“Desarrollo del Manual de Procesos Operativos para el CERT académico de la ESPE utilizando Estándares a nivel Internacional”

Estudiantes:

Pacha Morales Maycol Jonathan

Ruiz Vega Juan Jose

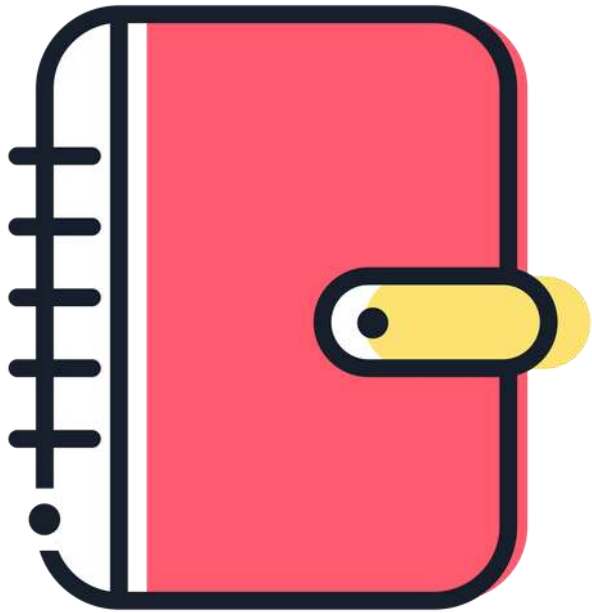
Tutor:

Ing. Ron Egas Mario Bernabé MSc

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Contenido

1. Introducción
2. Trabajos Relacionados
3. Desarrollo
4. Validación y Resultados
5. Conclusiones
6. Recomendaciones



Introducción

Antecedentes

La globalización de la Internet

Todo tipo de compañías

Activo importante para la organización

Prevenir sistemas digitales

Planteamiento del Problema

Actividades operacionales repetitivas

Demoras en el tiempo de atención y respuesta

Incapacidad para solventar todas las necesidades de los clientes

Malestar por parte de los clientes que solicitan algún servicio

Riesgos en la imagen corporativa

Dificultad en la gestión operacional de los servicios ofertados por el (ESPE-CERT)

Falta de información concerniente a las actividades y tareas del negocio

Procesos operativos no racionalizados

Control inexistente de las actividades y resultados obtenidos

Desconocimiento del catálogo de servicios del CERT por parte de sus operadores

Mala organización en cuanto a la delegación de roles y responsabilidades

Objetivo General

Desarrollar

Manual de Procesos Operativos

Estándares a nivel internacional

Racionalización de procesos

Ofrecer Herramienta/ Operación del CERT

Coadyuvando en la mejora de los servicios

Objetivos Específicos

Estudios relacionados

Falta de operatividad de un CERT

Revisión de literatura preliminar

OE1:

Identificar estudios relacionados con el bajo desempeño y la falta de operatividad de un CERT, mediante una revisión de literatura preliminar.

Objetivos Específicos

Revisión sistemática

Buenas prácticas y estándares

Operación CERT

OE2:

Realizar una revisión sistemática de las buenas prácticas y estándares a nivel internacional, para la operación de un equipo de respuesta ante incidentes informáticos.

Objetivos Específicos

Norma de procedimientos

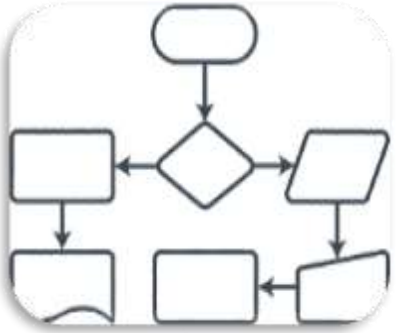
Procesos operativos

Nivel crítico

OE3:

Elaborar la norma de procedimientos de los procesos operativos identificados de acuerdo a su nivel crítico.

Objetivos Específicos



Diagramas de flujo

Actividades

Procedimientos

Servicios proactivos y reactivos

OE4:

Diseñar los diagramas de flujo de acuerdo a las actividades identificadas en cada uno de los procedimientos que soportan los servicios proactivos y reactivos en el ESPE-CERT.

