DGTIC UNAM CERT

2do Coloquio de Proyectos de Becarios en Seguridad Informática

Sistema de gestión del servicio de pruebas de penetración

Ing. Sandra Atonal Jiménez

Ing. José Luis Sevilla Rodríguez

Descripción

- Sistema de gestión, soportado por estándares y mejores prácticas reconocidas internacionalmente que administre y gestione el servicio de pruebas de penetración.

- Documentación de guías y procesos para realizar pentest.

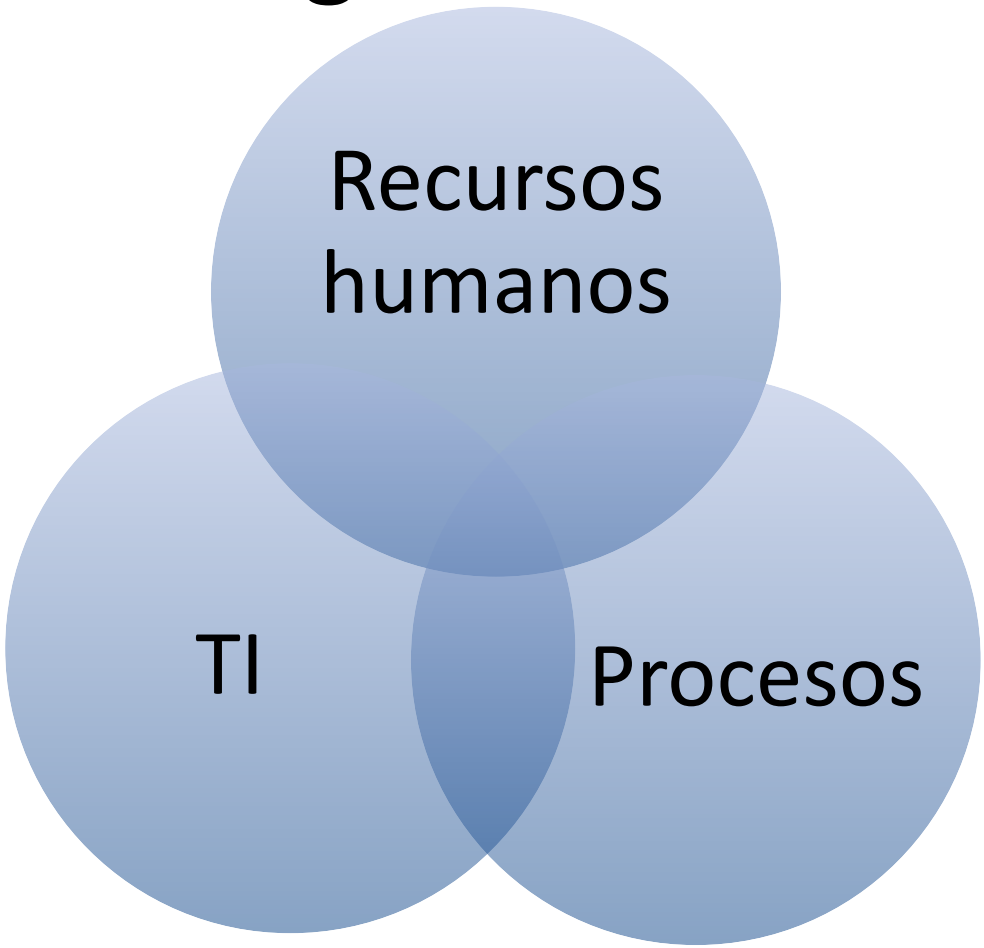
Justificación

- Servicio más solicitado del Departamento de Auditoría y Nuevas Tecnologías.
- Alta rotación del personal.
- Servicio no estructurado.

