



**Desarrollo del manual de procesos operativos para el CERT académico de la ESPE  
utilizando estándares a nivel internacional**

Pacha Morales, Maycol Jonathan y Ruiz Vega, Juan José

Departamento de Ciencias de la Computación

Carrera de Ingeniería de Sistemas e Informática

Trabajo de titulación, previo a la obtención del título de Ingeniero en Sistemas e Informática

Ing. Ron Egas, Mario Bernabé MSc.

09 de agosto del 2022



TESIS MANUAL DE PROCESOS OPERATIVOS 2022 - Final...

Scanned on: 2:20 August 10, 2022 UTC



Overall Similarity Score



Results Found

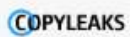


Total Words in Text

Identical Words	0
Words with Minor Changes	0
Paraphrased Words	0
Omitted Words	2112



MARIO  
BERNABE RON



Website | Education | Businesses



**Departamento de Ciencias de la Computación**

**Carrera de Ingeniería de Sistemas e Informática**

**Certificación**

Certifico que el trabajo de titulación: **“Desarrollo del manual de procesos operativos para el CERT académico de la ESPE utilizando estándares a nivel internacional”** fue realizado por los señores Pacha Morales, Maycol Jonathan y Ruiz Vega, Juan José; el mismo que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisado y analizado en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se lo sustente públicamente.

**Sangolquí, 05 de agosto 2022**

Firma:



Escanear el código QR para verificar

**MARIO  
BERNABÉ  
RON**

.....  
Ing. Ron Egas, Mario Bernabé MSc.  
C. C 1704229747



**Departamento de Ciencias de la Computación**  
**Carrera de Ingeniería de Sistemas e Informática**  
**Responsabilidad de Autoría**

Nosotros, **Pacha Morales, Maycol Jonathan** con cédula de ciudadanía N° **1722293048** y **Ruiz Vega, Juan José** con cédula de ciudadanía N° **1725122426** declaramos que el contenido, ideas y criterios del trabajo de titulación: “**Desarrollo del manual de procesos operativos para el CERT académico de la ESPE utilizando estándares a nivel internacional**” es de nuestra autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

**Sangolquí, 05 de agosto del 2022**

Firma:

Firma:

.....  
Pacha Morales, Maycol Jonathan

C.C.: 1722293048

.....  
Ruíz Vega, Juan José

C.C.: 1725122426



**Departamento de Ciencias de la Computación**

**Carrera de Ingeniería de Sistemas e Informática**

**Autorización de Publicación**

Nosotros, **Pacha Morales, Maycol Jonathan** con cédula de ciudadanía N° **1722293048** y **Ruiz Vega, Juan José** con cédula de ciudadanía N° **1725122426** autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: “**Desarrollo del manual de procesos operativos para el CERT académico de la ESPE utilizando estándares a nivel internacional**” en el Repositorio Institucional, cuyo contenido, ideas y criterios son de nuestra responsabilidad.

**Sangolqui, 05 de agosto 2022**

.....

**Pacha Morales, Maycol Jonathan**

**C.C: 1722293048**

.....

**Ruiz Vega, Juan José**

**C.C: 1725122426**

### **Dedicatoria**

*Dedico con todo mi corazón este trabajo de titulación a toda mi familia que estuvo siempre confiando en mí, esperando compartir estos momentos de alegría que no son solo míos sino también de ellos.*

*En especial a mi madre quien nunca dejó de confiar en mí, dándome su apoyo hasta el último día como universitario, me enseñó que con esfuerzo los sueños se cumplen.*

*Finalmente, a mis amigos que con su granito de arena han aportado para llegar a este momento.*

*Juan José Ruiz*

*Dedico este trabajo de titulación a toda mi familia, quienes han velado por mí diariamente en este arduo camino, y me han enseñado que, con esfuerzo, perseverancia y dedicación, algo que parecía una utopía al fin llega a su culminación.*

*Finalmente quiero dedicar esta tesis a mis compañeros de aula, quienes compartieron conmigo tantas anécdotas y siempre estuvieron en los buenos y malos momentos.*

*Maycol Pacha*

## Agradecimiento

Quiero agradecer primeramente a Dios por permitirme llegar a cumplir uno de mis tantos objetivos que me he propuesto en la vida, de igual forma agradecerle por haberme otorgado una maravillosa familia quienes siempre han confiado en mí, mis padres, mis hermanos, sobrinos y mi cuñada, ellos hacen que mi vida tenga sentido me han dado ejemplos de superación, humildad y sacrificio, a todos ellos les dedico el presente trabajo ya que sin ellos no hubiera llegado donde estoy en estos momentos.

A mis docentes ya que ellos aportaron con su granito de arena, conocimiento, amistad, y sobre todo consejos, todo esto me ha servido para ser un hombre de bien tanto en mi vida personal como profesional.

A Maycol por ser un buen amigo quien me ha ayudado en esta etapa universitaria.

Al Mayor Mario Ron Msc, por ser un buen docente y apoyarnos en este trabajo de titulación con su sabiduría.

Juan José Ruiz

Agradezco a mi familia quienes siempre han sido el motor para cada día esforzarme un poco más y a pesar de las circunstancias buenas o malas siempre permanecieron a mi lado, dándome su voto de confianza. Muchas gracias por sus consejos y palabras de aliento siempre tan oportunas y acertadas.

A mis docentes quienes fueron partícipes de tan riguroso camino, sembrando en mí el espíritu investigativo y alimentándome diariamente de su conocimiento, enseñanzas y experiencias vividas, que ahora las hago mías en la vida profesional.

Al Mayor Mario Ron, por su apoyo incondicional siempre predispuesto colaborar con su conocimiento a lo largo de este trabajo.

Maycol Pacha

## Índice de contenido

Herramienta de similitud de plagio copyleaks.....	2
Certificación .....	3
Responsabilidad de autoría.....	4
Autorización de publicación.....	5
Dedicatoria .....	6
Agradecimiento .....	7
Índice de contenido.....	8
Índice de tablas.....	12
Índice de figuras.....	13
Resumen.....	15
Abstract.....	16
Capítulo I.....	17
Introducción.....	17
Planteamiento del problema .....	18
Objetivos .....	22
General .....	22
Específicos .....	22
Justificación.....	23
Alcance.....	24
Capítulo II.....	27
Marco Metodológico.....	27
Estado del Arte.....	27
Planteamiento de la revisión de literatura preliminar .....	27
Criterios de inclusión y exclusión.....	28



	9
Criterios de inclusión .....	28
Criterios de exclusión .....	28
Grupo de control .....	28
Cadena de búsqueda.....	30
Proceso de selección.....	32
Resumen de los Estudios Primarios.....	33
Resumen general y conclusión del estado del arte .....	37
Metodología.....	38
Red de Categorías.....	40
Fundamentación Científica de la Variable Independiente .....	41
Gestión de TIC .....	41
Definición de Proceso .....	42
Clasificación de Procesos .....	42
Diagrama de flujo de Procesos.....	44
Mapa de Procesos .....	45
Racionalización de Procesos .....	46
¿Cómo racionalizar procesos? .....	46
Metodologías para racionalizar procesos.....	47
Business Process Management (BPM) .....	48
Six Sigma.....	49
Kaizen .....	50
Fundamentación Científica de la Variable Dependiente.....	51
Seguridad informática .....	51
CERT (Computer Emergency Response Team) .....	51
Normativa relativa a los CERT .....	51

	10
Revisión de la guía norteamericana para el manejo de incidentes informáticos	
NIST.SP.800-61r2 .....	52
INCIBE (Instituto Nacional de Ciberseguridad de España) .....	53
Revisión de la guía para la elaboración de una estrategia nacional de ciberseguridad mediante ITU (The International Telecommunication Union) .....	54
Estructura de un CERT .....	56
Servicios ofertados por los CERTs .....	56
Capítulo III .....	58
Introducción .....	58
Análisis comparativo de las metodologías para racionalizar procesos .....	58
Definición de la metodología ecléctica .....	60
Desarrollo metodológico de la racionalización de procesos .....	60
Análisis del Entorno .....	61
Mapa de Procesos .....	66
Norma de Procedimiento .....	68
Evaluación y Validación del proceso .....	73
Capítulo IV .....	87
Introducción .....	87
CONTENIDO .....	89
Prólogo .....	91
Introducción .....	92
Objetivo y campo de aplicación .....	93
Referencias normativas .....	93
Términos y condiciones .....	93
Público objetivo .....	94

	11
Autoridad .....	94
Descripción del documento.....	94
Mapa general de procesos.....	95
Roles y Funciones.....	96
Normas de procedimiento .....	97
Disposiciones generales .....	166
Disposiciones transitorias .....	166
Aprobación y legalización .....	166
Capítulo V .....	168
Conclusiones.....	168
Recomendaciones .....	169
Bibliografía .....	170

### Índice de tablas

Tabla 1 <i>Preguntas de Investigación</i> .....	25
Tabla 2 <i>Artículos que conforman el Grupo de Control</i> .....	29
Tabla 3 <i>Trazabilidad de la Cadena de Búsqueda</i> .....	31
Tabla 4 <i>Estudios Primarios</i> .....	32
Tabla 5 <i>Análisis comparativo de elementos para racionalizar procesos</i> .....	59
Tabla 6 <i>CERT- 01 Procesos Gobernantes</i> .....	68
Tabla 7 <i>CERT- 02 Procesos Generadores de valor</i> .....	69
Tabla 8 <i>CERT- 03. Procesos de apoyo</i> .....	71
Tabla 9 <i>Matriz de Priorización de Parámetros de Evaluación</i> .....	77
Tabla 10 <i>Rúbrica de evaluación de procesos</i> .....	79
Tabla 11 <i>Datos informativos de los Evaluadores</i> .....	82
Tabla 12 <i>Resumen de resultados de las Evaluaciones</i> .....	83
Tabla 13 <i>Análisis de Resultados</i> .....	84
Tabla 14 <i>Control de cambios</i> .....	90
Tabla 15 <i>Roles y Funciones Propuestos para el (ESPE-CERT)</i> .....	96
Tabla 16 <i>Código de servicios ofertados por el ESPE-CERT</i> .....	104

## Índice de figuras

Figura 1 <i>Principales causas de la dificultad en la gestión operacional de los servicios del ESPE-CERT</i> .....	19
Figura 2 <i>Causas de la demora en el tiempo de atención y respuesta a los clientes</i> .....	19
Figura 3 <i>Causas de los procesos y procedimientos operativos no racionalizados</i> .....	20
Figura 4 <i>Efectos de la problemática central</i> .....	21
Figura 5 <i>Árbol de problemas</i> .....	21
Figura 6 <i>Red de categorías correspondiente a la variable independiente</i> .....	40
Figura 7 <i>Red de categorías correspondiente a la variable dependiente</i> .....	41
Figura 8 <i>Esquema gráfico de un proceso</i> .....	42
Figura 9 <i>Tipos de Procesos</i> .....	43
Figura 10 <i>Servicios de un CERT</i> .....	57
Figura 11 <i>Metodología ecléctica para racionalizar procesos</i> .....	60
Figura 12 <i>Modelo organizacional por procesos</i> .....	65
Figura 13 <i>Procesos y Procedimientos generadores de valor</i> .....	67
Figura 14 <i>Cabecera de la ficha de procesos y procedimientos</i> .....	72
Figura 15 <i>Control de versionamiento y datos informativos de los procesos y procedimientos</i> ..	72
Figura 16 <i>Mapa General de Procesos ESPE-CERT</i> .....	95
Figura 17 <i>Estructura del código de ticket</i> .....	104
Figura 18 <i>CERT-02.01.01 Mesa de servicios</i> .....	107
Figura 19 <i>CERT-02.01.02 Gestión de Incidentes</i> .....	112
Figura 20 <i>CERT-02.01.03 Análisis de Vulnerabilidades</i> .....	119
Figura 21 <i>CERT-02.01.04 Monitoreo y alerta de primer nivel</i> .....	124
Figura 22 <i>CERT-02.01.05 Investigación Forense</i> .....	130
Figura 23 <i>CERT-02.01.06 Evaluación técnica de la seguridad de la información</i> .....	135

Figura 24 <i>CERT-02.01.07 Asesoramiento Técnico y Consultoría</i> .....	140
Figura 25 <i>CERT-02.01.08 Entrenamiento en el Ámbito de Ciberseguridad y Ciberdefensa</i> ....	147
Figura 26 <i>CERT-02.02.1 Investigación, Desarrollo e Investigación (I+D+i) de Artefactos</i> .....	158
Figura 27 <i>CERT-02.02.02 Procedimiento Sensibilización y Elaboración de materiales</i> .....	165

## Resumen

En línea con el crecimiento de Internet y las redes de datos, también lo han hecho las actividades tecnológicas que afectan negativamente a las personas y organizaciones, tales como; el robo de información, las pérdidas económicas, las repercusiones legales, la pérdida de credibilidad, las sanciones económicas e incluso afectaciones políticas y constitucionales.

Por lo tanto, se desarrolló un manual de procesos operativos basado en estándares y buenas prácticas a nivel internacional, que permita la gestión operacional del Equipo de Respuesta ante Incidentes Informáticos de la Universidad de Las Fuerzas Armadas (ESPE-CERT), al entregar una guía donde se especifican de manera metódica cada una de las actividades que soportan los servicios operacionales ofertados por la organización. La metodología utilizada para realizar la investigación fue (Ad-hoc) donde se aplicó las actividades de investigación, diseño, validación y evaluación. Además, se empleó una metodología ecléctica que reúne los mejores elementos para la racionalización de los procesos definidos para la organización, así como también, los diagramas de flujo de cada una de las actividades de acuerdo a los procedimientos que soportan los servicios proactivos y reactivos identificados en el CERT.

Al finalizar la investigación se pudo concluir que el manual de procesos operativos coadyuva en la gestión y mejora el rendimiento operacional en cuanto a la optimización de tareas y tiempos de respuesta de cada una de las peticiones solicitadas por parte de los clientes.

*Palabras clave:* buenas prácticas, procesos, incidente informático, cert.

### **Abstract**

In line with the growth of the Internet and data networks, so have technological activities that negatively affect people and organizations, such as; information theft, economic losses, legal repercussions, loss of credibility, economic sanctions and even political and constitutional effects.

Therefore, a manual of operational processes based on standards and good practices at the international level was developed, which allows the operational management of the Computer Incident Response Team of the University of the Armed Forces (ESPE-CERT), by providing a guide where each of the activities that support the operational services offered by the organization are specified in a methodical manner. The methodology used to carry out the research was (Ad-hoc) where the research, design, validation and evaluation activities were applied. In addition, an eclectic methodology was used that brings together the best elements for the rationalization of the processes defined for the organization, as well as the flow charts of each of the activities according to the procedures that support the proactive and reactive services identified. in the CERT.

At the end of the investigation, it was possible to conclude that the manual of operational processes helps in the management and improves operational performance in terms of optimizing tasks and response times of each of the requests requested by customers.

*Key words:* good practices, processes, computer incident, cert.



## Capítulo I

### Introducción

En los últimos años las redes de información se han convertido en una parte fundamental de nuestro diario vivir. Por ende, hoy por hoy gracias a la Internet, todo tipo de organización sean educativas, médicas, gubernamentales o financieras utilizan la red para la gestión y administración de sus datos e información, sin embargo, los avances en tecnología e investigación han dado paso a la existencia de distintos peligros como, suplantación de identidad, acceso no consentido a un sistema informático, interceptación ilegal de datos, revelación ilegal de base de datos, entre otros (Dentzel, 2013).