Objetivos Específicos

Rúbrica de evaluación

Matriz de priorización

Validez de los procesos

OE5:

Elaborar la rúbrica de evaluación y matriz de priorización de parámetros para determinar la validez de los procesos.

Trabajos Relacionados

Estado del Arte

Mejorar el rendimiento operacional de un CERT

Detalles técnicos de un CERT

Criterios de exclusión

Fuentes de bases digitales no reconocidas

Buenas prácticas y estándares a nivel internacional

Criterios de inclusión

Nessus® vulnerability scanner

Herramientas de respuesta a incidentes de seguridad de la información.

Artículos en otro idioma que no sea inglés

Artículos publicados entre 2010 y 2022

Estado del Arte

Grupo de control

5 estudios

Artículos relacionados

20 estudios

Conclusión del EA

01 02 03 04 05

Cadena de búsqueda

IEEE Xplore Digital Library

ALL ((CERT or CSIRT or RESPONSE TEAM) and (INFORMATIC SECURITY OR COMPUTER INCIDENT) and (TEAMWORK or TEAM PERFORMANCE) and (LOW PERFORMANCE or BAD RESULTS))

Estudios primarios

9 artículos

Desarrollo

Metodología Ad-Hoc

Revisión de literatura

Racionalización de procesos

Mapa de procesos

Norma de procedimiento

Validación del proceso

Manual de procesos operativos