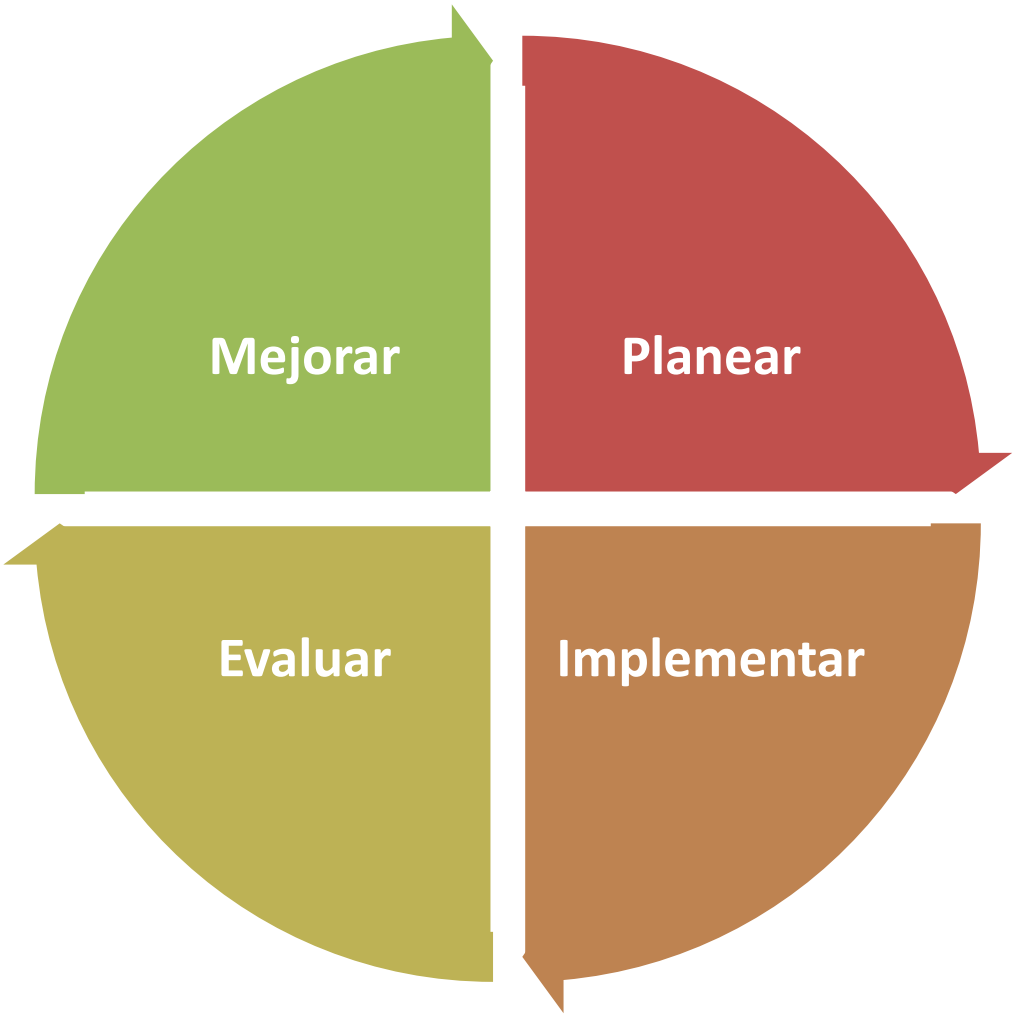
Beneficios

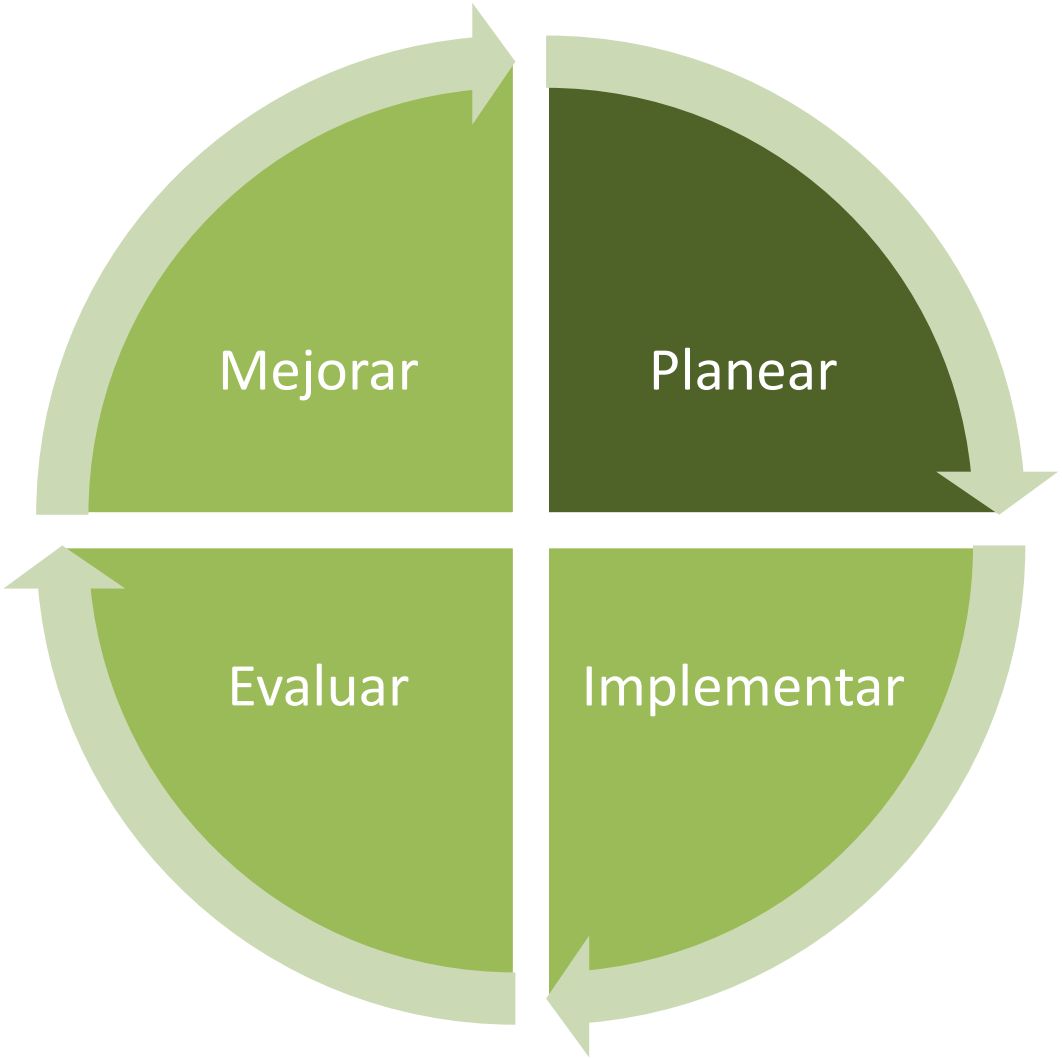
- Toma de decisiones.
- Calidad del servicio.
- Disminuir la curva de aprendizaje.
- Aumento en la productividad.