La ciberseguridad pretende salvaguardar a los sistemas digitales de usos no autorizados previniendo amenazas que pongan en riesgo su información (Academy Cisco Networking, 2020). Una de las prácticas que tratan de proteger a los sistemas digitales es la consolidación de un CERT (Computer Emergency Response Team), el cual se encarga de desarrollar medidas proactivas y reactivas ante incidencias de seguridad (Mendoza, 2015). El propósito de implantar un grupo de respuesta ante incidentes informáticos, es establecer un único punto de contacto dentro de las organizaciones para el manejo de incidentes, la recepción de notificaciones y el análisis de las vulnerabilidades (Haller et al., 2011).

Según (Egas et al., 2017) los CERT Nacionales se han implementado en muchos países de América Latina para ayudar a las instituciones estatales a cumplir con los requisitos de seguridad. Sin embargo, a menudo no han logrado los resultados deseados debido a la falta de experiencia técnica o de recursos, lo que ha llevado a varias universidades de la región a tomar conciencia de que no existen mecanismos enumerados que ayuden a proteger la información, particularmente de sus sistemas más críticos, Apenas una o dos Universidades de cada país en la región han construido CSIRT Académicos de forma eficaz, promoviendo el uso

buenas prácticas, estándares a nivel internacional y la formación de un personal idóneo que refuerce las unidades de seguridad de la información.

### **Planteamiento del problema**

La problemática que será abordada en esta investigación es la dificultad en la gestión operacional de los servicios ofertados por el ESPE-CERT.

La Biblioteca de Infraestructura de Tecnología de la Información (ITIL) publicó un informe sobre el estudio en 2019. “Incidencia de la Gestión Operativa en la Calidad del Servicio” (ITIL, 2019), en donde se estudiaron las situaciones de diferentes organizaciones en torno a la relación existente entre la gestión operativa y la calidad de los servicios ofertados por las mismas. Los principales desafíos encontrados tras el análisis de la situación son:

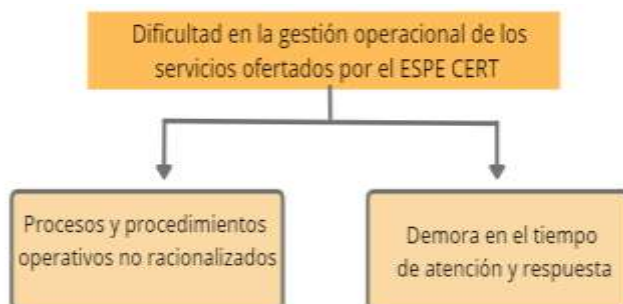
- Las empresas desconocen los beneficios de la gestión operativa o simplemente no saben cómo aplicarla en su negocio.
- Los procesos internos no están claramente documentados, se carece de planes de control o de hojas de procesos.
- Desconocimiento de los servicios de la organización.
- Procesos operativos no racionalizados.
- Demoras en el tiempo de atención y respuesta frente a las peticiones de los clientes.
- Personal no capacitado debido al desconocimiento de la totalidad de los servicios que existen en la empresa, así como también, las actividades que corresponden a dichos servicios.

Teniendo en cuenta estos factores, se identificó como principal problema la dificultad en la operación de los servicios que brinda la ESPE-CERT y sus principales causas del problema;

la demora en el tiempo de atención en las peticiones de los clientes y procesos operativos no racionalizados (ver Figura 1).

### Figura 1

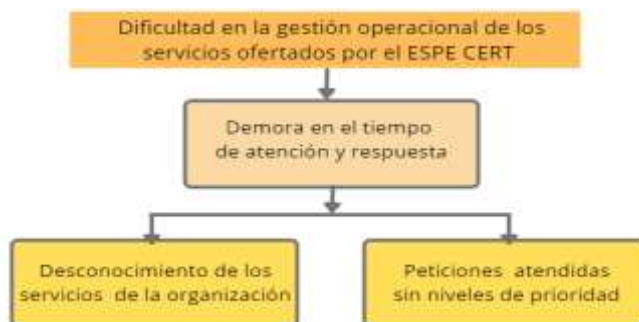
*Principales causas de la dificultad en la gestión operacional de los servicios del ESPE-CERT.*



La demora en el tiempo de atención y respuesta se debe principalmente a que los colaboradores desconocen en su totalidad los servicios y cada una de las actividades que apoyan a dichos servicios, por lo que destinan mucho tiempo realizando tareas repetitivas y monótonas impidiendo que su esfuerzo se enfoque en actividades más trascendentales y que aporten mayores beneficios (ver Figura 2).

### Figura 2

*Causas de la demora en el tiempo de atención y respuesta a los clientes.*



Los procesos operativos no racionalizados se suscitan principalmente por la ausencia de información concerniente a las actividades y tareas que engloban dichos procesos en las organizaciones, adicionalmente, es preciso destacar la falta de interés de las empresas al no destinar los recursos adecuados en favor del control y mejoramiento de sus servicios. Finalmente, sin una estructura operativa sólida, la organización pierde competitividad y no puede destacar entre sus competidores, además, cuando la estructura de gestión operativa es limitada perjudica a todas las áreas ya que todo está interconectado (ver Figura 3).

### Figura 3

*Causas de los procesos y procedimientos operativos no racionalizados.*

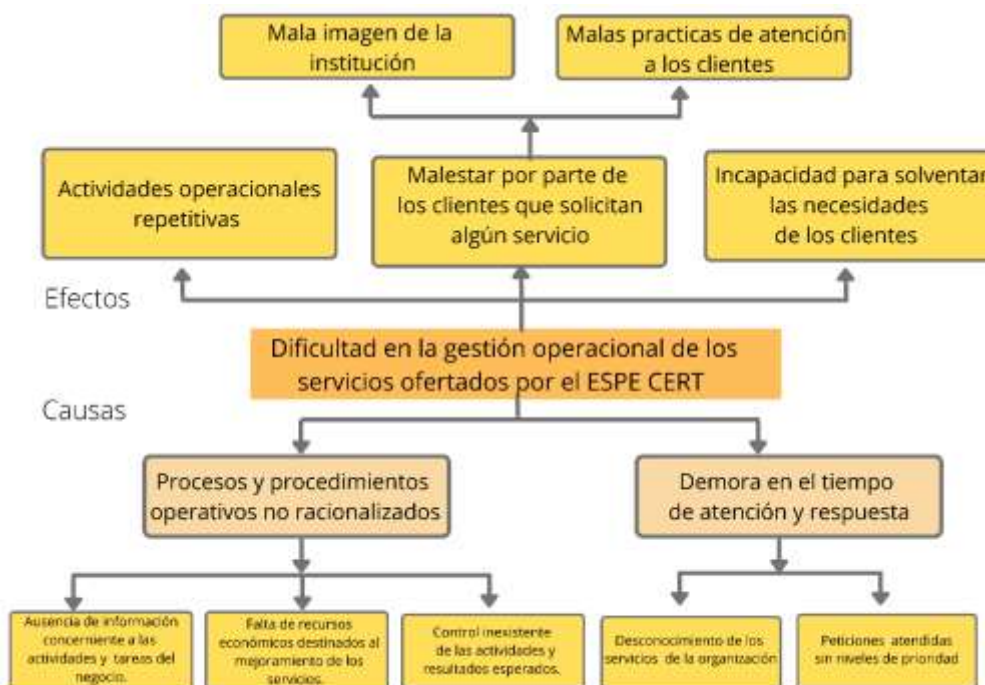


Después de haber discutido todos los factores que contribuyeron al problema, los efectos que son más indicativos del problema son los clientes insatisfechos que solicitan algún tipo de servicio, principalmente porque no se utilizan técnicas de seguimiento y control, lo que resulta en efectos que dañan la reputación de la empresa, desperdiciando tiempo y recursos. (González, 2018).

Por otra parte, las actividades operativas ejecutadas por los funcionales a cargo son repetitivas y monótonas, además, son ejecutadas sin tomar en cuenta ningún procedimiento, y mucho menos manuales o guías, impactando negativamente en los servicios que ofrece la institución a sus clientes. (ver Figura 4).

**Figura 4***Efectos de la problemática central*

A manera de resumen, en la Figura 5 se muestra un árbol de problemas que conecta el problema principal con sus causas y efectos.

**Figura 5***Árbol de problemas*

Esto sirvió de motivación para proponer el desarrollo de un manual de procesos operativos, que permita establecer un documento guía donde se describen de manera

secuencial cada una de las actividades que deben seguirse en la realización de las funciones de los servicios ofertados por la institución, así como también, políticas, tiempos, recursos y diagramas de flujo. Permitiendo de esta manera mejorar el control interno y tomar las medidas adecuadas en torno a una mejor calidad de servicio que influye directamente en la satisfacción de los clientes.

## **Objetivos**

### ***General***

Desarrollar un manual de procesos operativos para el CERT académico de la Universidad de las Fuerzas Armadas “ESPE”, utilizando estándares a nivel internacional mediante una racionalización de procesos, a fin de ofrecer una herramienta de trabajo que permita la operación del CERT coadyuvando en la mejora de los servicios ofertados a la comunidad universitaria.

### ***Específicos***

- Identificar estudios relacionados con el bajo desempeño y la falta de operatividad de un CERT, mediante una revisión de literatura preliminar.
- Realizar una revisión sistemática de las buenas prácticas y estándares a nivel internacional para la operación de un equipo de respuesta ante incidentes informáticos.
- Elaborar la norma de procedimientos de los procesos operativos identificados de acuerdo a su nivel crítico.
- Diseñar los diagramas de flujo de acuerdo a las actividades identificadas en cada uno de los procedimientos que soportan los servicios proactivos y reactivos ofertados por el ESPE-CERT.
- Elaborar la rúbrica de evaluación y matriz de priorización de parámetros para determinar la validez de los procesos.

## Justificación

La necesidad del mejoramiento de la gestión operacional y de la sistematización de los procesos y procedimientos del CERT académico, además de cumplir con la disposición de las autoridades de la Universidad, en el sentido de dar una pronta solución a los incidentes informáticos y al adecuado resguardo de la información institucional, ya que constituye uno de los activos más importantes debido a la gran cantidad de información sensible que se maneja en la comunidad universitaria.

De acuerdo con el informe anual de ciberseguridad de Cisco presentado en el año 2020, los tipos más comunes de ataques cibernéticos registrados en instituciones educativas son (Alvarado, 2020):

- Infección de computadores dentro de una red.
- Infección de servidores.
- Conexión con servidores externos maliciosos.
- Falta de control en el manejo de la estructura de TI dentro de las instituciones.
- Falta de control a los usuarios en los diferentes sistemas dentro de la institución.
- Acceso no autorizado a datos de estudiantes, profesores y personal administrativo, etc.

El presente proyecto de titulación se enfoca en dar respuesta inmediata a los incidentes informáticos que se suscitan en la Universidad de las Fuerzas Armadas “ESPE”, entregando así un Manual de Procesos Operativos práctico que facilite la gestión operacional y ayude en la formación y capacitación del personal que opera en el ESPE-CERT, fomentando el uso de buenas prácticas, estándares internacionales y promoviendo a la investigación activa (Hurtado, 2018).

Por lo tanto, al tener una cultura de calidad en todos los procesos de la organización, se conseguirá mejorar el rendimiento operacional permitiendo de esta manera dar una pronta respuesta a los incidentes informáticos que se presenten, además la estandarización aportará a que se pueda conseguir procesos maduros y eficientes con enfoque al mejoramiento continuo.

### **Alcance**

La actual investigación constituye la primera fase del proyecto de investigación “Diseño e Implementación del sistema de gestión de servicios e infraestructura de TI para el CERT Académico de la ESPE”, el cual fue creado como base esencial para la estructuración organizacional por procesos del CERT Académico constituida por todas las actividades metodológicas de racionalización de sus procesos operacionales, basado en los servicios determinados en el trabajo de titulación: “Implantación y Puesta en Marcha de un CSIRT Académico de Respuesta a Incidentes de Seguridad de la Información en el Departamento de Informática de la Universidad de las Fuerzas Armadas de España (ESPE)” desarrollado por el Ing. Jonathan Benavides en 2020, el trabajo está formado desde una revisión sistemática de las buenas prácticas vigentes, el mapa de procesos en base de los servicios definidos, la racionalización de estos procesos que su propósito es encontrar la mejor solución aceptable dentro de la situación real del CERT, para que, en base de esto, elaborar la norma de procedimiento, es decir el documento formal de práctica de cada proceso, para finalmente conformar el Manual de Procesos Operativos, que será aprobado formalmente por el nivel normativo o de control del CERT.

Se han establecido numerosas preguntas de investigación que están directamente relacionadas con los objetivos específicos propuestos con el fin de precisar el alcance del trabajo de titulación propuesto. (ver Tabla 1).



**Tabla 1***Preguntas de Investigación*

<b>Objetivos Específicos</b>	<b>Preguntas de Investigación</b>
<b>OE1:</b> Identificar estudios relacionados con el bajo desempeño y la falta de operatividad de un CERT, por medio de una revisión de literatura preliminar.	<p><b>RQ1</b> ¿Qué solución es la más adecuada, para determinar el buen desempeño de un CERT?</p> <p><b>RQ2</b> ¿Cuáles son las causas que afectan al desempeño operacional de un CERT?</p> <p><b>RQ3</b> ¿Qué recomiendan otros estudios para mejorar el desempeño operacional en un CERT?</p>
<b>OE2:</b> Realizar una revisión sistemática de las buenas prácticas y estándares a nivel internacional para la operación de un equipo de respuesta ante incidentes informáticos.	<p><b>RQ4</b> ¿Qué estándares y buenas prácticas son utilizadas a nivel internacional para mejorar la operatividad en el tiempo de respuesta ante incidentes informáticos en el CERT?</p> <p><b>RQ5</b> ¿De qué manera ayudan los estándares internacionales a mejorar el desempeño en las instituciones?</p>
<b>OE3:</b> Elaborar la norma de procedimientos de los procesos operativos identificados de acuerdo a su nivel crítico.	<p><b>RQ6</b> ¿Cómo se realiza una norma de procedimientos?</p> <p><b>RQ7</b> ¿De qué manera se identifican los procesos operacionales dentro de las organizaciones?</p>

Objetivos Específicos	Preguntas de Investigación
<p><b>OE4:</b> Diseñar los diagramas de flujo de acuerdo a las actividades identificadas en cada uno de los procedimientos que soportan los servicios proactivos y reactivos ofertados por el ESPE-CERT.</p>	<p><b>RQ8</b> ¿Qué herramientas se utilizan para diseñar diagramas de flujo?</p> <p><b>RQ9</b> ¿Cuáles son los porcentajes mínimos aceptables para que los procesos sean aprobados mediante la rúbrica de evaluación?</p>
<p><b>OE5:</b> Elaborar la rúbrica de evaluación y matriz de priorización de parámetros para determinar la validez de los procesos.</p>	<p><b>RQ10</b> ¿Cómo se clasifican los procesos de acuerdo a su nivel crítico?</p> <p><b>RQ11</b> ¿Qué técnicas se han utilizado para la valoración de los procesos operativos a fin de evaluar su rendimiento?</p>

*Nota: Esta tabla muestra los objetivos específicos, con sus respectivas preguntas de investigación.*

## **Capítulo II**

### **Marco Metodológico**

Este capítulo introduce el estudio del estado del arte, seguido de una descripción de la metodología a utilizar en el proyecto, destacando cada tarea a realizar para cada etapa del modelo de investigación de la propuesta Ad-Hoc, y finalmente desarrollando el marco teórico, a través del desarrollo de una red de categorías.