Revisión de literatura

Propósito

Metodologías | Marcos de trabajo | Normas | Estándares | Buenas Prácticas

CERTs – Internacional

Organismos Internacionales

ITIL V4

NIST SP 800-50

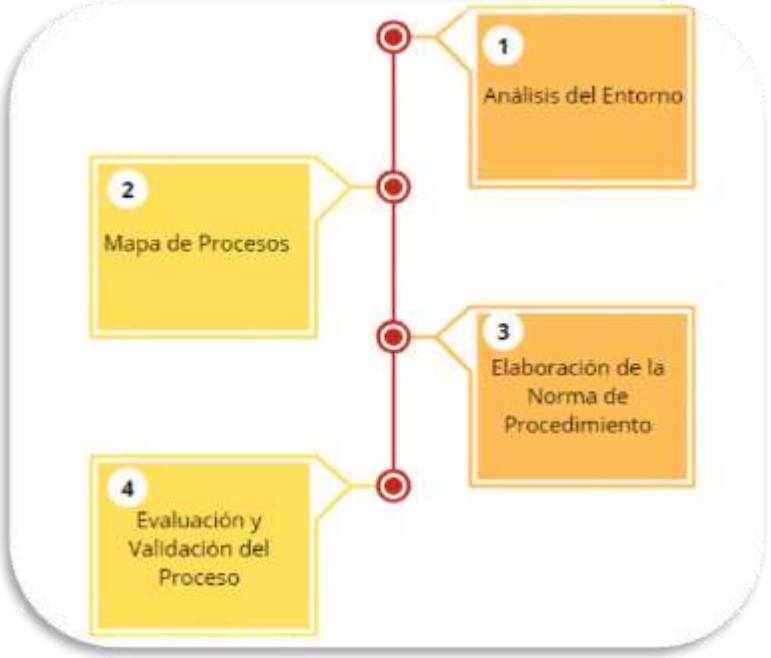
NIST SP 800-61

Racionalización de Procesos

Simplificar / Eliminar

Mejorar la eficiencia de los procesos

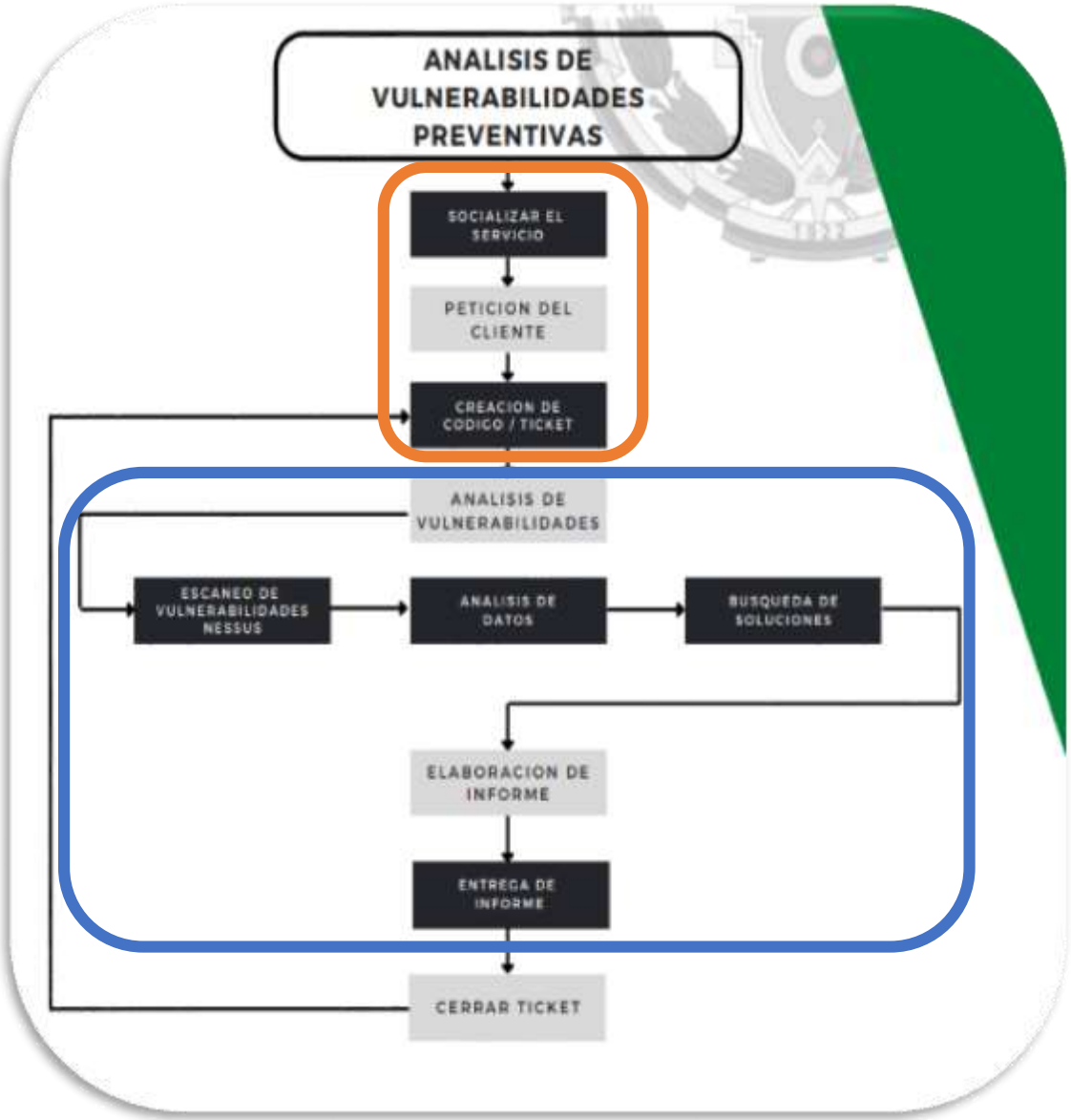
Metodologías de mejora de procesos



Metodología ecléctica

Racionalización de Procesos

Situación Actual



Propuesta

Mesa de Servicios

Análisis de Vulnerabilidades

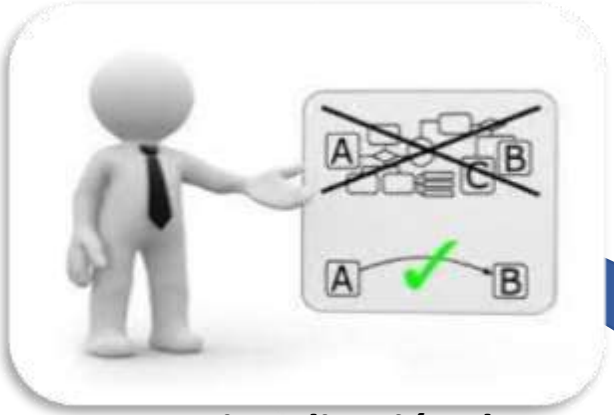
Gestión de Incidentes

Situación Actual

ESPE-CERT

PROACTIVO

REACTIVO



Racionalización de procesos

Demoras en atención

Malestar de clientes

Manual

Mapa de Procesos

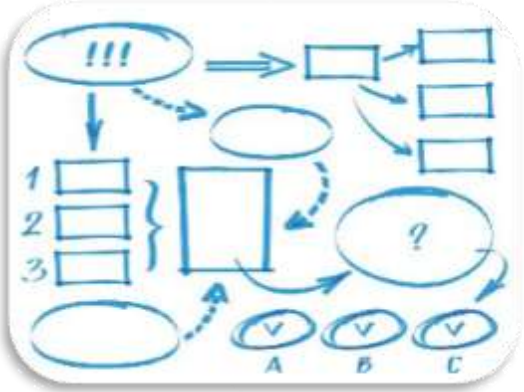
Participación directa de los miembros operadores del CERT

Servicios definidos por el trabajo de titulación “Implementación y puesta en marcha de un CSIRT”

Progreso

Prosperidad

No independientes / Persiguen un mismo fin



Interrelacionan los procesos

Mapa de Procesos

Procesos Gobernantes

Políticas, directrices y planes estratégicos.

Procesos de Apoyo

Gestionar y administrar los recursos.

