Auditorías Internas para la fiscalización de la Ciberseguridad

Aspectos

1. Contexto
2. Marco orientador
3. Diagnóstico
4. Estrategia
5. Herramientas
6. Aprendizajes

Contexto

2020-2021

Desafío 3 del PEI: Transformación digital del Sector Público.
Valor agregado en estudios de ATI

2022 - I Semestre

Emergencia nacional de ciberseguridad

2022 - II Semestre

Seguimiento de la Gestión Pública en 267 entidades, para medir nivel de prácticas en SI

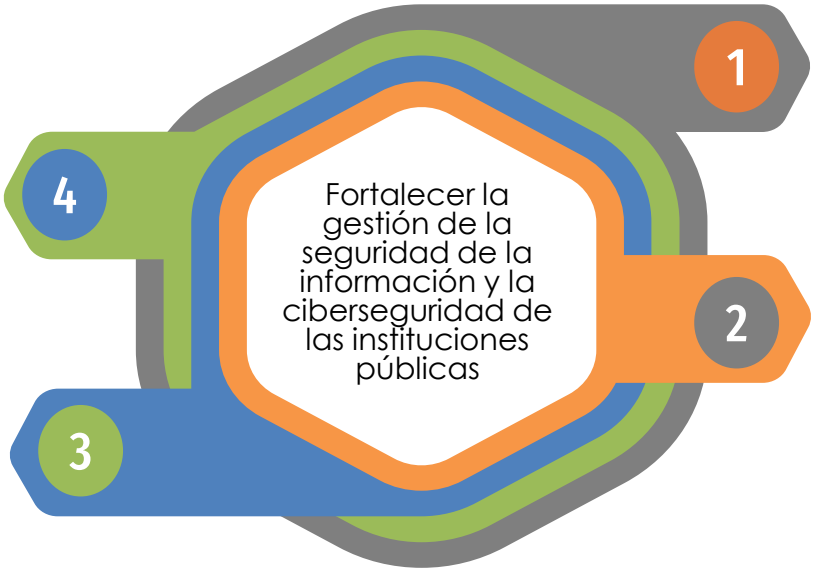
2023

Programa fortalecimiento AIs por medio herramientas SI Ciberseguridad

Marco orientador

02/05/2023 al 30/10/2023

Utilizar y aplicar las herramientas desarrolladas



Desarrollar y compartir herramientas ágiles, adaptables y sencillas para auditar la seguridad de la información con énfasis en la ciberseguridad

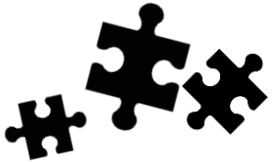
Crear un impacto de concienciación sobre la importancia que tienen las AIs, en el aseguramiento razonable sobre la continuidad de los servicios de su entidad

Diagnóstico inicial

1. Estudios realizados por las Auditorías Internas, período 2021-2023
2. Nivel de capacitación y personal con certificaciones
3. Apoyo en herramientas y marcos de buenas prácticas

Estrategia

Unidades de Auditoría Interna CGR



Herramientas

Herramientas desarrolladas

Evaluación del Sistema de Gestión de la Seguridad de la Información

Herramienta basada en la norma ISO 27001:2023

Evaluación del nivel de ciberseguridad

Herramienta basada en el Marco de Ciberseguridad de NIST (NIST CSF)

Confianza digital, sensibilización y concienciación

Formulación de los elementos esenciales y demostración de una campaña

Herramienta para evaluación del SGSI

Objetivo:

- Determinar si la gestión de seguridad de la institución cumple razonablemente con el marco regulatorio aplicable.