#### **Estado del Arte**

Para llevar a cabo el estado del arte de la presente investigación se realizó una búsqueda exhaustiva de la información con la finalidad de identificar las fuentes más relevantes para el desarrollo del Manual de Procesos Operativos, basados en un proceso de revisión de literatura semi inicial apoyado en las guías de revisión sistemática de literatura propuestas por (Kitchenham, Budgen, & Brereton, 2015). A continuación, en la figura 6 se muestran las actividades que se consideraron para este proceso.

#### **Planteamiento de la revisión de literatura preliminar**

En esta fase se realizó una breve descripción del problema de investigación el cual fue abordado en la sección denominada Planteamiento del problema; posteriormente se procedió a definir un objetivo el cual corresponde al objetivo específico OE1 y plantear las preguntas de investigación las cuales se encuentran detalladas en la sección denominada Alcance. Finalmente, se definieron los criterios de inclusión y exclusión para la obtención del grupo de control y para guiar todo el proceso de revisión.

## **Criterios de inclusión y exclusión**

### ***Criterios de inclusión***

- Artículos que presenten propuestas, metodologías de análisis y racionalización de procesos fáciles de implementar y enfocados principalmente a mejorar el rendimiento operacional de un CERT.
- Artículos en los cuales se reportan estudios acerca de marcos de trabajo, uso de buenas prácticas y estándares a nivel internacional para la evaluación de la efectividad del desempeño de un CERT.
- Artículos en los cuales se trate de la implementación y puesta en marcha de herramientas de respuesta a incidentes de seguridad de la información (CERT).
- Artículos publicados entre 2010 a 2022.

### ***Criterios de exclusión***

- Artículos en los que el enfoque sea centrado netamente en detalles técnicos de un CERT.
- Fuentes de información que no estén catalogadas en bases digitales reconocidas.
- Artículos publicados antes de 2010 y escritos en un idioma distinto al inglés.

## **Grupo de control**

Con el establecimiento de los criterios de inclusión y exclusión se procede a definir o delimitar varios artículos que cumplen con dichos criterios, con el fin de que se eliminen aquellos estudios científicos que no estén alineados con el objetivo de la investigación (Petersen et al., 2008).

Para la conformación del grupo de control fue primordial la colaboración de tres investigadores. Con el propósito de que cada uno haga su aportación, proponiendo estudios

que pueden ser parte del grupo de control. Finalmente, por medio de una validación cruzada se estableció el grupo de control con el cual se va a trabajar, el cual se muestra en la Tabla 2.

**Tabla 2**

*Artículos que conforman el Grupo de Control.*

<b>Código</b>	<b>Título</b>	<b>Términos relevantes</b>
EC1	Intelligent Method for CSIRT Performance Evaluation in Critical Information Infrastructure.	CSIRT, KPI, Correlation Matrix, Efficiency, Critical Information Infrastructure.
EC2	Computer Security Incident Response Team Effectiveness: A Needs Assessment.	Incident handling, team performance, CSIRT, collaborative sensemaking, internal communication, CERT, team cognition.
EC3	Improving cybersecurity incident response team (csirt) skills, dynamics and effectiveness.	Cyber incident response, response teams, cognitive task analysis, team performance, low performance, CERT, Teams-Based Research.
EC4	Chronic workload problems in CSIRTs.	Information Security, Incident Response, Incident Management,

<b>Código</b>	<b>Título</b>	<b>Términos relevantes</b>
		CERT, CSIRT, Risk Management, System Dynamics.
EC5	Improving Cybersecurity Incident Response Team Effectiveness Using Teams-Based Research.	Team adaptation, shared knowledge, protection of digital, teamwork, computer security, problem-solvin.

*Nota: La tabla muestra los artículos seleccionados por los investigadores para formar del grupo de control.*

Tras un análisis de los estudios realizados por el grupo de control, se eligieron palabras clave que debían alinearse estrechamente con los objetivos de la investigación entre las que aparecen con mayor frecuencia en artículos científicos relacionados. Como consecuencia, se pudo identificar las siguientes palabras clave: RESOLUCIÓN DE PROBLEMAS, MANEJO DE INCIDENCIAS, TRABAJO EN EQUIPO, SEGURIDAD INFORMÁTICA, CERT, CSIRT, EQUIPO DE RESPUESTA, BAJO RENDIMIENTO.

### **Cadena de búsqueda**

En la forma final de la consulta de búsqueda se encuentran los contextos según la investigación con la que se decidió trabajar. Se localizan las tres versiones que tenía la consulta de búsqueda. La consulta de búsqueda tenía muchas versiones con varias palabras clave obtenidas de los artículos del grupo de control. detalladas en la Tabla 3.

Se abandonó la versión inicial ya que no se podían encontrar todos los contextos en el buscador. La segunda versión mostró una cantidad considerable de artículos, pero la mayoría

no tenía nada que ver con el tema de investigación. La tercera versión, que tuvo en cuenta todos los contextos definidos en el grupo de control, fue la definitiva.

**Tabla 3**

*Trazabilidad de la Cadena de Búsqueda*

<b>Versión</b>	<b>Número de Artículos obtenidos</b>	<b># Resultados</b>
1	ALL((CERT or CSIRT) and (RESPONSE TEAM or TEAMWORK) and (COMPUTER INCIDENT or COMPUTER SECURITY) and (KPI or TEAM PERFORMANCE))	130
2	ALL((CERT or CSIRT RESPONSE TEAM) and (TEAM PERFORMANCE or TEAMWORK) and (COMPUTER INCIDENT or COMPUTER SECURITY) and (KPI or PROBLEM-SOLVING))	50
3	ALL ((CERT or CSIRT or RESPONSE TEAM) and (INFORMATIC SECURITY OR COMPUTER INCIDENT) and (TEAMWORK or TEAM PERFORMANCE) and (LOW PERFORMANCE or BAD RESULTS))	20

*Nota: La tabla muestra la trazabilidad de la cadena de búsqueda basándonos en términos obtenidos por los artículos seleccionados en el grupo de control por los investigadores.*

Después de realizar varias pruebas con distintas combinaciones de cadenas, se seleccionó la cadena que corresponde a versión número 3: ALL ((CERT or CSIRT or RESPONSE TEAM) and (INFORMATIC SECURITY OR COMPUTER INCIDENT) and (TEAMWORK or TEAM PERFORMANCE) and (LOW PERFORMANCE or BAD RESULTS))

### Proceso de selección

Al usar el motor de búsqueda de IEEE Xplore en la base de datos digital, un total de 20 artículos candidatos.

Una vez finalizada la revisión, se descargaron los textos completos de los estudios pertinentes y se leyeron para ver si cumplían con los criterios de inclusión y exclusión establecidos. Finalmente se realizó una validación cruzada entre los dos investigadores tesisistas al aplicar este filtro, se obtuvieron 9 estudios primarios que se listan en la Tabla 4.

**Tabla 4**

*Estudios Primarios*

<b>Código</b>	<b>Título</b>	<b>Cita</b>
<b>EP1</b>	A Management Model for Building a Computer Security Incident Response Capability.	(Mooi & Botha, 2016)
<b>EP2</b>	Improving Cybersecurity Incident Response Team Effectiveness Using Teams-Based Researches.	(Steinke, y otros, 2015)
<b>EP3</b>	Cybersecurity Culture in Computer Security Incident Response Teams: Investigating difficulties in communication and coordination.	(Ioannou, Stavrou, & Bada, 2019)



Código	Título	Cita
EP4	Improving cybersecurity incident response team (csirt) skills, dynamics and effectiveness.	(Steinke, y otros, 2015)
EP5	Adding the fourth "R" [CERT's model for computer security strategies].	(Endicott-Popovsky & Frincke, 2005)
EP6	Computer Security Incident Response Team.	(Mooi & Botha, 2016)
EP7	Dimensional data model for early alerts of malicious activities in a CSIRT	(Valladares, Fuertes, Tapia, Toulkeridis, & Pérez, 2017)
EP8	The Organisation of Islamic Conference — Computer Emergency Response Team(OIC-CERT): Answering cross border cooperation	(Ahmad & Hashim, 2011)
EP9	Security Research at NASK: Supporting the Operational Needs of a CERT Team and More	(Kijewski & Kozakiewicz, 2011)

*Nota: La tabla muestra los artículos seleccionados por los investigadores para formar del grupo de estudios primarios.*

## Resumen de los Estudios Primarios

### EP1 (Mooi & Botha, 2016) **A Management Model for Building a Computer Security Incident Response Capability**

Este artículo tiene como propósito desarrollar un modelo de gestión en el cual se plantee un Equipo de respuesta a incidentes de seguridad informática (CSIRT). Para lo cual se ha elegido una perspectiva apoyada en la ciencia del diseño de todo el proyecto, aunque el presente documento trata sobre sobre las tres primeras actividades del estudio de la ciencia del

diseño, identificación del problema, planteamiento de objetivos con su respectiva solución y finalmente el desarrollo del modelo, se hace necesario una revisión exhaustiva de la literatura la cual tiene dos metas los cuales son: confirmar el problema y proporcionar una forma estructurada de revelar las áreas de requisitos.

**EP2 (Steinke, y otros, 2015) Improving Cybersecurity Incident Response Team Effectiveness Using Teams-Based Research.**

El correcto funcionamiento de los equipos de respuesta a incidentes de ciberseguridad (CSIRT) es esencial para la protección digital de la información, la cual es utilizada por las organizaciones y personas alrededor de todo el mundo. Aunque, debido a que los CSIRT en la actualidad son equipos totalmente nuevos para las personas, hace que aprovechar su efectividad no cumpla con las expectativas deseadas. Para lo cual, al mejorar el rendimiento y desarrollo de los CSIRT, los autores establecen áreas importantes que ayudan a los CSIRT a funcionar eficazmente como equipo de respuesta a estos incidentes. Exactamente, se centran en la adecuación del equipo, la resolución de problemas, la comunicación, la confianza y el desarrollo del conocimiento compartido entre los miembros del equipo.

**EP3 (Ioannou, Stavrou, & Bada, 2019) Cybersecurity Culture in Computer Security Incident Response Teams: Investigating difficulties in communication and coordination.**

La presente investigación tiene como propósito identificar todos los factores que tengan relación con la creación de una cultura de ciberseguridad en un entorno organizacional y además enfrentando las dificultades para la comunicación dentro de un CSIRT. Precisamente, los propósitos principales son identificar: 1) Los obstáculos que pueden restringir la comunicación y la organización del proceso en gestión de incidentes dentro de un CSIRT, 2) los obstáculos que pueden restringir la contribución de la alta dirección a los empleados y

revertir y 3) los puntos de vista para tratar las cuestiones que restringen la comunicación y la organización de un CSIRT. Para obtener un punto de vista más objetivo se realizó una encuesta en línea a personas que tenían conocimientos en el área de seguridad de la información implementados a un CSIRT.

**EP4 (Steinke, y otros, 2015) Improving cybersecurity incident response team (csirt) skills, dynamics and effectiveness.**

Para que un (CSIRT) tenga un mejor rendimiento es necesario que cumpla con tres objetivos principales los cuales son minimizar y controlar el daño, analizar el incidente, evitar la ocurrencia de incidentes similares. Los objetivos antes mencionados se centran en proporcionar una respuesta eficaz a estos incidentes, limitando el daño para que los riesgos sean menos peligrosos, para esto se crean culturas dentro de las organizaciones para que sepan cómo actuar ante estos incidentes que se suscitan a diario. Finalmente se pueden seguir normas y estándares a nivel internacional para que los operadores que se encargan del control del CSIRT puedan tener una guía de cómo se debe proceder ante los incidentes de seguridad informática.

**EP5 (Endicott-Popovsky & Frincke, 2005) Adding the fourth "R" [CERT's model for computer security strategies.**

En este artículo se habla del cumplimiento de estándares, que se definen como la cualidad de un sistema de cumplir con sus propósitos de manera adecuada, ante la concurrencia de fallas, ataques y accidentes. No obstante, las soluciones mencionadas anteriormente como firewalls, PKI y VPN se enfocan en bloquear ataques, experimentando una supervivencia para así poder recuperarse rápidamente a estos ataques. A continuación, se menciona un modelo 3 R de CERT (resistencia, reconocimiento y recuperación) el cual nos

describe una táctica enfocada en la supervivencia, aumentando la seguridad de los intrusos para no tener consecuencias legales y no ser víctima de los piratas informáticos. Esto nos lleva a aumentar una cuarta R a este modelo, el cual se enfocará básicamente en la recuperación inmediata a estos ataques.

**EP6 (Mooi & Botha, 2016) Computer Security Incident Response Team.**

En el presente documento se identificó unos requisitos comerciales por parte de La Red Nacional de Investigación y Educación (NREN) de Sudáfrica (SA), las cuales están asociadas a cinco áreas que son: autoridad, medio ambiente, comunidad, financiación y las consideraciones legales. En el sector académico el CSIRT de NREN se estableció como un CSIRT, el cual sirve a la comunidad de investigación y educación de Sudáfrica. Además, existen dos organizaciones y un correspondiente modelo organizacional integrado que pertenecen a la NREN.

**EP7 (Valladares, Fuertes, Tapia, Toulkeridis, & Pérez, 2017) Dimensional data model for early alerts of malicious activities in a CSIRT.**

Con el pasar del tiempo han crecido y evolucionado las vulnerabilidades, amenazas y ciberataques, lo cual genera que los incidentes de seguridad tengan un gran impacto negativo dentro de las organizaciones. Para lo cual se presentó un sistema de procesamiento analítico llamado (OLAP) en cual consiste en alertas tempranas de actividades maliciosas. El propósito de este estudio es brindar apoyo en ciberseguridad a los (CSIRT), con el fin de establecer un mecanismo que analice y mejore los niveles de seguridad en las redes, implementando servicios de alerta temprana a todos los equipos de la organización. Con el fin de cumplir con estas tareas, se ha creado una solución de Business Intelligence la cual utiliza una metodología de Ralph Kimball que ayuda en el análisis de incidentes de seguridad informática.

**EP8 (Ahmad & Hashim, 2011) The Organisation of Islamic Conference - Computer Emergency Response Team (OIC-CERT): Answering cross border cooperation.**

En la actualidad el acelerado crecimiento de las infraestructuras y sistemas de red de la tecnología de la información y la comunicación (TIC) han provocado que la Internet no disponga de fronteras dando lugar a que se puedan mitigar delitos cibernéticos transfronterizos. Al percatarse del peligro y el gran impacto de este asunto los (CSIRT) o (CERT) han realizado colaboraciones regionales e internacionales con el fin de hacer frente a las ciberamenazas transfronterizas, para así colaborar con mejores prácticas, desafíos e inteligencia y conocer de los errores de otros, coadyuvando a impulsar y formular iniciativas referentes a políticas internacionales, las cuales ayudarán a países miembros a proteger su infraestructura de información que se encuentra vulnerable.

**EP9 (Kijewski & Kozakiewicz, 2011) Security Research at NASK: Supporting the Operational Needs of a CERT Team and More.**

El presente artículo nos muestra una investigación actual enfocada en el área de seguridad informática de redes en NASK, guiándose en las actividades que realizan los equipos del CERT Polska y NISM. Algunas de estas actividades están fomentadas por las necesidades operativas de CERT Polska. Por ende, toda la investigación se centra en métodos de detección de amenazas, repartición de información relacionada con la seguridad e inteligencia de amenazas, con el objetivo de brindar mayor seguridad a todas las organizaciones que lo empleen.