Estructura

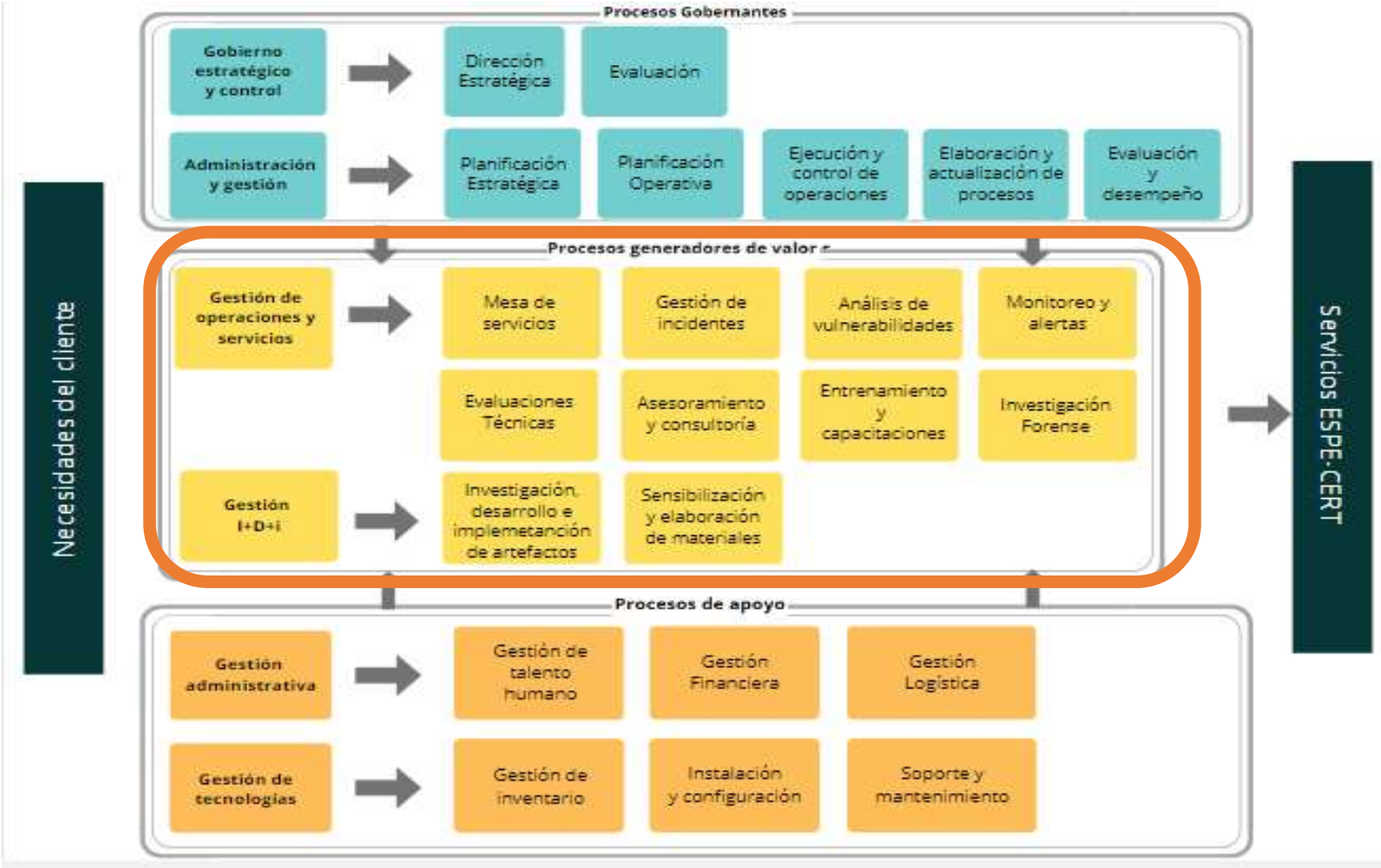
Procesos Generadores de Valor

Valor agregado a los clientes y a la institución.

Raíz de los servicios del ESPE-CERT.

Bienes y servicios que se dirigen a los clientes.