Sistema de gestión de servicios

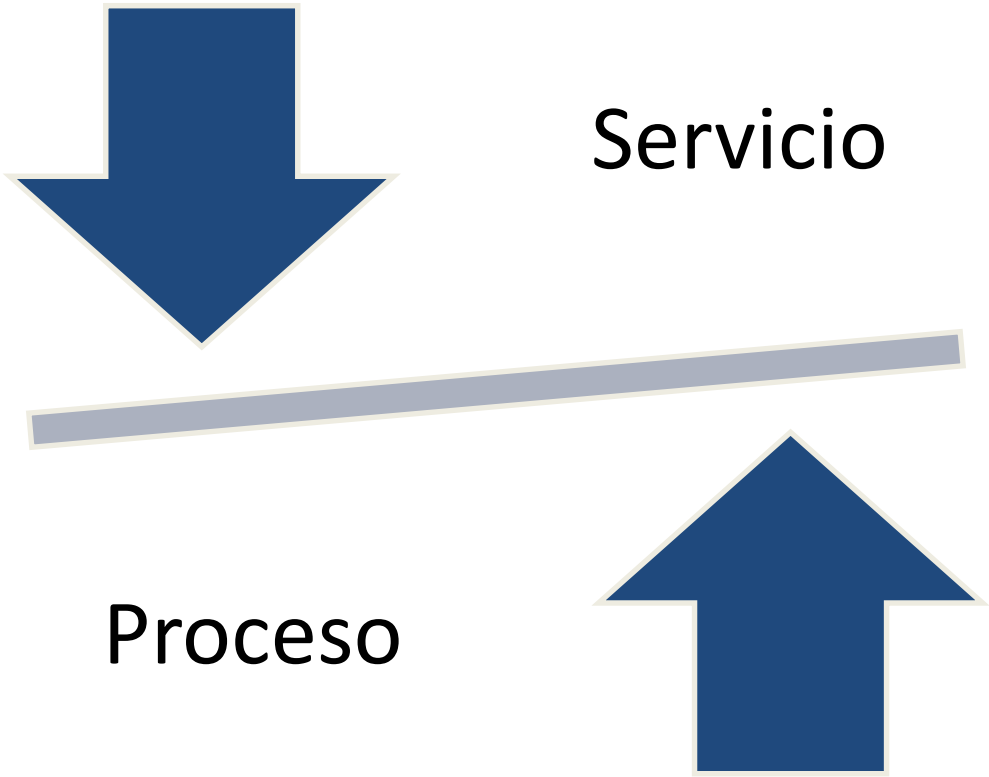


Modelo PDCA




Mejorar
Planear
Evaluar
Implementar

Planeación



Planeación

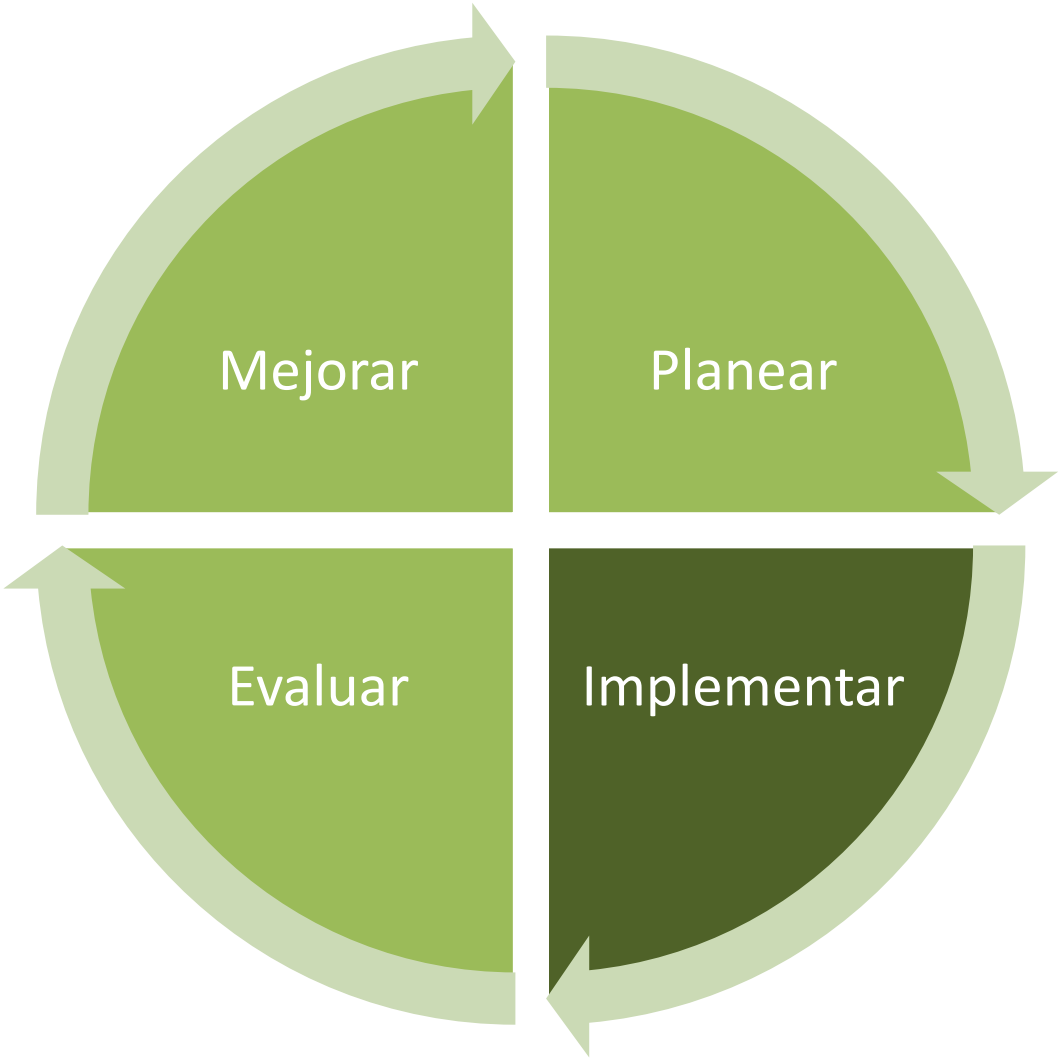
- **Servicio**
  - Política del sistema de gestión de servicios.
  - Portafolio de servicios del Departamento de Auditoría y Nuevas Tecnologías.
  - Encuesta de satisfacción del cliente.