**Resumen general y conclusión del estado del arte**

En un entorno en constante cambio, un equipo de respuesta a incidentes de seguridad informática (CERT) tiene que evolucionar para mantener o mejorar su operatividad. La tarea principal de un CERT es mitigar los efectos de los incidentes de seguridad informática. Los

problemas que se identifican con mayor frecuencia en los CERT son: sobrecarga de trabajo, falta de personal capacitado, mala gestión operacional, falta de financiación, entre otros. Esto conlleva a que no se pueda medir la efectividad ni tampoco mejorar su desempeño. Algunas soluciones que plantean los autores son las siguientes: Modelos de simulación dinámica de sistemas, Teoría de la mejora de procesos, Mejora de la eficacia del equipo de respuesta a incidentes de ciberseguridad mediante la investigación basada en equipos, Métodos inteligentes para la evaluación del desempeño CERT basados en Benchmarking.

### **Conclusiones:**

Concluida la revisión literaria se puede afirmar que varios autores hacen referencia a la problemática que gira en torno al mal rendimiento operacional de un CERT y las causas que eso conlleva en cuanto a la toma de decisiones, desconocimiento del protocolo de funcionamiento, evaluación del desempeño operativo, tiempos de operaciones y satisfacción de clientes. Donde se describe la importancia de la gestión correcta de los procesos operativos, aplicando modelos de simulación y teorías de mejora de procesos, entre otros. Sin embargo, a pesar de su importancia, los procesos operativos son un tipo de gestión cuyo único objetivo es mejorar el desempeño de una organización. Se componen de varias metodologías, no se encontraron estudios enfocados netamente a los mismos, razón por la cual se justifica la propuesta presentada en torno a la Elaboración de un Manual de Procesos Operativos para un CERT académico utilizando estándares a nivel internacional.

### **Metodología**

Para desarrollar el proyecto, teniendo en cuenta el alcance del tema, se consideró aplicar una metodología a medida (Ad-Hoc). La metodología de investigación se centra en un objetivo específico y busca producir una mayor comprensión del tema. Esta metodología va a contar con 6 fases, mismas que se detallan a continuación:

**Fase I: Revisión de literatura.** - Se realizará una revisión sistemática de literatura acerca de las buenas prácticas a nivel internacional para la operación de un equipo de respuesta ante incidentes informáticos.

**Fase II: Mapa de procesos.** - Se elabora el mapa detallado de los procesos y procedimientos operativos del CERT, en base de los servicios definidos del trabajo de titulación del Ing. Jonathan Benavidez, con la participación de los miembros del proyecto de investigación.

**Fase III: Análisis y racionalización de procesos.** - Utilizando la metodología de análisis y racionalización de procesos se definirán las mejores alternativas de cada proceso, probando su solución.

**Fase IV: Norma de procedimiento.** - Se elabora y documenta la norma de procedimiento de cada uno de los procesos seleccionados, de acuerdo al formato de la Norma Técnica NTE-ISO-IEC-9001.

**Fase V: Evaluación y Validación del proceso.** – Se realiza la evaluación y validación del proceso, mediante la implementación de la matriz de Holmes que permite establecer el rango máximo y mínimo aceptable que por cuestiones de calidad se lo define al 80% del cumplimiento total de los parámetros de evaluación definidos.

**Fase VI: Elaboración del Manual de Procesos Operativos:** En esta fase se realizará la propuesta del Manual de Proceso Operativos, su estructura y formato se basará en estándares internacionales.

## Marco Teórico

### Red de Categorías

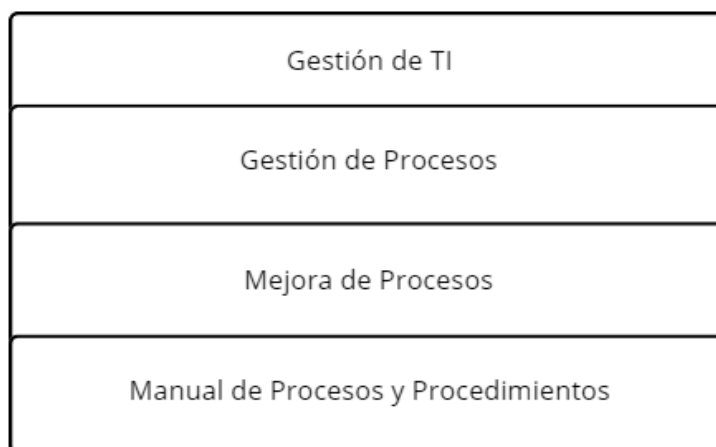
El propósito de la red de categorización es buscar la coherencia en los fundamentos teóricos del proyecto de investigación actual, con el fin de estructurar redes de categorías para la variable dependiente e independiente, cuya hipótesis está fundamentada en las variables antes mencionadas, las cuales se observan en las Figuras 7 y 8, respectivamente.

**VI:** Manual de procesos.

**VD:** Normativa para proveer servicio de respuesta ante incidentes informáticos.

### Figura 6

*Red de categorías correspondiente a la variable independiente.*

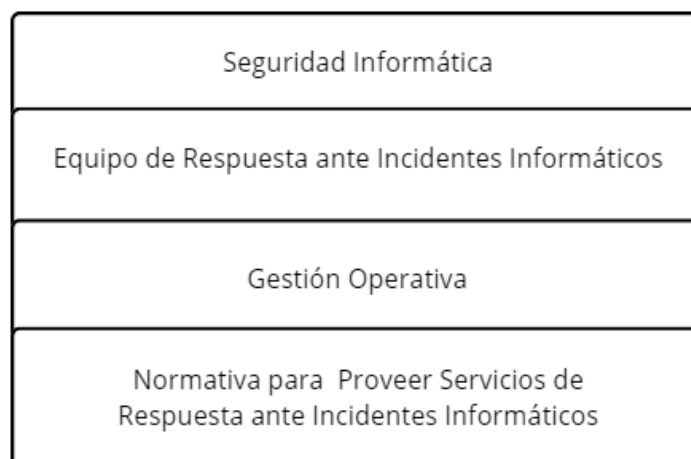


*Nota: El gráfico muestra la red de categorías de la VI, la cual está conformada desde el término más general hasta el específico.*



## Figura 7

*Red de categorías correspondiente a la variable dependiente*



*Nota: El gráfico muestra la red de clasificación de VD, que se compone de términos que van desde el más amplio hasta el más específico.*

## Fundamentación Científica de la Variable Independiente

### **Gestión de TIC**

Con el paso del tiempo las tecnologías han ido avanzando de forma acelerada, lo que hace que las tecnologías de la información y la comunicación (TIC), sean más vulnerables, obligando a las organizaciones a realizar una buena gestión en seguridad, para reducir el impacto en la distribución, transmisión, procesamiento y almacenamiento de información, con el fin de salvaguardar los activos de la organización. (Pazmiño, Serrano, & González, 2020)

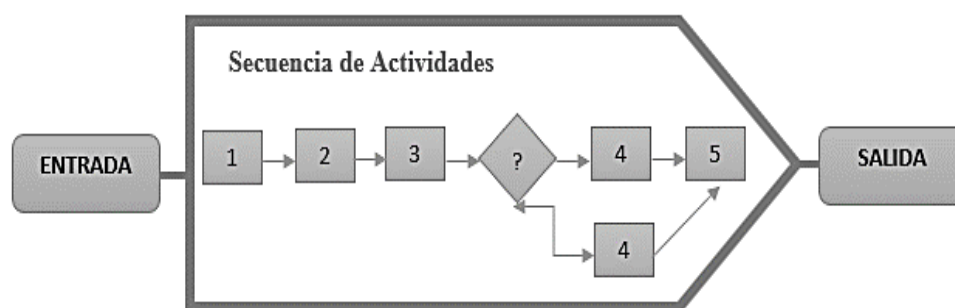
En la gestión de incidentes de seguridad, se hace necesario un tratamiento proactivo y reactivo, que permita prevenir, identificar, detener y/o minimizar ataques informáticos, permitiendo el monitoreo de todas las actividades que se desarrollan en la organización, por medio de herramientas automatizadas y procedimientos que son gestionados por el personal encargado de dichas tareas (Pazmiño, Serrano, & González, 2020).

### **Definición de Proceso**

Un proceso es una colección de actividades relacionadas que incluyen un equipo de personas que trabajan juntas y recursos materiales para cambiar las entradas, (materia prima, información) en salidas (bienes o servicios) para conseguir el objetivo previamente identificado. En la figura 8 se muestra la secuencia lógica de un proceso (Romero, 2020).

### **Figura 8**

*Esquema gráfico de un proceso*



*Nota: Los procesos se representan mediante flujogramas y los rendimientos se miden por medio de indicadores. Tomado de (Romero, 2020).*

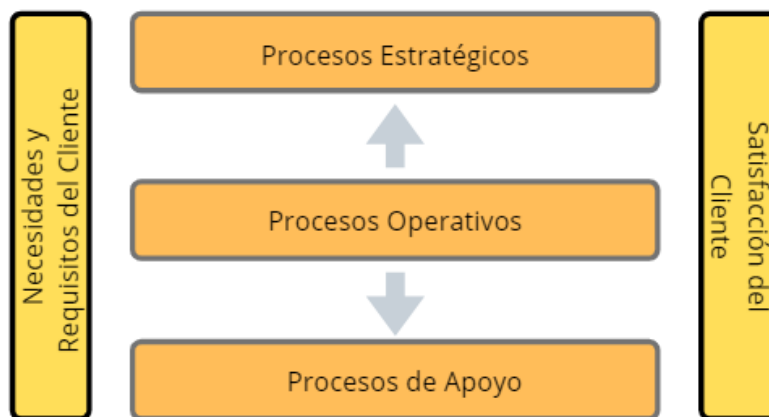
### **Clasificación de Procesos**

Dentro de toda organización se pueden identificar tres tipos de procesos (estratégicos, operativos y de apoyo), estos normalmente se llaman de diversas maneras, pero su objetivo sigue siendo el mismo.

En la figura 9 se puede visualizar los tres tipos de procesos que se detallarán a continuación.

## Figura 9

### *Tipos de Procesos*



*Nota: Los Tipos de procesos que las empresas pueden implementar a su organización dependiendo de la actividad que realizan.*

**Procesos Estratégicos:** Son aquellos procesos que definen el sentido y la manera en la que marcha la organización mediante la formulación de una estrategia que guíe y asegure la mejor forma de crear un bien o servicio el cual cumpla con las expectativas del cliente (Pérez, 2010).

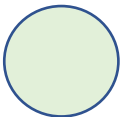
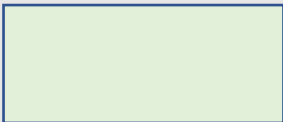
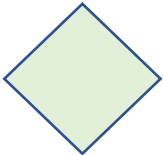
**Procesos Operativos:** Son aquellos procesos que se enfocan en gestionar los objetivos de la organización, cumpliendo con todas las actividades para tener un producto o servicio terminado que satisfaga las necesidades del cliente (López, 2011).

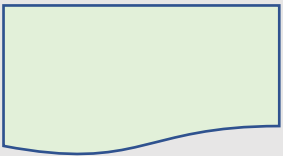
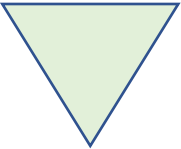
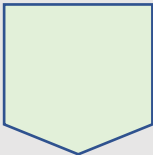
**Procesos de Apoyo:** Son aquellos procesos que se encargan de cooperar con los recursos necesarios para que los demás procesos (operacionales y estratégicos) puedan operar de manera oportuna. Siendo este proceso una actividad complementaria que no afecta a la calidad del producto, servicio o la satisfacción del cliente (López, 2011).

### **Diagrama de flujo de Procesos**

Los diagramas de flujo de procesos tienen por objetivo ilustrar una serie de actividades que componen a un proceso y saber quiénes son los encargados de ejecutar cada una de estas actividades, de tal forma que se muestre la importancia de cada actividad en la realización de cada proceso con el fin de determinar los puntos críticos que sean susceptibles a cambios (Agudelo, 2007).

La ANSI (American National Standards Institute) ha establecido los símbolos para la elaboración de diagramas de flujo, presentados en la tabla 5.

<b>Símbolo</b>	<b>Nombre</b>	<b>Descripción</b>
	Inicio o término	Este símbolo muestra el inicio o el fin del flujo, se relaciona a una acción o lugar.
	Actividad	Este símbolo especifica las funciones que realizan las personas involucradas en el procedimiento.
	Decisión o alternativa	Este símbolo especifica un punto dentro del flujo para tomar una elección entre dos o más posibilidades.

Símbolo	Nombre	Descripción
	Documento	Este símbolo representa un documento en general.
	Archivo o almacenamiento	Este símbolo muestra el resguardo de un documento o producto de forma temporal o permanente
	Conector de página	Este símbolo muestra un enlace o conexión con otra hoja diferente, que indica la continuación del diagrama de flujo.

*Nota: La tabla muestra los símbolos que se utilizarán para diagramar los procesos operativos.*

### **Mapa de Procesos**

Un manual de procesos es un documento indispensable que engloba información sobre (políticas, normas, estándares, reglamentos, historia y procedimientos de una empresa), de forma organizada y sistemática que son necesarios para un buen desarrollo del trabajo. Contribuyendo a la sistematización de las actividades a realizar dentro de la organización, permaneciendo estas documentadas para que se puedan utilizar en cualquier momento. Los manuales de procesos forman parte de un documento técnico que abarca datos relacionados con las actividades y tareas que ayudan a orientar de manera eficiente a los trabajadores (Toro, 2015).

### ***Racionalización de Procesos***

La racionalización de procesos es la composición y aprobación de normas que se emplean para simplificar o eliminar actividades innecesarias dentro de un proceso, asegurando la calidad de un servicio o producto y la garantía de funcionamiento, dicho de otra manera, es el proceso de crear, poner en práctica y mejorar las reglas que se dan a las diferentes tareas para organizarlas y mejorarlas. Para supervisar y administrar de manera efectiva cada uno de los recursos organizacionales (humanos, tecnológicos y financieros), es esencial tener un registro u otra prueba de cada tarea completada a lo largo de la racionalización. (Mosquera, 2007).

La racionalización tiene tres características fundamentales que son:

- Disminuir los modelos, permaneciendo solo con los más necesarios.
- Facilita la intercambiabilidad a nivel internacional.
- Busca determinar errores de identificación elaborando un lenguaje claro y preciso.

### ***¿Cómo racionalizar procesos?***

Al racionalizar los procesos dentro de la organización, se puede lograr muchas cosas diferentes, que requieren menos trabajo y liberan tiempo. Posteriormente, se hablará de algunos pasos que servirán para racionalizar los procesos (Marcasco, 2021).

**Evaluar los procesos existentes:** En el momento que se evalúan los procesos, es más sencillo tener una idea apropiada de cómo se hacen las cosas, antes de poder percatarse qué áreas podrían optimizarse en gran medida mediante la racionalización. En concreto, puede ser conveniente hacer un registro de los procesos utilizando los términos más simplistas a fin de determinar cuáles son los beneficios de cada proceso y saber cuál es la persona encargada de cada actividad.

**Clasificar los procesos:** Al existir muchos procesos en la organización, se hace necesario listar cada uno de ellos, a fin de racionalizar los procesos del más al menos importante, ayudando así a reducir los flujos de trabajo que son necesarios para cumplir con todas las actividades que demanda el proceso.

**Analizar los resultados:** Al concluir los flujos de trabajo y las evaluaciones, es posible analizar los resultados de dichos flujos de trabajo y procesos, dando una mejor visión de que procesos no se ajustan al presupuesto y además son innecesarios, con el objetivo de poder tomar las mejores decisiones que ayuden a la organización.