Mapa de Procesos



Norma de Procedimiento

Objetivo

Alcance

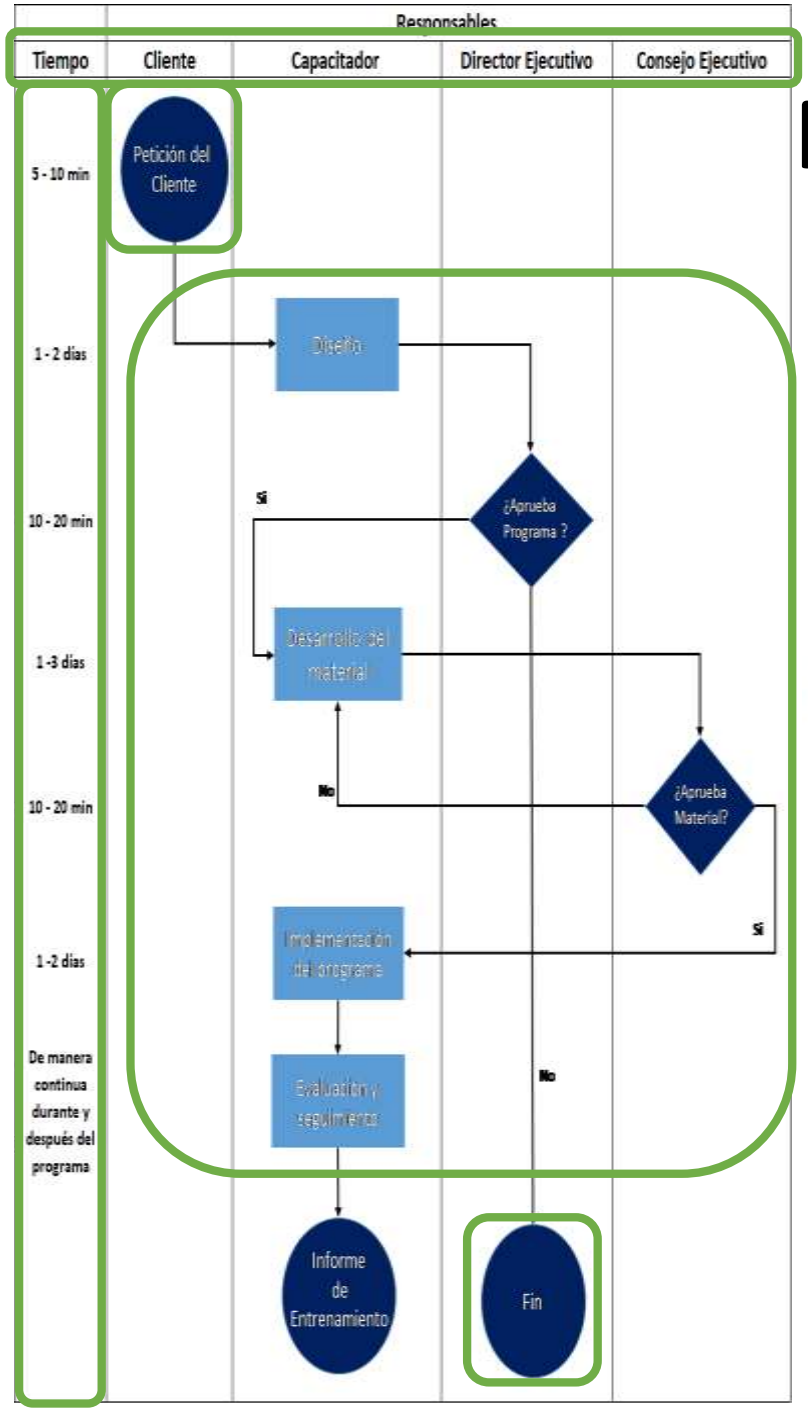
Responsables

Base legal y políticas

Definición

Desarrollo

Indicadores



Norma de Procedimiento

Tiempo

Responsables

Referencias Normativas

Manual de Procesos Operativos

Versión	Fecha	Autor	Revisado	Aprobado	Descripción
1.0.0	05-AGO-2022	-Maycol Pacha -Juan Ruiz	Ing. Mario Ron MSc.	Dr. Walter Fueres D.	Emisión inicial.

Historial de cambios

Términos y Condiciones

Objeto y campo de aplicación

Referencias Normativas

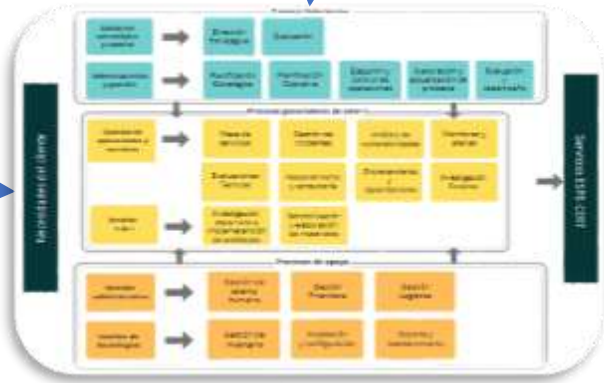
Manual de Procesos Operativos

Publico objetivo

Autoridad

