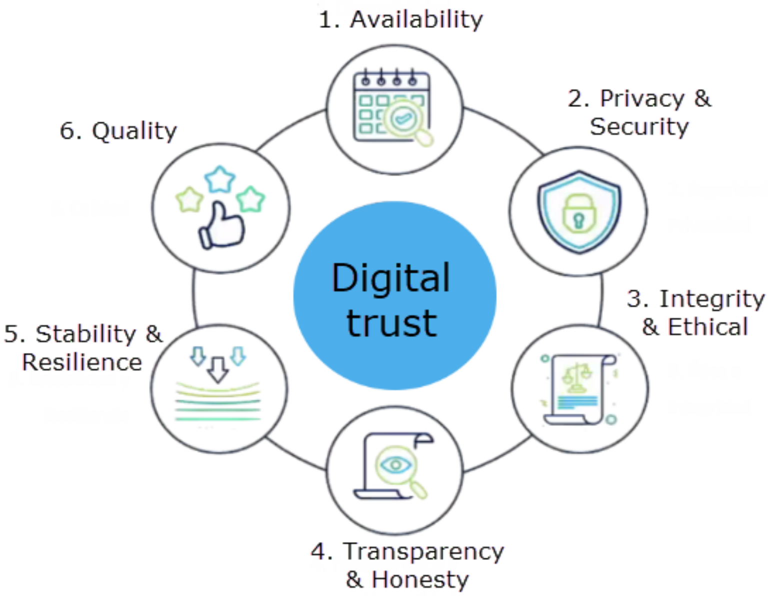
Detail:

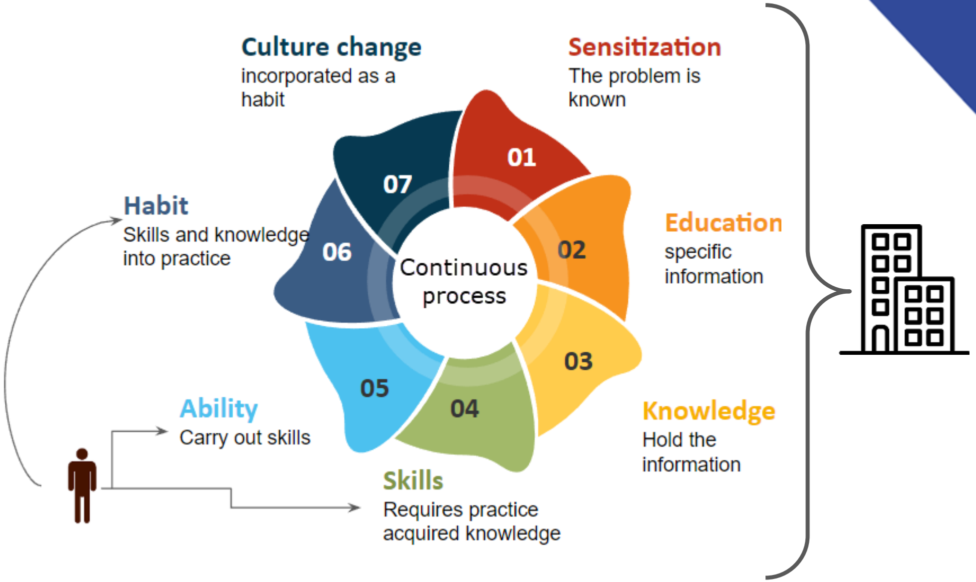
- The importance of digital trust as a basis for decision-making by technology users is presented, as well as the cycle of awareness and education on cybersecurity. Finally, the elements to consider in the development of an awareness and education campaign are explained.

Approach:

- Awareness-raising tools and documentation of campaigns from recognized entities, such as INCIBE and the OAS, are taken as a basis.

Digital trust, sensitization and awareness





Learning

- The construction of tools involves an effort of research, learning and understanding of the base frameworks. This allows knowledge about these frameworks to be internalized.
- The dynamic of co-creation and co-learning allows us to create awareness about the reality of each participating unit, the exchange of experiences and promotes greater generation of value from the tools created.
- The generation of synergies of the CGR with the Internal Audits, and the dynamics of the sessions held, encourages collaboration and formation of strategic alliances for the evaluation of cybersecurity in the Public Sector
- The value that Internal Audit teams have in institutions and how it can contribute positively to the continuity of operations

Thanks!

Questions or comments