**Pedir opiniones referentes a la racionalización de procesos:** Los analistas y operadores pueden tener valiosas opiniones con respecto a los procesos que ellos manejan, dando sus propios criterios sobre el funcionamiento y de cómo pueden mejorar estos procesos para ahorrar tiempo, completar las actividades y cumplir con los objetivos de forma eficiente.

**Automatizar los procesos:** Uno de los pasos fundamentales dentro de la racionalización es la automatización, el cual se enfoca en mejorar el progreso del flujo de trabajo, con la finalidad de reducir el costo, tiempo, desperdicio y mano de obra aumentando así la productividad y disminuyendo considerablemente los fallos (9001, 2016).

**Adecuar y optimizar los procesos:** Todo proceso con el pasar del tiempo necesita cambios continuos para que siga siendo útil, de lo contrario este quedaría obsoleto y no cumpliría con su objetivo, siendo necesario un cambio en los procesos en base a los resultados obtenidos.

### **Metodologías para racionalizar procesos**

Dentro de la racionalización de procesos existen varias metodologías que ayudan a las organizaciones a optimizar los procesos, mediante herramientas con las que cuentan cada

metodología, las cuales se implementan dependiendo de las necesidades de cada organización.

### ***Business Process Management (BPM)***

BPM es una metodología que busca mejorar los procesos mediante la gestión sistemática, la cual se orienta a mejorar la eficiencia y la eficacia de los procesos que se implementan dentro de la organización. Al ser un conjunto de principios, estos procesos deben ser modelados, automatizados, monitoreados, integrados y optimizados de forma continua, con el fin de poder medir los resultados obtenidos y así poder tomar las mejores decisiones que ayuden a la organización (Paz, 2017).

A continuación, se describen algunas de las principales ventajas de la adopción e implantación de la metodología:

- Optimización y control de procesos dentro de la organización, con alta pretensión de sistemas y personas.
- Creación y gestión de procesos dentro de la organización, en tiempo real.
- Dar seguimiento a los procesos en tiempo real, con el fin de poder realizar una buena auditoría, control y trazabilidad.

Dentro de BPM existen actividades de gestión de procesos, que se pueden agrupar en varias categorías como (diseño, análisis, monitorización, ejecución y optimización).

- **Análisis de Procesos:** Para comprender cómo (elegir tareas a completar, llevar a cabo dichas tareas, determinar quién completará las tareas y determinar dónde se completarán las tareas), se examinarán los procesos nuevos o actuales
- **Diseño de Procesos:** Para el diseño de procesos se toma en cuenta los procesos existentes y futuros, los cuales son representados mediante flujos de procesos, además estos tendrán



factores de alerta de notificaciones, acuerdos de nivel de servicio a fin de garantizar un diseño eficiente.

- **Ejecución de los procesos:** Consiste en la puesta en marcha de un proceso modelado, el cual tiene que estar promulgado por la organización de forma manual o automática.
- **Monitorización de procesos:** En la monitorización se realizará un seguimiento a cada uno de los procesos con los que cuenta la organización, de modo que se pueda tener información sobre la condición en la que se encuentra el proceso y así proporcionar estadísticas sobre el rendimiento de los procesos.
- **Optimización de procesos:** En la optimización se analizará el desempeño del proceso que se hizo en la fase de monitoreo, identificando los cuellos de botella que no permiten a la organización ahorro de costes y una mejor productividad. A fin de poder diseñar nuevos procesos sin estos inconvenientes.

### **Six Sigma**

Six Sigma orienta su metodología a eliminar la variabilidad, mejorando la calidad, tiempo de ciclo de cualquier proceso, coste, producción y servicio. Analizando los procesos repetitivos dentro de la organización, corrigiendo los problemas antes que se presenten es por eso que se distingue de otras metodologías ya que su objetivo es llevar la calidad a niveles sumamente cercanos a la excelencia (Sejzer, 2017).

Al aplicar Six Sigma se llevará a cabo por medio de cinco pasos, que conforman el ciclo DMAIC (definir, medir, analizar, mejorar y controlar), los cuales se describe a continuación:

- **Definir:** El propósito de este paso es identificar, definir y especificar el proyecto a realizar para que sea útil y accesible.

- **Medir:** El propósito de este paso es organizar y recopilar datos para caracterizar la entidad.
- **Analizar:** El objetivo de este paso es identificar el estado actual del proceso y los factores críticos dentro de él.
- **Mejorar:** La finalidad de este paso es determinar y establecer mejoras que se van a aplicar dentro del proceso, realizando pruebas rápidas.
- **Controlar:** El propósito de este paso es implementar mecanismos para asegurar que las mejoras se mantengan en el tiempo.

### ***Kaizen***

La metodología al implementarse ayuda a eliminar los desperdicios productivos dentro de la organización, persiguiendo siempre el cambio y la mejora continua, esto quiere decir que nunca se deja de ejecutar, es decir, no hay día que no se note alguna mejora. Por tanto, cuando se la ejecuta dentro de la organización se debe administrar y desarrollar los procesos haciendo énfasis en las necesidades del cliente, dando como resultado una eliminación completa de desperdicios y la optimización de recursos (Antonucci, 2021).

A continuación, se describen los elementos que conforman la metodología descrita:

- **Planear:** Partiendo del objetivo de la organización, debemos saber con exactitud cuál es la situación actual (problema) para poder plantear un plan de acción.
- **Hacer:** Para este paso, se recomienda establecer acciones que se realizarán en nuestro plan, siempre y cuando se tenga claro el punto de la planificación, con el fin de ponerlas en marcha.
- **Comprobar:** En este paso se plantean algunas interrogantes como (qué objetivos se cumplen y cuáles no, cómo se calcula el avance de las estrategias), analizando los

resultados conseguidos y compararlos con los datos que se tenían antes de que fueran puestos en marcha. A fin de comprobar si los resultados obtenidos fueron los que se plantearon en el objetivo, para así poder avanzar de lo contrario se debe volver a empezar.

- **Actuar:** En este paso verificamos que las acciones que nos planteamos, cumplan con el objetivo propuesto, con el propósito de estandarizarlas y así utilizarlas en los procesos. Teniendo en cuenta que estas acciones siempre se las podrá mejorar.

## **Fundamentación Científica de la Variable Dependiente**

### ***Seguridad informática***

La seguridad informática es un proceso que busca prevenir y detectar el uso no autorizado a los sistemas informáticos mediante la confidencialidad, integridad, disponibilidad y autenticación. Esto implica que la organización pueda proteger todos sus activos informáticos, de intrusos que buscan intenciones maliciosas a fin de obtener ganancias, para ello se implementan medidas de seguridad como antivirus, firewalls, encriptación, inteligencia artificial, plan de seguridad informática y pentesting, etc. (Rocha, 2011)

### ***CERT (Computer Emergency Response Team)***

Es un equipo de personas dedicadas a implantar medidas preventivas, proactivas, reactivas y de gestión de la seguridad con el fin de mitigar y responder rápidamente a los incidentes que se suscitan sobre los sistemas informáticos. El objetivo de implementar un CERT en las organizaciones es disminuir el daño en los sistemas y así garantizar la continuidad de los servicios que soportan (Moyle, 2019).

### **Normativa relativa a los CERT**

Dada la importancia que ha tenido la seguridad informática en los últimos años, debido principalmente a los siniestros que se han reportado a nivel internacional, se han creado

normativas que proveen marcos de trabajo cuyo objetivo consiste en mejorar los servicios, productos, procesos y personal de trabajo, definiendo especificaciones técnicas mínimas que la organización debe cumplir y poder trabajar con normalidad. A continuación, se presentan las normativas de mayor relevancia y aceptación por parte de los CERT a nivel mundial.

### ***Revisión de la guía norteamericana para el manejo de incidentes informáticos***

#### ***NIST.SP.800-61r2***

La guía NIST.SP.800-61r2, fue elaborado por la NIST (National Institute of Standards and Technology), el cual acatando la ley pública FISMA (Federal Information Security Management Act), Es una guía de contratación para agencias federales en los Estados Unidos de América, sin embargo, puede ser utilizada voluntariamente y no está sujeta a derechos de autor por parte de organizaciones no gubernamentales. Esta guía ayuda a las organizaciones a reducir los riesgos de los incidentes de seguridad de la información al brindar pautas prácticas para responder de manera rápida y eficaz a los incidentes. Incluyendo pautas en la creación de un programa de respuesta a incidentes eficaz, pero la perspectiva principal de la guía es descubrir, analizar, priorizar y manejar incidentes, los modelos se pueden mantener independientemente de los sistemas operativos, plataformas de hardware y aplicaciones (Cichonski, Millar, Grance, & Scarfone, 2012).

La guía se divide en 4 secciones y 8 apéndices. En la Sección 2, se plantea la necesidad de responder a los incidentes y se describen las posibles opciones de estructura del CERT. El mecanismo fundamental de gestión de incidentes se describe en la Sección 3 junto con las recomendaciones para llevarlo a cabo con éxito. La cuarta sección analiza cómo se organizan los incidentes y cómo se distribuye la información. Los apéndices contienen información detallada sobre varios temas. El Apéndice A abarca ambientes de respuesta a incidentes y preguntas para utilizar en la mesa de respuesta a incidentes. El Apéndice B provee

catálogos de campos de datos propuestos para recopilar para cada incidente. Los Apéndices C y D abarcan un glosario y un catálogo de acrónimos, respectivamente. El Apéndice E determina los recursos que pueden ser útiles en la preparación y ejecución de la respuesta a incidentes. El Apéndice F aborda las preguntas más comunes sobre la respuesta a incidentes. El Apéndice G lista los pasos fundamentales a cumplir cuando se utiliza una crisis relacionada con un incidente de seguridad informática. El Apéndice H abarca una lista de cambios significativos desde el análisis anterior.

### ***INCIBE (Instituto Nacional de Ciberseguridad de España)***

La guía INCIBE (National Institute of Cybersecurity) que en español significa Instituto Nacional de Ciberseguridad, Contribuir al crecimiento de la ciberseguridad y disfrutar de un alto nivel de confianza online que, entre otras cosas, fomenta una cultura de seguridad y protección entre los ciudadanos. La red académica y de investigación española RedIRIS proporciona acceso a Internet, en particular para industrias estratégicas. Contribuir al crecimiento de la ciberseguridad y disfrutar de un alto nivel de confianza online que, entre otras cosas, fomenta una cultura de seguridad y protección entre los ciudadanos. La red académica y de investigación española RedIRIS proporciona acceso a Internet, en particular para industrias estratégicas. Como resultado, el objetivo de estas directrices y estudios es aportar valor tanto práctico como teórico para promover y mejorar la seguridad digital para las organizaciones en todos los contextos sociales. Estas guías se encuentran en la página oficial de INCIBE en el apartado sección de guías (INCIBE-CERT, 2018).

Dentro de la Sociedad de la Información INCIBE juega un papel muy importante, ya que su objetivo consiste en fortalecer el entorno dentro de la ciberseguridad, protección de la información y el acceso a ella, priorizando siempre a los clientes dándoles valor a las organizaciones, redes académicas, recursos de TI y la investigación española que ellos

manejan. Por tanto, INCIBE muestra esta guía como un instrumento para impulsar la ciberseguridad como motor de transición social y oportunidad de perfeccionamiento, para esto siguen algunos lineamientos basados en la investigación española, prestación de servicios y disposición por parte de personas expertas en la materia, es por esto que INCIBE lidera varias presentaciones en cuanto a ciberseguridad a nivel nacional e internacional. Del mismo modo mientras más pasa el tiempo esta guía logra distinción como un CERT de referencia por parte de NIS que significa Seguridad de la Red y la Información, la cual pasa a nombrarse exactamente el 01/10/2018 como INCIBE-CERT y va dirigido a personas y organizaciones en derecho privado en España.

Esta terminología, enlazada a un nuevo cambio de figura, contesta al propósito de optimizar a los servicios que operan con el organismo INCIBE, y este a su vez necesita del Ministerio de Economía y Empresa para ir de la mano con la Secretaría de Estado para el Avance Digital, no por nada INCIBE-CERT en la actualidad es uno de los servicios más decisivos e importantes que el instituto brinda al pública a los que comanda. Es por esto que en su trabajo dentro de un CERT nacional, INCIBE-CERT emplea procedimientos de prevención y detección temprana de incidentes, de forma proactiva, que afectan a clientes y organizaciones en todo el mundo. Además, INCIBE cuenta con otra guía nombrada Directrices nacionales españolas para la notificación y gestión de incidentes cibernéticos la cual provee modelos sobre informes de incidentes en ciberseguridad, ayuda a la notificación y gestión de los mismos (INCIBE, 2020).

### ***Revisión de la guía para la elaboración de una estrategia nacional de ciberseguridad mediante ITU (The International Telecommunication Union)***

La guía ITU (The International Telecommunication Unión) fue fundada en 1865 con la finalidad de agilizar la conectividad internacional de las redes de comunicación coadyuvando en

el entorno mundial con las órbitas de satélite y el espectro de frecuencias radioeléctricas, mediante normas técnicas que aseguran la interconexión equilibrada de redes y tecnologías, mejorando el acceso a las TIC con el fin de atender a las comunidades que no dispongan de una buena conexión alrededor del mundo, además la ITU cuenta con una guía llamada “Guía nacional de estrategia de ciberseguridad” que fue realizada por socios de esta entidad la cual ofrece seguridad en cuanto a la ciberdelincuencia mediante estrategias que fueron las que mejor resultado dieron al ser implementadas.

Esta guía parte de la situación actual de las organizaciones o países, tomando en cuenta sus culturas y valores, para ayudar a todos los estados que tienen relación con esta guía, maximizando el uso de las TI y aumentando el desarrollo económico y social. Específicamente esta guía la desarrollaron 12 socios de los sectores público y privado, con la ayuda del público civil y personas expertas en la materia (UIT, 2018).

A continuación, se realiza un resumen de la estructura general de la guía, resumiendo cada una de sus secciones.

- **Sección 1:** Descripción general del documento: En este capítulo se describe la finalidad de esta guía, así como también sus ámbitos de aplicación.
- **Sección 2:** Introducción: En este capítulo se describen los beneficios de la implementación de las TI dentro y fuera de las organizaciones.
- **Sección 3:** Ciclo de elaboración de la estrategia: En este capítulo se describen las etapas de elaboración, estrategias y su gestión durante todo su ciclo de vida.
- **Sección 4:** Principios generales: En este capítulo se describen nueve principios que al unirlos todos, pueden crear una nueva estrategia basada en ciberseguridad.

- **Sección 5:** Buenas prácticas en la estrategia general de ciberseguridad: En este capítulo se describe un modelo de gestión para identificar los temas y aspectos fundamentales relacionados a la ciberseguridad.
- **Sección 6:** Materiales de referencia de apoyo: En este capítulo se describen fuentes relevantes que las partes interesadas pueden analizar durante el proceso de elaboración de la guía.
- **Sección 7:** Acrónimos: Palabras clave que se utilizan en ciberseguridad.

A manera de resumen se puede acotar lo siguiente; en la sección 3 se habla del proceso y sus características en la elaboración de una táctica nacional de ciberseguridad, en el ciclo de elaboración de estrategias, mientras que las secciones 4 y 5 se focalizan en el plan nacional de ciberseguridad, poniendo como prioridad ciertos conceptos que necesariamente deben ir en el documento, además en el capítulo 6 se habla de guías similares que sirven de apoyo en la implementación de ciberseguridad para las organizaciones. El objetivo de esta guía es proveer un marco adecuado que sea fácil de implementar en cualquier parte del mundo, partiendo de la situación actual y respetando los valores culturales y sociales para crear sociedades seguras basadas en las TIC (UIT, 2018).