Descripción del documento

Roles y responsabilidades



Mapa general de procesos

Manual de Procesos Operativos

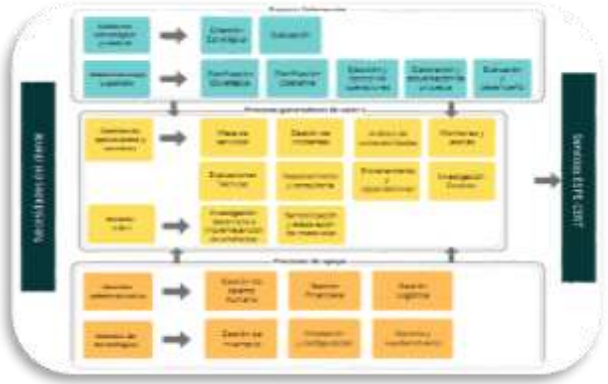
Norma de procedimiento

Disposiciones generales y transitorias

Aprobación y legalización

Validación y Resultados

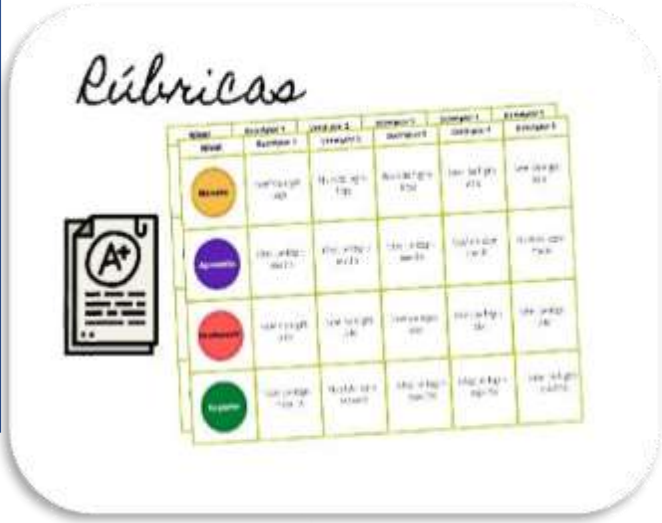
Validación del Proceso



Mapa General de procesos

- [A] Cumplimiento del objetivo del procedimiento.
- [B] Eficiencia en el proceso.
- [C] Sintaxis, redacción y semántica del contenido.
- [D] Asignación de roles y responsabilidades.
- [E] Uso de normas internacionales de referencia.
- [F] Secuencia lógica de actividades.