Planeación

- **Servicio**
  - Documentación requerida para el servicio de pruebas de penetración:
    - Acuerdo de niveles de servicio.
    - Hoja técnica.
    - Permiso para realizar el servicio.
    - Minuta pentest.
    - Guía de administración de documentos.
    - Formato del informe de hallazgos y vulnerabilidades.
    - Descripción de CVSS.

Planeación

- **Proceso**
  - Plan de capacitación.


Mejorar
Planear
Evaluar
Implementar

Implementación

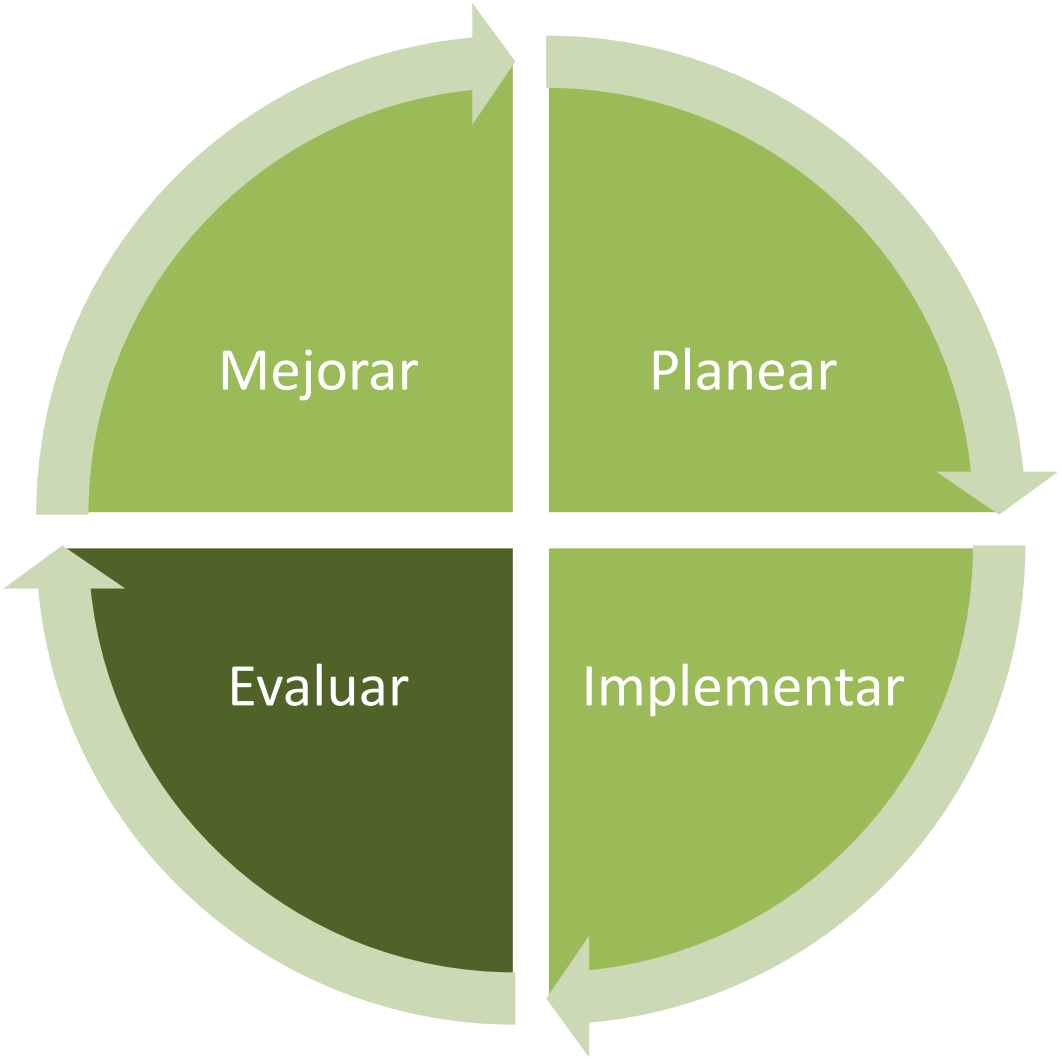
- **Proceso**
  - Presentación de los documentos al Departamento de Auditoría y Nuevas Tecnologías.
  - Administración de documentos de acuerdo a una guía propuesta.
  - Adopción del uso de minutas.