## **Estructura de un CERT**

### **Servicios ofertados por los CERTs**

Según la (Organización de los Estados Americanos, 2016) en su explicación de Buenas Prácticas para Establecer un CSIRT nacional, indica que los servicios de un CSIRT se pueden diferenciar en tres grupos: reactivos, proactivos y de valor agregado, de tal manera que estos mismos servicios se pueden utilizar dentro de un CERT, dependiendo de los recursos con los que cuenta cada organización, los cuales se describen a continuación:



- **Servicios reactivos:** Los servicios más importantes dentro de un CSIRT para una organización son los servicios reactivos, ya que se encargan de responder activamente los incidentes, eventos o requerimientos de seguridad que se presentan en ese momento, es decir en tiempo real.
- **Servicios Proactivos:** Estos servicios tratan de prevención de incidentes, ya que intenta cuidar a la institución, organización, empresa y su infraestructura de TI, con información e investigación que ayude a evitar los ataques presentes y futuros.
- **Servicios de valor agregado:** Este servicio se basa en el mejoramiento de la calidad que se brinda como CERT académico, coadyuvando a la mejora continua de la organización.

A continuación, se muestran los sub servicios de cada uno de los literales mencionados anteriormente en la figura 10.

## Figura 10

### Servicios de un CERT

<u>Servicios reactivos</u>	<u>Servicios proactivos</u>	<u>Manejo de instancias</u>
<ul style="list-style-type: none"> <li>• <u>Alertas y advertencias</u></li> <li>• <u>Tratamiento de incidentes</u></li> <li>• <u>Análisis de incidentes</u></li> <li>• <u>Apoyo a la respuesta a incidentes</u></li> <li>• <u>Coordinación de la respuesta a incidentes</u></li> <li>• <u>Respuesta a incidentes in situ</u></li> <li>• <u>Tratamiento de la vulnerabilidad</u></li> <li>• <u>Análisis de la vulnerabilidad</u></li> <li>• <u>Respuesta a la vulnerabilidad</u></li> <li>• <u>Coordinación de la respuesta a la vulnerabilidad</u></li> </ul>	<ul style="list-style-type: none"> <li>• <u>Comunicados</u></li> <li>• <u>Observatorio de tecnología</u></li> <li>• <u>Evaluaciones o auditorías de la seguridad</u></li> <li>• <u>Configuración y mantenimiento de la seguridad</u></li> <li>• <u>Desarrollo de herramientas de seguridad</u></li> <li>• <u>Servicios de detección de intrusos</u></li> <li>• <u>Difusión de información relacionada con la seguridad</u></li> </ul>	<ul style="list-style-type: none"> <li>• <u>Análisis de instancias</u></li> <li>• <u>Respuesta a las instancias</u></li> <li>• <u>Coordinación de la respuesta a las instancias</u></li> </ul>
		<u>Gestión de la calidad de la seguridad</u>
		<ul style="list-style-type: none"> <li>• <u>Análisis de riesgos</u></li> <li>• <u>Continuidad del negocio y recuperación tras un desastre</u></li> <li>• <u>Consultoría de seguridad</u></li> <li>• <u>Sensibilización</u></li> <li>• <u>Educación / Formación</u></li> <li>• <u>Evaluación o certificación de productos</u></li> </ul>

Nota: Tomado de *Cómo crear un CSIRT paso a paso* por Enisa.

## **Capítulo III**

### **Desarrollo de la Investigación**

#### **Introducción**

El presente capítulo tiene como finalidad la revisión y verificación de una metodología ecléctica que permita llevar a cabo la racionalización de procesos en las organizaciones, para ello inicialmente se efectuó un análisis comparativo de los elementos que conforman las diferentes metodologías de mejora de procesos desarrolladas en el capítulo II, de los cuales, por medio de un análisis comparativo se seleccionaron únicamente aquellos elementos con mayor ponderación. Como resultado se obtuvo una metodología fundamentada en la mejora de los procesos internos de las organizaciones partiendo desde su análisis de entorno hasta la elaboración de la norma de procedimientos apoyados en estándares y normativas de calidad internacionales.

#### **Análisis comparativo de las metodologías para racionalizar procesos**

Los elementos que conforman las diferentes metodologías de mejora de procesos, se los detallan en la tabla número 5, en donde se partió por determinar cada uno de estos y con base en ello realizar un análisis comparativo describiendo su grado de importancia por medio de las siguientes métricas: Alto (A), Medio(M), Bajo(B) y No Aplica (N/A).

**Tabla 5***Análisis comparativo de elementos para racionalizar procesos*

<b>Elementos</b>	<b>BPM</b>	<b>Six Sigma</b>	<b>Kaizen</b>
Levantamiento de procesos	B	A	M
Análisis del entorno	A	A	A
Definición de recursos	B	B	B
Análisis de secuencia de procesos	M	M	N/A
Ciclo de mejora continua	B	N/A	M
Mapa de procesos	A	M	M
Normalización y documentación de procesos	M	B	B
Definición del proceso y validación	A	A	M
Norma de procedimiento	A	M	M

*Nota: Tabla que indica los elementos que conforman las metodologías mayormente implementadas para mejora de procesos.*

## Definición de la metodología ecléctica

Tras el análisis realizado se obtiene una serie de pasos ordenados que guiarán el desarrollo metodológico de la racionalización de procesos en base a cada uno de los servicios ofertados por el ESPE-CERT, dichos pasos se muestran en la figura 12.

**Figura 11**

*Metodología ecléctica para racionalizar procesos*



*Nota: La imagen muestra de manera secuencial cada uno de los elementos que se considerarán para la racionalización de procesos.*

## Desarrollo metodológico de la racionalización de procesos

A continuación, se abordan cada una de las fases que conforman la metodología ecléctica para racionalizar procesos:

### **Análisis del Entorno**

El objetivo del presente análisis es recabar toda la información necesaria sobre el entorno y flujo de trabajo del ESPE-CERT, que servirá como guía para representar el mapa de procesos que se establece como punto número 2 en la metodología propuesta.

### **ESPE-CERT:**

Para servir a toda la comunidad universitaria, el Equipo de Respuesta a Emergencias Informáticas de la Universidad de las Fuerzas Armadas orienta y desarrolla sus sistemas y servicios con base en los siguientes principios:

- a) El ESPE-CERT se debe a la Universidad Ecuatoriana y se crea para propiciar la investigación, formación profesional y desarrollo tecnológico, en cumplimiento de sus obligaciones constitucionales.
- b) El desarrollo de sus actividades y servicios se realizan para satisfacer con calidad y excelencia los requerimientos de su comunidad objetivo.
- c) La actividad y enfoque técnico-académico del ESPE-CERT se encuentra orientado al dominio principal de la Universidad de las Fuerzas Armadas ESPE, referido a la Seguridad y Defensa.
- d) La Organización es una Institución generadora de conocimiento, en donde la flexibilidad y el cambio planificado sirven tanto como hábito como base para producir alternativas creativas. en el contexto de la ciberseguridad y ciberdefensa.

### **Misión:**

Equipo de Respuesta ante Emergencias Informáticas centralizado en la generación de alternativas I+D+I, formación y entrenamiento especializado en ciberseguridad, ética científica,

calidad humana y conciencia social de protección cibernética al servicio de la ESPE y la sociedad ecuatoriana, con base a tecnología de punta y personal altamente calificado.

**Visión:**

El ESPE-CERT, pretende alcanzar un reconocimiento internacional como un CERT de carácter académico, orientado a la ciberseguridad y ciberdefensa, para satisfacer los requerimientos de la comunidad con calidad y excelencia.

**Valores institucionales:**

Los valores institucionales que rigen el comportamiento y proceder de los miembros que conforman el ESPE-CERT son: ética científica, honestidad, integridad, respeto, trabajo en equipo y lealtad. En definitiva, promover los valores eleva los niveles de compromiso y motivación de los equipos de trabajo. No obstante, es necesario que también se vean reflejados en la interacción con los clientes, aliados y grupos con los que se relaciona la institución.

**Estrategia general:**

Su estrategia va enfocada en el continuo mejoramiento de sus servicios que permita el establecimiento de una organización flexible, dinámica y proactiva, utilizando diferentes métodos como la mejora continua por los procedimientos, el trabajo en equipo, el desarrollo de la capacidad humana y la constante innovación tecnológica.

**Fases estratégicas:**

Con la finalidad de alcanzar la visión propuesta por la organización, su esfuerzo estratégico se subdivide en tres fases consecutivas: Fortalecimiento, Consolidación e Innovación.

### **Fase I.- Fortalecimiento**

La fase uno de fortalecimiento coadyuva en la parte educativa para el incremento de ofertas académicas de grado y postgrado en el ámbito de la seguridad de la información y la ciberseguridad, además comprende el desarrollo de proyectos I+D+i con los estudiantes de la universidad para integrar los servicios del ESPE CERT, así como también el desarrollo del manual de procesos específicos, la elaboración del código de ética profesional, la capacitación, formación y especialización del personal en temas de ciberseguridad, y finalmente una evaluación continua de la realización de proyectos y planificaciones por parte de una comisión evaluadora.

### **Fase II.- Consolidación**

En la fase dos de consolidación se establecen cada de uno de los objetivos organizacionales, donde se destaca el fortalecimiento de las áreas académicas en ámbitos de ciberseguridad y ciberdefensa, así como también promover y ayudar en la implantación del Sistema de Gestión de Seguridad de la Información (SGSI) de la ESPE, además gestionar alianzas estratégicas entre el ESPE-CERT y el Comando de Ciberdefensa (COCIBER) a fin de incrementar las posibilidades de I+D+i.

### **Fase III.- Innovación**

Para la fase tres de innovación se plantea la creación de un centro de investigación dedicado a la ciberseguridad y ciberdefensa, utilizando servicios open source que permitan la gestión de incidentes de seguridad informática, promoviendo así la participación en redes de investigadores para incrementar el número de proyectos de investigación con el fin de trascender local e internacionalmente colaborando con otras instituciones.

## **Estructura Organizacional Por Procesos**

### **Modelo Organizacional**

La estructura organizacional del ESPE-CERT y sus recursos se ubican en un sitio central que facilita la recopilación de una gran variedad de información para su respectivo tratamiento, ya que la Universidad al contar con algunas extensiones deberá trabajar con expertos de sistemas y plataformas de la Unidad de Tecnologías de la Información y las Comunicaciones (UTIC) en sus múltiples sedes, que darán respuesta para actuar con eficacia en la prestación del servicio. Adicionalmente, la ESPE-CERT es responsable de gestionar reportes, analizar incidentes e identificar vulnerabilidades con autoridad para publicar alertas, mejores prácticas, pasos de respuesta y recuperación de seguridad.

### **Servicios del ESPE-CERT**

Para establecer los servicios que brinda el ESPE-CERT de acuerdo con el trabajo de titulación "Fue necesario establecer una base de datos con información de los académicos CSIRTs/CERTs que operan en la región para implementar y poner en marcha un equipo basado en ITIL para responder a incidentes de seguridad de la información en el Departamento de Ciencias de la Computación de la Universidad de las Armadas. Fuerzas de la Unión Europea. En concreto, se realizó un análisis a nivel de los CSIRT de Latinoamérica, las propuestas de la ENISA, de la Organización de los Estados Americanos (OEA) y FIRST, con ello los servicios propuestos para la etapa inicial de ESPE-CERT contemplan la gestión de incidentes, la gestión de vulnerabilidades, el monitoreo del sistema, la publicación de alertas y propuestas de soluciones de I+D+i.



## Organización por procesos

De acuerdo con la Propuesta Estratégica del ESPE-CERT, para el cumplimiento de la misión y objetivos, la institución tiene previsto desarrollar su gestión a través de procesos internos, los cuales se los detallan en la figura 12.

### Figura 12

*Modelo organizacional por procesos*



*Nota: La imagen representa el modelo organizacional propuesto en el Plan Estratégico para el ESPE-CERT 2021.*

Es importante mencionar que la institución, pese a que en su plan estratégico recalca el trabajo y la organización por procesos, es algo que hasta en su momento no se había implementado, por lo cual no posee un mapa general, ni un documento guía en donde se especifiquen las actividades que apoyan a los diferentes servicios que oferta el ESPE-CERT. Sus esfuerzos únicamente se centran en el procedimiento de gestión de incidentes que apoya al servicio reactivo correspondiente y es usado como punto base para atender todas las peticiones de los clientes.

### **Mapa de Procesos**

Para llevar a cabo el mapa de procesos del ESPE-CERT, fue necesaria la participación directa de todos sus miembros activos que contribuyeron con su conocimiento y experiencia, facilitando la recolección de la información y completando el análisis de entorno realizado en el punto número 1, de lo cual se establece lo siguiente:

- Se elaborará el mapa detallado de los procesos y procedimientos operativos del CERT, en base a los servicios definidos en el trabajo de titulación del Ing. Jonathan Benavidez, con la participación de los miembros del proyecto de investigación.
- Los procesos dentro del ESPE-CERT no deberán ser independientes ya que todos persiguen el mismo fin, que es el progreso y la prosperidad del observatorio. Aunque cada uno funcione en un ámbito de acción específico todos los procesos se vinculan con otros para que, en conjunto, se alcance un objetivo común.
- Los procesos y procedimientos identificados van acorde a los servicios reactivos y proactivos que son ofertados por los CERTs.
- El mapa de procesos propuesto representará de manera gráfica cómo se interrelacionan todos los procesos que se desarrollarán dentro del observatorio. Funciona como un diagrama de valor en el que se pone de manifiesto la importancia de cada uno de ellos dentro de la visión global de funcionamiento de la institución.

Previo a definir la estructura, fue necesario clasificar los procesos. Por lo general, se utilizan tres categorías:

### **Procesos Gobernantes**

Los procesos gobernantes proveen políticas, directrices y planes estratégicos para el correcto funcionamiento del observatorio. Estos procesos son gestionados por el directorio y/o

las altas autoridades de la institución, para lograr de esta manera el cumplimiento de los objetivos y políticas institucionales planteadas.

### **Procesos Generadores de Valor**

Estos procesos se refieren a toda actividad que genere valor agregado a los clientes y a la institución. También son definidos como operativos y formarán parte de la raíz de los servicios del ESPE-CERT, Es el comienzo de una serie de actividades interconectadas que eventualmente producirán un resultado. Todos estos procesos utilizan recursos, y de esos recursos provienen los bienes y servicios que se dirigen a los clientes para satisfacer sus necesidades.

Los Procesos y Procedimientos Generadores de Valor que serán desarrollados en el manual de acuerdo a su nivel crítico se los representan de manera gráfica en la Figura 13:

**Figura 13**

*Procesos y Procedimientos generadores de valor*



*Nota: La imagen representa los procesos y procedimientos operativos que serán desarrollados en el manual de procesos*

### **Procesos de apoyo**

Son aquellos procesos que se encargan de gestionar los diferentes departamentos y actividades que realizan, manteniendo un control sobre los objetivos y las misiones de cada actividad planteada.

### **Norma de Procedimiento**

Para la identificación y desarrollo de los procesos y procedimientos del ESPE-CERT, fue necesario caracterizarlos mediante códigos de procesos y procedimientos, donde procesos se refiere a las funciones generales del ESPE-CERT y procedimientos son las actividades a realizar por cada proceso.

A continuación, se representan los procesos y procedimientos según sus respectivos códigos.