Selección de parámetros



Rúbrica de evaluación

Parámetros	A	B	C	D	E	F	Suma	Porcentaje
A		1	1	1	1	1	5	0,33
B	0		1	1	1	1	4	0,27
C	0	0		1	0	0	1	0,07
D	0	0	0		1	0	1	0,07
E	0	0	1	0		0	1	0,07
F	0	0	1	1	1		3	0,20
Total							15	1

Matriz de Priorización

Validación del Proceso

Parámetros

0.33

Objetivo

0.27

Eficacia

0.20

Actividades

0.07

Roles

0.07

Normas

0.07

Redacción

Categorías

- C. ACEPTABLE **5**
- ACEPTABLE **4**
- A. C. MENORES **3**
- A. C. MAYORES **2**
- NO ACEPTABLE **1**

Evaluación de expertos

Toma de decisiones

Validación del Proceso

Nombres	Cargo	Fecha de Evaluación	Firma
Ing. Jonathan Francisco Benavides Cabascango	Encargado de servicios operativos e infraestructura del ESPE-CERT (Ayudante de Investigación)	14-07-2022	JONATHAN FRANCISCO BENAVIDES CABASCANGO Firmado digitalmente por JONATHAN FRANCISCO BENAVIDES CABASCANGO Fecha: 2022.07.14 12:21:51 -05'00'
Ing. Marco Antonio Bonilla Vergara	Operador ESPE-CERT	14-07-2022	MARCO ANTONIO BONILLA VERGARA
Capt. Jhon Darío Arcos Poma	Operador ESPE-CERT	15-07-2022	
Capt. Christian Fabricio Parra Martínez	Operador ESPE-CERT	15-07-2022	