Implementación

- **Proceso**
  - Elaboración de informes con la plantilla establecida.
  - Ejecución de pruebas de penetración de acuerdo a la metodología general.
  - Consulta de guías técnicas para realizar pruebas de penetración.

Implementación

- **Servicio**
  - Envío de encuestas de satisfacción a clientes.


Mejorar
Planear
Evaluar
Implementar

Evaluación

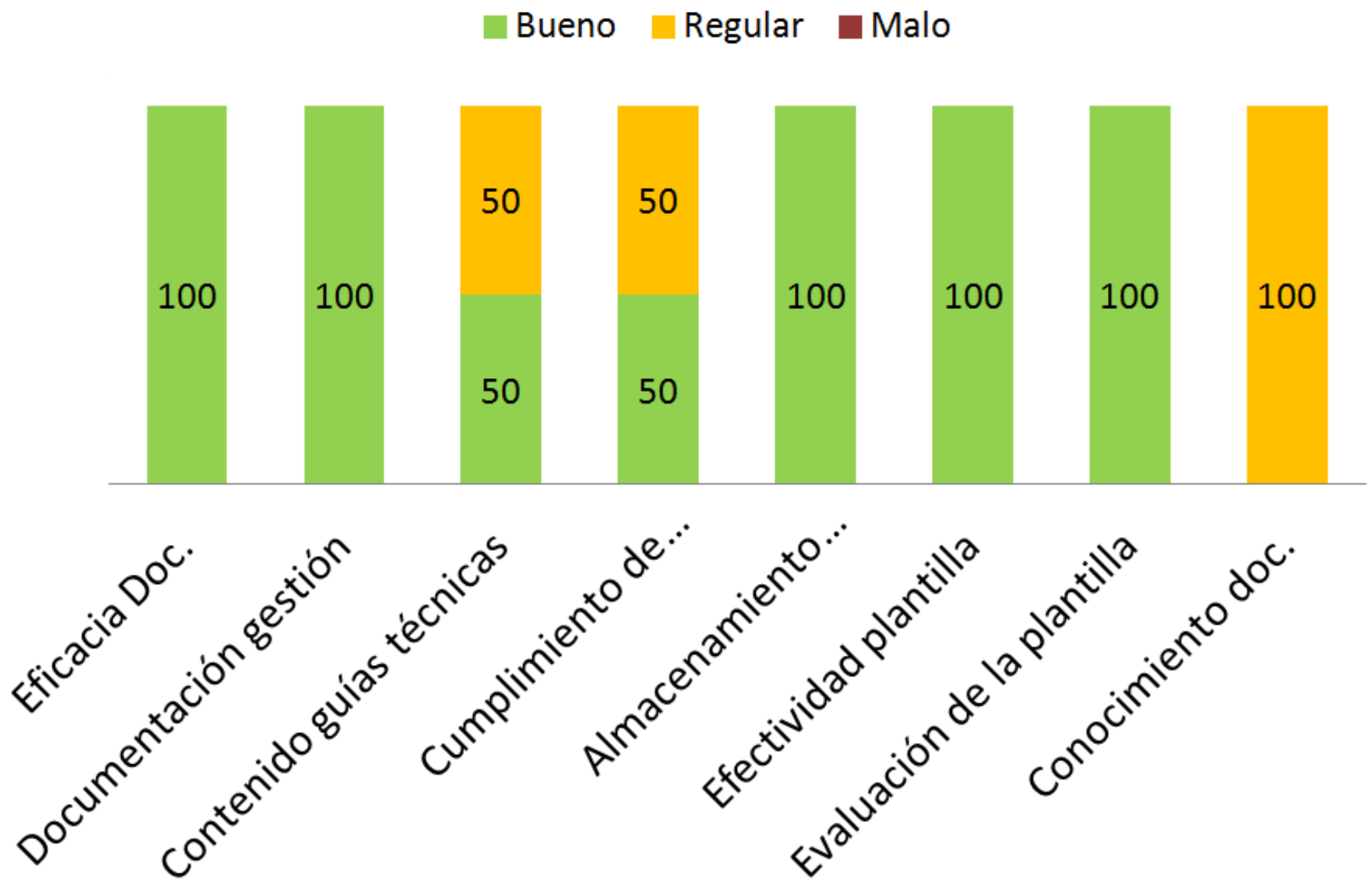
- **Proceso**
  - Definición de métricas.
  - Encuesta sobre efectividad del proceso.
  - Identificación de debilidades y fortalezas.
- **Servicio**
  - Definición de métricas.
  - Encuesta sobre satisfacción del cliente.