**Tabla 6**

*CERT- 01 Procesos Gobernantes*

<b>Cod.</b>	<b>Procesos</b>	<b>Cod.</b>	<b>Procedimientos</b>
CERT-01.01	Gobierno Estratégico y control	CERT-01.01.01	Dirección Estratégica.
		CERT-01.01.02	Evaluación.
CERT-01.02	Administración y Gestión	CERT-01.02.01	Planificación Estratégica.
		CERT-01.02.02	Planificación Operativa.

<b>Cod.</b>	<b>Procesos</b>	<b>Cod.</b>	<b>Procedimientos</b>
		CERT-01.02.03	Elaboración y actualización de procesos y procedimientos.
		CERT-01.02.04	Ejecución y control de operaciones.
		CERT-01.02.05	Evaluación de desempeño.

*Nota: En la tabla se muestran los Procesos Gobernantes con sus respectivos procedimientos caracterizados por sus códigos.*

### **Tabla 7**

*CERT- 02 Procesos Generadores de valor*

<b>Cod.</b>	<b>Procesos</b>	<b>Cod.</b>	<b>Procedimientos</b>
CERT-02.01	Gestión de las operaciones y servicios del CERT.	CERT-02.01.01	Mesa de Servicios.
		CERT-02.01.02	Gestión de Incidentes.
		CERT-02.01.03	Análisis de vulnerabilidades.
		CERT-02.01.04	Monitoreo y alerta de primer nivel.

<b>Cod.</b>	<b>Procesos</b>	<b>Cod.</b>	<b>Procedimientos</b>
		CERT-02.01.05	Investigación Forense.
		CERT-02.01.06	Evaluación Técnica de Seguridad de la Información.
		CERT-02.01.07	Asesoramiento técnico y consultoría.
		CERT-02.01.08	Entrenamiento en el ámbito de la ciberseguridad y ciberdefensa.
CERT-02.02	Gestión de I+D+I	CERT-02.02.01	Investigación, Desarrollo e implementación (I+D+i) de artefactos.
		CERT-02.02.02	Análisis de sensibilización y elaboración de materiales.

*Nota: En la tabla se muestran los Procesos Generadores de Valor con sus respectivos procedimientos caracterizados por sus códigos.*

**Tabla 8***CERT- 03. Procesos de apoyo*

<b>Cod.</b>	<b>Procesos</b>	<b>Cod.</b>	<b>Procedimientos</b>
CERT- 03.01	Gestión administrativa.	CERT-03.01.01	Gestión de Talento Humano
		CERT-03.01.02	Gestión Financiera
CERT- 03.02	Gestión de tecnologías.	CERT-03.02.01	Gestión de inventario
		CERT-03.02.02	Instalación y configuración
		CERT- 03.02.03	Soporte y mantenimiento

*Nota: En la tabla se muestran los Procesos de Apoyo con sus respectivos procedimientos caracterizados por sus códigos.*

**Ficha de procesos y procedimientos:**

El formato establecido para la elaboración de la norma de procedimientos se apoyará en la guía técnica NTE-ISO-IEC-9001: 2015 Sistemas de Gestión de la Calidad y se la describe a continuación:

**Figura 14**

*Cabecera de la ficha de procesos y procedimientos*

CERT- "CÓDIGO". "NOMBRE DEL PROCESO O PRECEDIMIENTO"

Nro. de Proceso:	Nro. Hoja:
Elaboró:	NTE INEN- ISO 9001
Título:	

*Nota: La imagen representa la cabecera de la ficha, en donde se especifica la información concerniente al procedimiento.*

**Figura 15**

*Control de versionamiento y datos informativos de los procesos y procedimientos*

Nro. de cambio al proceso	Elaboró	Revisó	Aprobó	Nro. de Páginas
	Cargo: Nombre:	Cargo: Nombre:	Cargo: Nombre:	
	Firma:	Firma:	Firma:	
	Fecha:	Fecha:	Fecha:	
<b>CONTROL DE COPIAS DEL PROCESO</b>				
<b>DEPARTAMENTO</b>		<b>FIRMA DE RECIBIDO</b>		<b>FECHA</b>
<b>Nro. DE CAMBIO AL PROCESO</b>	<b>DESCRIPCION DEL CAMBIO</b>			

*Nota: La imagen representa el control de versionamiento, creador, revisor, y aprobador, de cada uno de los procesos y procedimientos operativos.*



**Contenido de la Ficha:**

- **OBJETIVO:** Se establece el/los objetivos del procedimiento a desarrollar.
- **ALCANCE:** Se describe de forma clara la finalidad de los objetivos que se intentarán alcanzar.
- **RESPONSABLES:** Se identifican los encargados de la consecución de las actividades de los procedimientos.
- **BASE LEGAL:** Documentos oficiales que sustentan de forma legal el desarrollo de cada procedimiento.
- **POLÍTICAS:** Se establecen las normativas básicas que presiden el proceder de la institución frente a cada uno de los procedimientos desarrollados.
- **DEFINICIÓN:** Se describen los términos de mayor relevancia dentro de cada procedimiento.
- **DESARROLLO:** Se describen de inicio a fin cada una de las actividades de los procedimientos. Todas estas actividades resultaron del análisis e investigación de estándares y normativas a nivel internacional.
- **INDICADORES DE DESEMPEÑO:** Se establecen las métricas que evalúan el rendimiento y desempeño de cada procedimiento.
- **DIAGRAMAS:** Representación gráfica de todo el flujo del procedimiento, desde sus entradas, actores, tiempos, actividades y salidas.

***Evaluación y Validación del proceso*****Antecedentes**

Desde la creación del ESPE-CERT la organización ha venido trabajando de una u otra forma sin un manual de procesos operativos, lo cual se ha visto reflejado en la calidad del servicio

que prestan, por esta razón se presenta un manual de procesos operativos que es parte de la tesis llamada “Desarrollo del manual de procesos operativos para el CERT académico de la ESPE utilizando estándares internacionales” en el cual se describen todos los procesos, procedimientos, diagramas de flujo, bases legales, políticas, responsables y métricas que coadyuvan en la operatividad de los servicios que oferta el ESPE-CERT.

Sin embargo, con el rápido crecimiento de Internet y las redes de datos, también han aumentado las actividades maliciosas, que tienen un impacto negativo en las organizaciones, afectando directamente al activo más valiosos que es la información, partiendo de esto, se toma como punto de partida la creación de servicios proactivos y reactivos que ayuden a reducir el impacto de estas actividades maliciosas. Por esta razón se pone énfasis en la norma de procedimiento ya que esta abarca los puntos más importantes como el proceso, procedimiento y diagrama de flujo los cuales ayudarán a evaluar cada uno de los procedimientos.

**Descripción:**

Con los procesos y procedimientos establecidos, se procedió con la socialización a los miembros activos que conforman el ESPE-CERT liderado por el Ing. Jonathan Benavides ayudante de Investigación. En la socialización se explicó de manera detallada la norma de procedimientos en donde constan cada uno de los procesos, procedimientos y sus diagramas de flujo que corresponden a cada uno de los servicios establecidos por el CERT.

Para la validación del proceso se elaboró una rúbrica de evaluación en la que se establecen los parámetros más importantes que serán evaluados, así como también, las métricas que serán utilizadas.

El objetivo de la evaluación es comprobar un nivel mínimo de desempeño para validar los procesos y procedimientos identificados, a fin de conseguir el cumplimiento del ciclo PHVA de mejora de la calidad, para que finalmente sean aprobados y colocados en operación.

### **Rúbrica de evaluación de procesos:**

#### **Selección de parámetros de evaluación**

Los parámetros de evaluación son obtenidos de los objetivos de las normas de procedimiento, de manera particular, para luego generalizarlos y aplicarlos a todos los procesos.

Los parámetros seleccionados son los que se detallan a continuación:

**Cumplimiento del objetivo del procedimiento (eficacia).** - Se refiere al porcentaje de cumplimiento del objetivo del proceso en forma efectiva y se mide en base de los componentes del objetivo, es necesario tener una evidencia concreta del resultado conseguido con el proceso.

**Eficiencia en el proceso.** - Mejor uso de recursos (Tiempo-Costo), se refiere al uso adecuado y completo de todos los recursos del proceso, sean estos humanos, materiales, equipos, insumos y otros, su uso adecuado redundará en el costo del proceso y el tiempo en el que se consigue cumplir el objetivo.

**Sintaxis, redacción y semántica del contenido.** - Se refiere a la forma en la que se expresan las ideas, de tal manera que sean de fácil comprensión para el lector, con un significado correcto y sin ambigüedades, es muy importante para que el proceso cumpla con su objetivo de dirección.

**Asignación de roles y responsabilidades.** - Debe haber una correspondencia adecuada entre las responsabilidades que se asignan y los roles establecidos en la organización, la idea es medir esa correspondencia para que el proceso se cumpla en concordancia con las capacidades de los recursos humanos establecidas en la organización.

**Uso de normas internacionales de referencia.** – Uso extensivo de normas de referencia, considerando su tipo y pertinencia.

**Secuencia lógica de actividades.** – Correspondencia que tienen las actividades en cada uno de los procesos, teniendo en cuenta tres aspectos fundamentales que son: situación inicial, situación de cambio, situación final, considerando que cada actividad debe tener relación con su predecesor y su sucesor.

### **Rango de medición**

El rango se establece entre el nivel superior y el nivel inferior de medición posible, en este caso se determina el rango entre 1 y 5, de tal manera de no hacer muy extensiva la apreciación que de alguna manera tendrá un grado de subjetividad. El rango será concurrente con el número de categorías que se definirán posteriormente.

Así mismo la estandarización de los parámetros (nivel mínimo aceptable) se establece en base del período de iniciación de operaciones, para en el futuro lograr su mejora continua y alcanzar un nivel mayor de madurez.

### **Priorización de Parámetros:**

Para tener jerarquía dentro de los parámetros de evaluación fue necesario crear la matriz de alternativas o también llamada matriz de Holmes, la cual sirve como herramienta de

priorización, evaluando diferentes alternativas y coadyuvando en la toma de las mejores decisiones.

A continuación, en la tabla 9 se describe cada uno de los parámetros establecidos para la matriz de HOLMES.

- [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.

**Tabla 9**

*Matriz de Priorización de Parámetros de Evaluación*

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

*Nota: En la tabla se observa la matriz de priorización de parámetros, que contribuye en el apoyo de toma de decisiones.*

**Categorías. -**

Se consideran cinco categorías que serán descritas en la rúbrica de evaluación, desde no aceptable hasta completamente aceptable, pasando por las categorías: Aceptable con correcciones mayores, aceptable con correcciones menores, aceptable.

A continuación, en la tabla 10 se detalla los criterios de cada categoría, que se tomarán en cuenta para ponderar cada uno de los parámetros seleccionados.

Tabla 10

*Rúbrica de evaluación de procesos*

<b>Parámetros</b>	<b>Coefficiente de importancia</b>	<b>Completamente aceptable</b>	<b>Aceptable</b>	<b>Aceptable con correcciones menores</b>	<b>Aceptable con correcciones mayores</b>	<b>No aceptable</b>
<b>Cumplimiento del objetivo del proceso</b>	0,33	Se cumplen con todos los objetivos de manera efectiva.	Se cumplen con la mayoría de los objetivos de manera efectiva.	Se cumplen con algunos de los objetivos de manera efectiva.	El cumplimiento de objetivos es mínimo y se realizan de manera poco efectiva.	No se cumplen con los objetivos.
<b>Eficiencia en el proceso</b>	0,27	Se aprovecha completamente los recursos del proceso, contribuyendo en la productividad y mejorando el tiempo de ejecución de sus actividades.	Se aprovecha adecuadamente los recursos del proceso, aumentando la productividad y mejorando el tiempo de ejecución de sus actividades.	Se aprovecha de los recursos del proceso, mejorando el cumplimiento de sus actividades, pero no el tiempo de su ejecución.	Existe una contribución mínima en cuanto a la optimización de los recursos de los procesos, no se aumenta la productividad y tampoco se mejora el tiempo de cumplimiento de las actividades.	No contribuye en la optimización de recursos, además, no aumenta la productividad y tampoco mejora el cumplimiento de sus actividades.
<b>Secuencia lógica de actividades</b>	0,20	El proceso denota excelente correspondencia con su predecesor y su	El proceso denota buena correspondencia con su predecesor y su	El proceso denota limitada correspondencia con su predecesor y su	El proceso denota limitada correspondencia con su predecesor y su	El proceso carece de correspondencia con su predecesor y su

<b>Parámetros</b>	<b>Coefficiente de importancia</b>	<b>Completamente aceptable</b>	<b>Aceptable</b>	<b>Aceptable con correcciones menores</b>	<b>Aceptable con correcciones mayores</b>	<b>No aceptable</b>
		sucesor, además es entendible cada una de las actividades del proceso.	sucesor, además es entendible cada una de las actividades del proceso.	sucesor, además es poco entendible cada una de las actividades del proceso.	sucesor causando confusión en cada una de las actividades del proceso.	sucesor causando confusión en cada una de las actividades del proceso.
<b>Asignación de roles y responsabilidades</b>	0,07	Hay una excelente correspondencia entre las responsabilidades y los roles de la organización, lo cual hace que se pueda medir la correspondencia en base al cumplimiento del proceso y sus recursos.	Hay una buena correspondencia entre las responsabilidades y los roles de la organización, pero al medir la correspondencia no se obtienen los mejores resultados.	Hay correspondencia entre las responsabilidades y los roles de la organización, pero no se puede medir en base al cumplimiento del proceso y sus recursos.	Existe una limitada correspondencia entre las responsabilidades y los roles de la organización, además carece de medición en base al cumplimiento del proceso y sus recursos.	La correspondencia entre las responsabilidades y los roles es nula, además carece de medición en base al cumplimiento del proceso y sus recursos.
<b>Uso de normas internacionales de referencia</b>	0,07	Se aplica correctamente la norma a la cual hace referencia el proceso, cumpliendo con	Se aplica adecuadamente la norma a la cual hace referencia el proceso, acatando los	Se aplica parcialmente la norma a la cual hace referencia el proceso, cumpliendo de manera	La aplicación de la norma es mínima a la cual hace referencia el proceso, por lo cual los estándares y	El proceso carece de la aplicación de alguna norma, denotando déficit en los







<b>Parámetros</b>	<b>Coefficient e de importancia</b>	<b>Completamente aceptable</b>	<b>Aceptable</b>	<b>Aceptable con correcciones menores</b>	<b>Aceptable con correcciones mayores</b>	<b>No aceptable</b>
		los estándares y lineamientos.	estándares y lineamientos.	inadecuada los estándares y lineamientos	lineamientos son deficientes.	estándares y lineamientos.
<b>Sintaxis, redacción y semántica del contenido</b>	0,07	La redacción es completamente clara, con significado correcto, sin ambigüedades y de fácil comprensión.	La redacción es clara, con significado correcto, sin ambigüedades y de fácil comprensión.	La redacción es clara, con un significado correcto, pero muy extensa.	La redacción es ambigua, redundante y de difícil comprensión.	La redacción es pobre, prácticamente un escrito sin sentido.
<b>VALOR</b>		<b>5</b>	<b>4</b>	<b>3</b>	<b>2</b>	<b>1</b>

**Hallazgos:**

A continuación, se presenta de manera detallada el resumen y análisis de resultados realizados a los miembros del ESPE-CERT:

**Datos de los Evaluadores:****Tabla 11**

*Datos informativos de los Evaluadores*

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

*Nota: La tabla representa la información personal de cada uno de los evaluadores del proceso.*

**Resumen de resultados:****Tabla 12***Resumen de resultados de las Evaluaciones*

<b>Evaluador</b>	<b>Cumplimiento del objetivo del proceso</b>	<b>Eficiencia en el proceso</b>	<b>Sintaxis, redacción y semántica del contenido</b>	<b>Asignación de roles y responsabilidades</b>	<b>Uso de normas internacionales de referencia</b>	<b>Secuencia lógica de actividades</b>
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

*Nota: La tabla representa cada una de las ponderaciones realizadas por parte de los evaluadores de acuerdo a la rúbrica de evaluación enviada.*

**Tabla 13***Análisis de Resultados*

<b>Parámetros</b>	<b>Ponderaciones</b>				<b>Valor alcanzado</b>	<b>Valor Máximo (100%)</b>	<b>Estándar: Valor mínimo (80%)</b>	<b>% Alcanzado</b>
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 %

*Nota: En la tabla se detalla a manera de resumen cada una de las ponderaciones realizadas, así como también, el porcentaje de cumplimiento alcanzado.*

**Interpretación de resultados:**

**Cumplimiento del objetivo del proceso:** Con respecto al parámetro de cumplimiento del objetivo del proceso tras su evaluación se obtiene un cumplimiento del 100%, lo que indica

que cada una de las metas definidas hacia las cuales se dirigen las acciones que se pretenden lograr son cumplidas en su totalidad.