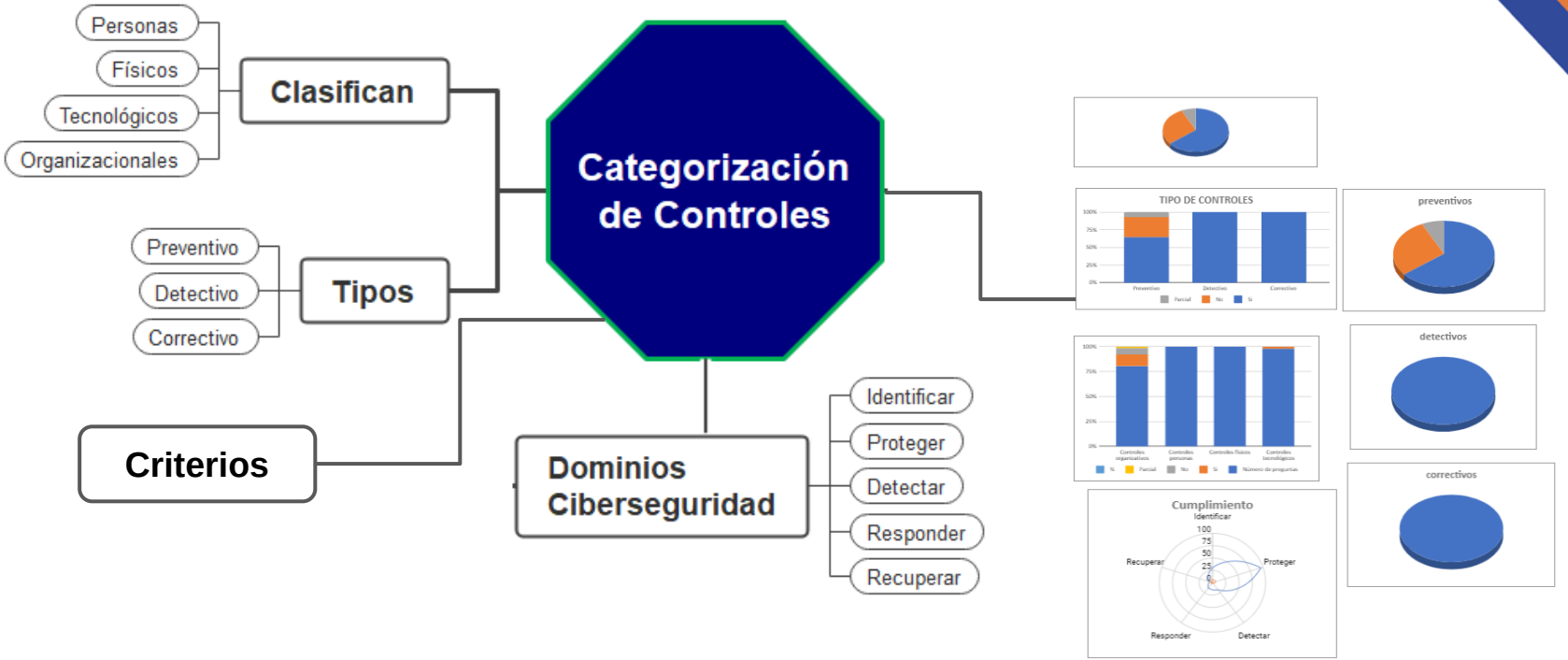
Detalle:

- Esta herramienta toma la estructura de la ISO 27001:2023 para desarrollar un cuestionario de cumplimiento.

Enfoque:

- Se utiliza la categorización de los controles por temas y atributos, para brindar una comprensión detallada de cómo los controles influyen en la gestión de riesgos y la seguridad de la información.

Herramienta para evaluación del SGSI



Herramienta para evaluación del nivel de ciberseguridad

Objetivo:

- Determinar si el nivel actual de seguridad cibernética de la institución le permite cumplir razonablemente con el marco regulatorio aplicable y los objetivos establecidos por la institución.

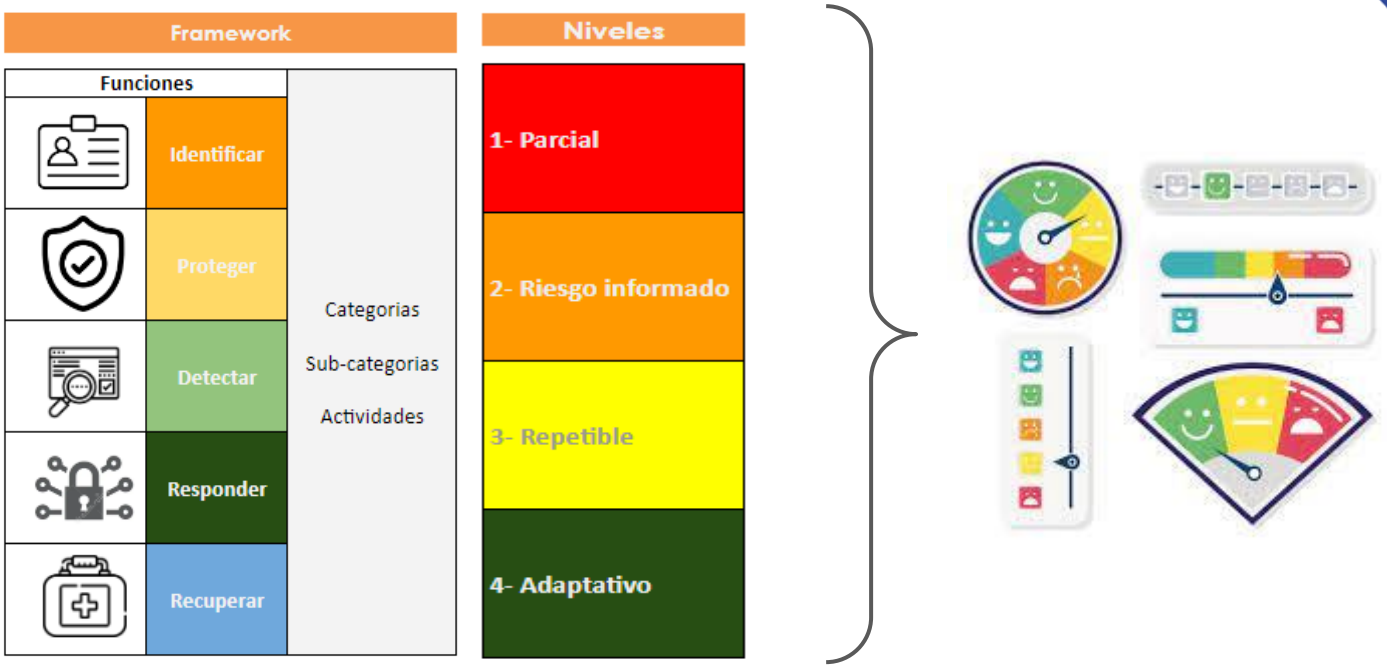
Detalle:

- Esta herramienta emplea el Marco de NIST (checklist versión 1.1) con el propósito de detectar deficiencias en la actual estrategia de gestión de riesgos de ciberseguridad. Su función es suministrar a la dirección información crucial para la formulación de un plan de acción orientado a la mejora continua.

Enfoque:

- Se utiliza la estructura del Framework, que incluye la Función, Categorización y la Subcategorización de los controles, con el fin de proporcionar una comprensión detallada del nivel en el que se encuentra la institución durante la autoevaluación.

Herramienta para evaluación del nivel de ciberseguridad



Confianza digital, sensibilización y concienciación

Objetivo:

- Generar conciencia de la importancia que tiene la confianza digital
- Brindar orientaciones sobre cómo ejecutar una campaña de concientización sobre la ciberseguridad, con un presupuesto limitado o nulo.

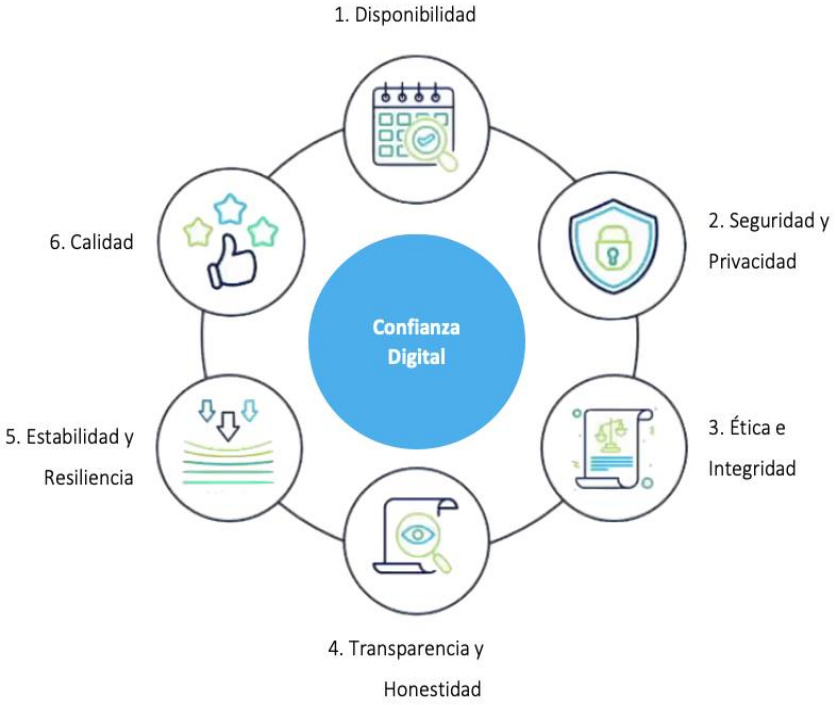
Detalle:

- Se presenta la importancia de la confianza digital como base para la toma de decisiones de los usuarios de tecnología, así como el ciclo de sensibilización y educación en materia de ciberseguridad. Finalmente, se explican los elementos a considerar en el desarrollo de una campaña de sensibilización y educación.

Enfoque:

- Se toman como base herramientas de concientización y documentación de campañas de entidades reconocidas, como INCIBE y la OEA.

Confianza digital, sensibilización y concienciación



Aprendizajes

- La construcción de herramientas implica un esfuerzo de investigación, aprendizaje y comprensión de los marcos de trabajo base. Ello permite interiorizar el conocimiento sobre dichos marcos
- La dinámica de co-creación y co-aprendizaje permite crear conciencia sobre la realidad de cada unidad participante, el intercambio de experiencias y propicia una mayor generación de valor de las herramientas creadas
- La generación de sinergias de la CGR con las Auditorías Internas, y la dinámica de las sesiones efectuadas, fomenta la colaboración y formación de alianzas estratégicas para la evaluación de la ciberseguridad en el Sector Público
- El valor que tienen los equipos de Auditoría Interna en las instituciones y cómo puede aportar de manera positiva en continuidad de las operaciones

Consultas o comentarios