Resultados

- **Proceso**
  - Encuesta sobre efectividad:
    - Apoyo provisto por la documentación.
    - Contenido de los documentos para la gestión.
    - Contenido de las guías técnicas.
    - Cumplimiento de las actividades.

Resultados

- **Proceso**
  - Almacenamiento centralizado de hallazgos e informes.
  - Uso de la plantilla para elaborar informes.
  - Contenido de la plantilla.
  - Conocimiento de la documentación.
  - Recomendaciones y observaciones.


Bueno
Regular
Malo
100
100
50
50
50
50
100
100
100
100
Eficacia Doc.
Documentación gestión
Contenido guías técnicas
Cumplimiento de...
Almacenamiento...
Efectividad plantilla
Evaluación de la plantilla
Conocimiento doc.

Resultados

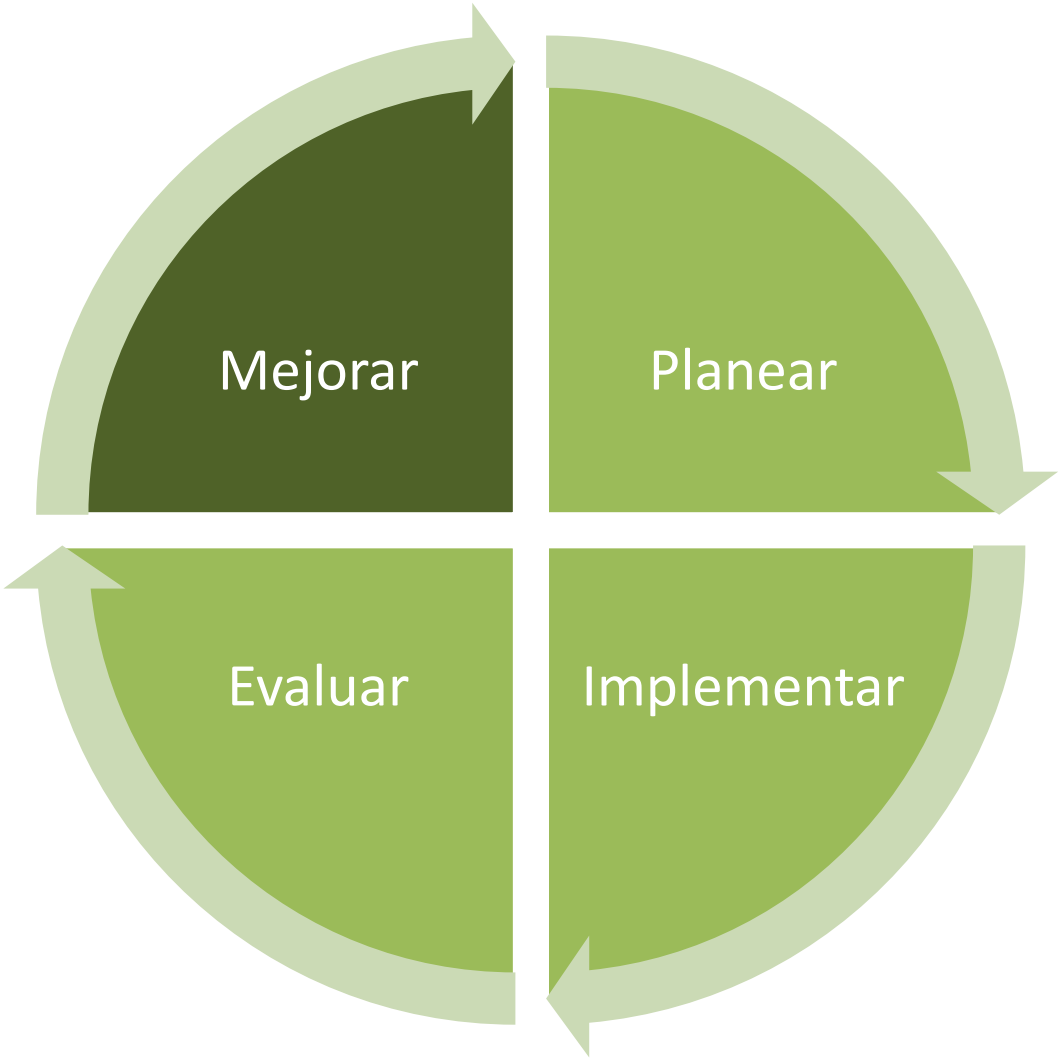
- **Proceso**
  - Perspectiva de los ejecutores:
    - Los documentos proporcionan una guía de las actividades que deben realizarse en el proceso.
    - Se disminuye el tiempo en la capacitación de las personas en cuanto al proceso.
    - Disponibilidad de información.
    - Reducción en el tiempo de elaboración de informes.

Resultados

- **Servicio**
  - Encuesta de satisfacción:
    - Atención recibida por parte del personal.
    - Satisfacción del servicio.
    - Calidad del servicio.
    - Comunicación con el personal.

Resultados

- **Servicio**
  - Encuesta de satisfacción:
    - Cumplimiento de actividades.
    - Solicitud futura del servicio.
    - Medio por el que se entero del servicio.
    - Recomendación del servicio.
    - Recomendaciones y observaciones.


Mejorar
Planear
Evaluar
Implementar

Mejora continua

- **Servicio**
  - Establecer un mecanismo de comunicación para que los clientes envíen quejas durante el servicio.
  - Carta compromiso.
  - Sanciones.
  - Difusión de la documentación relacionada con el servicio.
  - Evaluación del cumplimiento del proceso cada determinado tiempo.

Mejora continua

- **Proceso**
  - Creación de guías.
  - Fortalecer medidas de seguridad de la información.
  - Base de conocimientos.
  - Adoptar el proceso de control de cambios.
  - Registro de tiempos.

Estándares, mejores prácticas y metodologías

- **Servicio**
  - Information Technology Infrastructure Library (ITIL)
  - ISO 20000
- **Proceso**
  - SANS
  - NIST SP 800-115
  - OSSTMM
  - ISSAF

¿Preguntas?