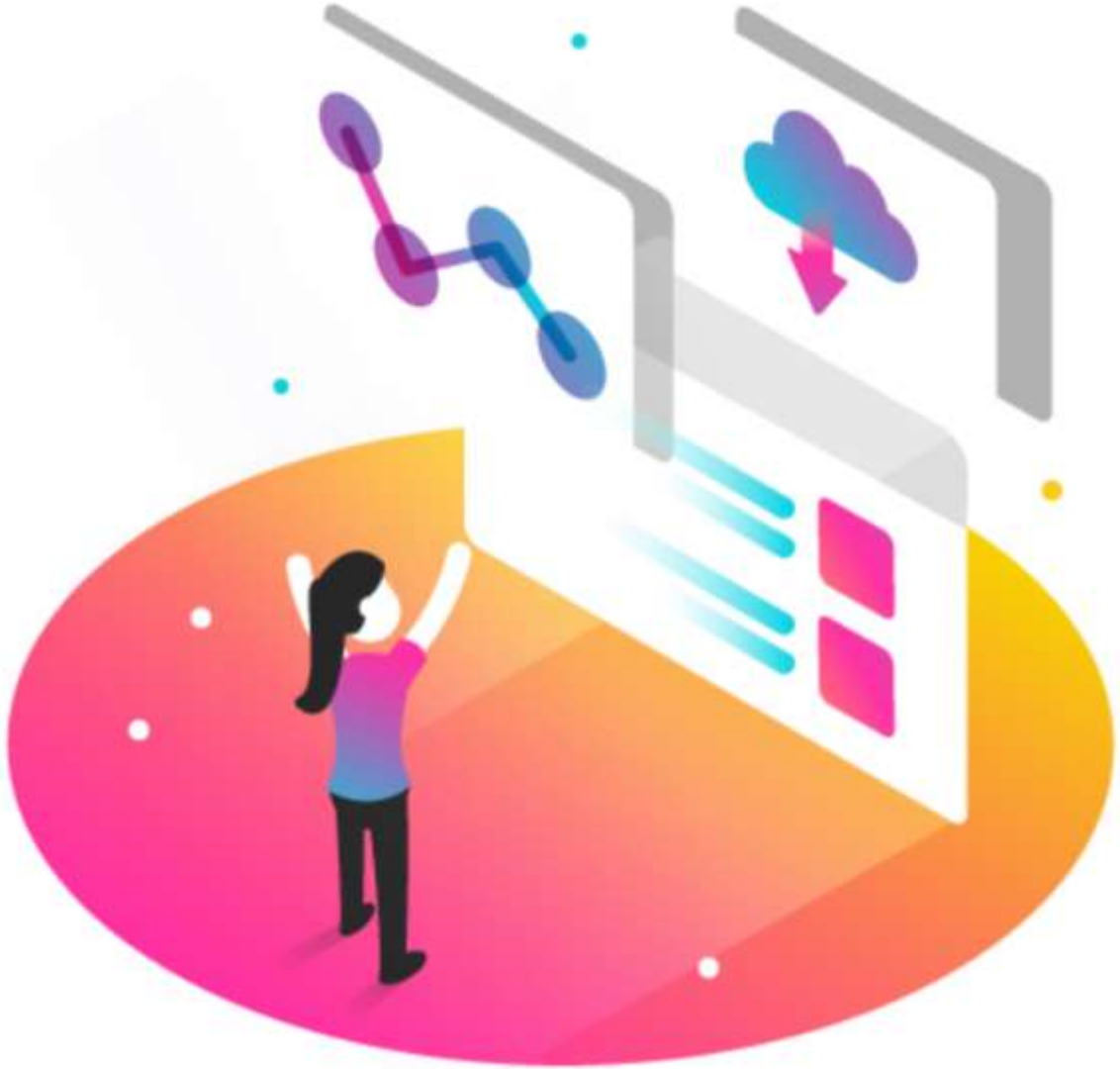
Resumen de Resultados

Evaluador	Cumplimiento del objetivo del proceso	Eficiencia en el proceso	Sintaxis, redacción y semántica del contenido	Asignación de roles y responsabilidades	Uso de normas internacionales de referencia	Secuencia lógica de actividades
Ing. Marco Antonio Bonilla Vergara	5	5	5	5	4	5
Ing. Jonathan Francisco Benavides Cabascango	5	5	5	5	4	5
Capt. Jhon Darío Arcos Poma	5	5	5	4	4	5
Capt. Christian Fabricio Parra Martínez	5	5	5	4	5	5

Análisis de Resultados

Parámetros	Ponderaciones P= $(c.priorización * nEvaluador)$				Valor alcanzado	Valor Máximo (100%)	Estándar: Valor mínimo (80%)	% Alcanzado
Cumplimiento del objetivo del proceso	1,65	1,65	1,65	1,65	6,6	1,65	1,32	100 %
Eficiencia en el proceso	1,35	1,35	1,35	1,35	5,4	1,35	1,08	100 %
Sintaxis, redacción y semántica del contenido	1	1	1	1	4	1	0,8	100 %
Asignación de roles y responsabilidades	0,35	0,35	0,28	0,28	1,26	0,35	0,28	90 %
Uso de normas internacionales de referencia	0,28	0,28	0,28	0,35	1,19	0,35	0,28	85 %
Secuencia lógica de actividades	0,35	0,35	0,35	0,35	1,4	0,35	0,28	100 %

Conclusiones



Conclusiones

Manual de Procesos ESPE-CERT

Mejora de Servicios

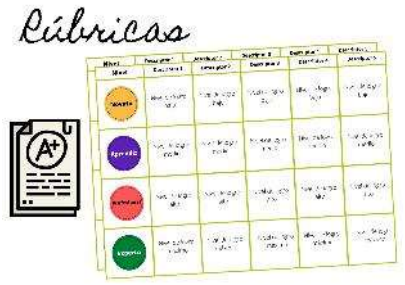
Identificación y revisión sistemática

Base de diseño adecuado del manual de procesos

Servicios proactivos y reactivos

Norma de Procedimiento

Rubrica de Evaluación



Mejoras al documento

Recomendaciones

Recomendaciones

Asignar roles y responsabilidades de acuerdo al manual

Estratégicos y Apoyo

FIRST

Rúbrica de evaluación

¡GRACIAS POR SU ATENCIÓN!