**Eficiencia en el proceso:** En relación al parámetro de Eficiencia en el proceso, luego de su evaluación se obtiene un cumplimiento del 100%, lo que indica un aprovechamiento total de los recursos del proceso, contribuyendo en su productividad y mejorando el tiempo de ejecución de sus actividades.

**Sintaxis, redacción y semántica del contenido:** En cuanto al parámetro de Sintaxis, redacción y semántica del contenido, después de su evaluación se obtiene un cumplimiento del 100%, lo que indica que el documento se encuentra completamente claro, su significado es correcto, sin ambigüedades y de fácil comprensión.

**Asignación de roles y responsables:** Se determina que el parámetro de asignación de roles y responsables obtuvo un cumplimiento del 90% lo cual evidencia que hubo buena correspondencia entre las responsabilidades y los roles en la organización, haciendo que el parámetro este dentro del mínimo aceptable que es del 80%.

**Uso de normas internacionales de referencia:** Se determina que el parámetro de uso de normas internacionales de referencia obtuvo un cumplimiento del 85% lo cual evidencia que hubo correcta aplicación de las normas, a pesar de que el parámetro se encuentre dentro del mínimo aceptable se hace necesario mejorarlo con el propósito de alcanzar un 100% de cumplimiento.

**Secuencia lógica de actividades:** Se determina que el parámetro secuencia lógica de actividades obtuvo un cumplimiento del 100% lo cual denota una excelente correspondencia entre su predecesor y su sucesor haciendo entendible cada una de las actividades del proceso, superando el mínimo aceptable que es del 80%.

**Oportunidades de mejora:**

Tras la interpretación de los resultados, se definen los parámetros de evaluación que, a pesar de cumplir con el porcentaje mínimo aceptable, no obtienen una calificación del 100% por lo cual se resumen los diferentes puntos de vista de los evaluadores que servirán para tomar las medidas necesarias y contribuir en el desempeño de los procesos.

- Asignación de roles y responsabilidades:

Los roles y responsabilidades definidos a nivel organizacional son los adecuados, sin embargo, hay que tener en consideración que en el ESPE-CERT, un operador con un rol definido puede colaborar en otras actividades que se necesiten y no solo en las que se establezcan para su rol, esto debido a la disponibilidad que tienen cada uno de los colaboradores.

Es conveniente que todas las personas que conforman el ESPE-CERT sean evaluadas de forma práctica y teórica por un superior, con el fin de asignar un rol y responsabilidades en base a las aptitudes demostradas en las evaluaciones.

- Uso de normas internacionales de referencia:

Se recomienda hacer un mejor uso de la norma internacional ISO 9001 ya que ayudará en la gestión y seguimiento continuo de la calidad de todos los procesos. Esta norma de calidad se considera una de las más importantes a nivel internacional, así como el estándar de referencia.

En cuanto a las normas de seguridad informática se recomienda hacer uso de las que tengan mayor impacto para que en un futuro conseguir una certificación ISO para garantizar que el CERT posee estándares o lineamientos para garantizar la efectividad, seguridad y alta calidad de sus servicios o productos.

## **Capítulo IV**

### **Introducción**

Con base al desarrollo metodológico establecido en el Capítulo III y las definiciones planteadas en el marco teórico del presente proyecto, se procede con la elaboración de la solución establecida frente a la problemática identificada en el ESPE-CERT, la cual corresponde al desarrollo de un Manual de Procesos Operativos para esta entidad.

**MANUAL DE PROCESOS Y PROCEDIMIENTOS**

**OPERATIVOS “ESPE-CERT”**

---

**AGOSTO 2022**

**SANGOLQUÍ - ECUADOR**



**CONTENIDO**

Historial de cambios

Prólogo

Introducción

Objeto y campo de aplicación

Referencias normativas

Términos y condiciones

Público objetivo

Autoridad

Descripción del documento

Mapa general de procesos

Roles y funciones

Normas de procedimiento

Disposiciones generales de aplicación

Disposiciones transitorias

Aprobación y legalización

**Historial de cambios:****Tabla 14***Control de cambios*

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

---

*Nota: En la tabla se detalla la información general del manual.*

## ***Prólogo***

Este manual es el resultado del trabajo conjunto realizado por docentes investigadores, personal del ESPE-CERT y alumnos tesistas. Fue desarrollado como parte del trabajo de titulación denominado “Desarrollo del manual de procesos operativos para el CERT académico de la ESPE utilizando estándares internacionales”, de la carrera de Ingeniería en Sistemas e Informática, destinado a proveer una guía para la ejecución de los servicios ofertados por el CERT.

A lo largo del proceso de elaboración de este manual, se enfrentaron problemas debido principalmente a la falta de información y acuerdos en la racionalización de procesos y construcción de las normas de procedimiento, pero con el apoyo de personal técnico y expertos en el tema, se logró solventar las dudas, corregir errores y terminar de manera satisfactoria el trabajo propuesto.

Con todas las experiencias vividas en el desarrollo del proyecto, se logró adquirir crecimiento a nivel académico y profesional, considerando que la seguridad informática es un área muy amplia, se realizó una extensa investigación acerca de normas y buenas prácticas de uso común en los equipos de respuesta nacionales e internacionales, con miras a la certificación del ESPE-CERT por parte del Foro Global de Equipos de respuesta ante Incidentes (FIRST- Forum of Incident Response and Security Teams).

## ***Introducción***

El Manual de Procesos Operativos se ha desarrollado con el objetivo de proporcionar una guía orientadora para la operación de cada uno de los servicios ofrecidos por el ESPE\_CERT, los procesos inherentes y cada una de las actividades que se llevan a cabo para su funcionamiento, para de esta manera constituirse en una herramienta que permita la operación del Equipo de Respuesta ante Emergencias Informáticas de la ESPE.

El manual describe de forma metódica las actividades que se han identificado en el CERT, contribuye al establecimiento de procesos y procedimientos documentados y de fácil comprensión para el personal a cargo y nuevos funcionarios, además, favorece al crecimiento y madurez de la organización al mejorar la relación con sus usuarios y permite enfrentar de manera adecuada nuevos requerimientos que surjan en el futuro.

### ***Objetivo y campo de aplicación***

- **Objetivo.** – Proporcionar una guía orientadora al personal del ESPE-CERT, para la ejecución de los procesos, procedimientos y actividades necesarios para prestar los servicios ofertados por la organización y de esta manera cumplir con la misión del Equipo de Respuesta.
- **Campo de Aplicación.** – El presente Manual de Procesos Operativos se aplicará a todos los servicios proactivos y reactivos que oferta el ESPE\_CERT.

### ***Referencias normativas***

- Norma NTC-ISO 9001:2015, sistemas de gestión de la calidad.
- Norma NTE INEN-ISO/IEC 27001 para la Gestión de Seguridad de la Información.
- Norma NIST SP 800-61, guía de gestión de incidentes de seguridad informática.
- La Norma NTE INEN-ISO/IEC 27002:2009, proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información.
- Norma NIST 800-50, creación de un programa de concientización sobre seguridad en TI.
- Norma NIST 800-115, guía técnica para la evaluación y pruebas de seguridad de la información.
- INCIBE Guía Técnica de Ciberataques presentados por el Instituto Nacional de Ciberseguridad.

### ***Términos y condiciones***

El manual es de uso particular para el personal del ESPE-CERT, puede utilizarse como referencia para otros equipos de respuesta, sin responsabilidad del autor al ser adoptado o modificado para uso externo.

Se prohíbe suprimir, alterar o modificar ya sea de forma total o parcial, cualquier sección del contenido del manual salvo que se expida una nueva versión legalmente aprobada por la Institución. Las recomendaciones de cambio o actualización o actualización de los procesos, procedimientos o actividades serán recibidas por el responsable del ESPE-CERT y serán consideradas por el equipo de revisión del manual.

### ***Público objetivo***

El público objetivo al cual está orientado este manual son pasantes, investigadores y especialmente personal de planta del ESPE-CERT que desempeñe funciones y responsabilidades operativas en la organización, así como los supervisores y personal relacionado de la UTIC y la Unidad de Seguridad Integrada (USI).

### ***Autoridad***

Se refiere a la obligación de cumplimiento y quien ejerce la autoridad general de aplicación de los procesos.

Los procesos son de obligatorio cumplimiento por el personal responsable de cada proceso, de su aplicación general en cada escalón jerárquico son responsables: la USI, la UTIC, el DCCO, el CERT.

### ***Descripción del documento***

El documento se encuentra dividido en tres partes, el primer apartado corresponde a la introducción, objetivos, campo de aplicación, autoridad y público objetivo. En la segunda parte se establece el mapa de procesos general de la organización en donde se resumen todos los procesos, procedimientos y cómo estos se interrelacionan entre sí, contiene también, las normas de procedimiento que se identifica con un código que facilita su clasificación y ubicación dentro del documento, la ficha técnica se estableció en base del formato establecido

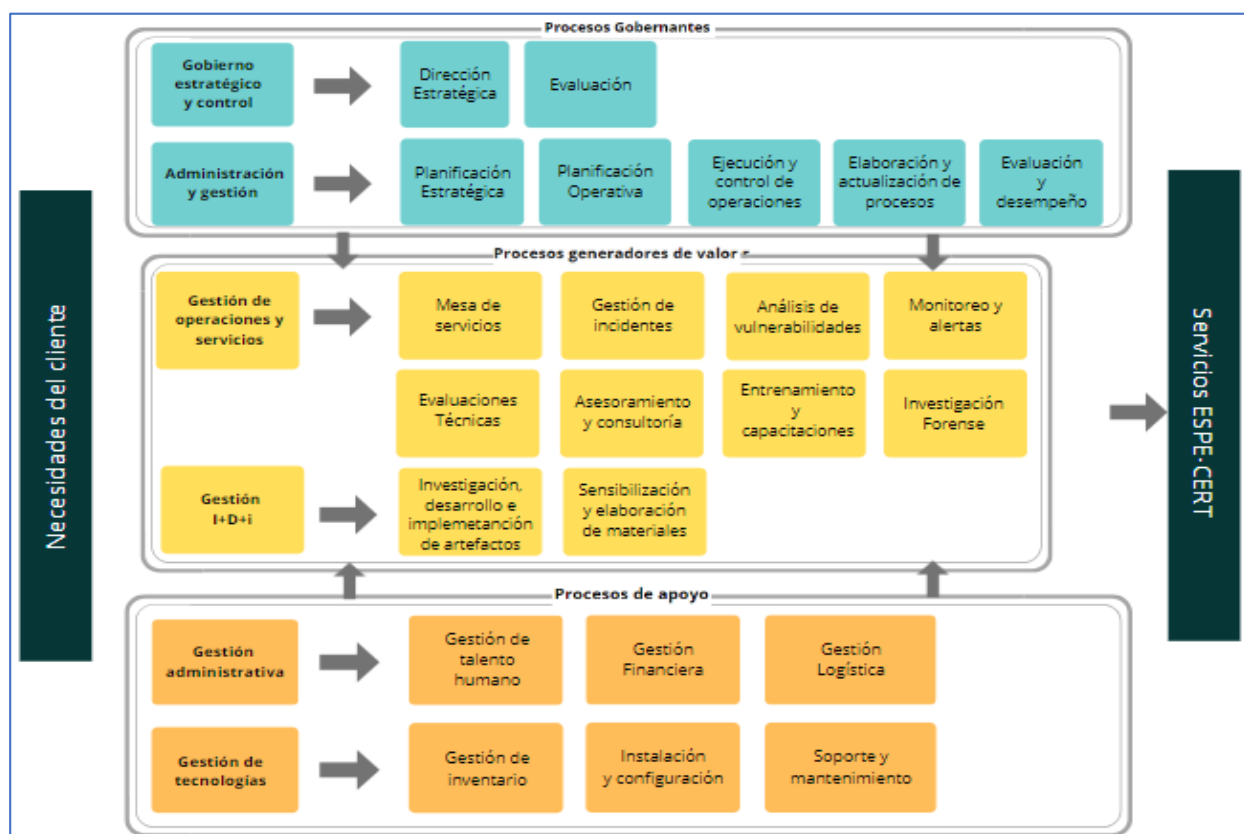
por la Norma NTC-ISO 9001:2015, Sistemas de Gestión de la Calidad. El contenido de la ficha, resulta del análisis e investigación de normativas internacionales referentes a las mejores prácticas relacionadas con los servicios que ofertan los equipos de respuesta ante incidentes informáticos en el mundo. Finalmente, en la tercera parte se definen las disposiciones generales, transitorias y la aprobación del manual.

### Mapa general de procesos

El mapa de procesos suministra una perspectiva global de la organización y permite visualizar los procesos, procedimientos y la interrelación entre ellos.

**Figura 16**

Mapa General de Procesos ESPE-CERT



*Nota:* La figura muestra la interrelación de los procesos del ESPE-CERT

## **Roles y Funciones**

En la siguiente tabla se resumen cada uno de los roles propuestos para el ESPE-CERT, así como también, sus respectivas funciones de las cuales estarán a cargo.

**Tabla 15**

*Roles y Funciones Propuestos para el (ESPE-CERT)*

<b>Roles</b>	<b>Funciones</b>
Operador	Encargado de ejecutar todas las actividades operativas de acuerdo a su disponibilidad y conocimiento en determinado tema.
Analista	Recepta, analiza y gestiona todas las peticiones realizadas por parte de los clientes.
Director Ejecutivo	Encargado de la aprobación de los planes de entrenamiento y concientización en el ámbito de Ciberseguridad y Ciberdefensa.
Consejo Ejecutivo	Encargado de la revisión y aprobación del diseño de los programas de entrenamiento y concientización en el ámbito de Ciberseguridad y Ciberdefensa.

*Nota: En la tabla se definen los roles y actividades propuestas para las operaciones diarias del ESPE-CERT.*



**Normas de procedimiento****CERT-02.01. Gestión de las operaciones y servicios del CERT.**

<b>Nro. de Proceso:</b> CERT-02.01.	<b>Nro. Hoja:</b> 10
<b>Elaboró:</b> Maycol Pacha	<b>NTE INEN- ISO 9001</b>
<b>Título:</b> Gestión de las operaciones y servicios del CERT.	

<b>Nro. de cambio al proceso</b>	<b>Elaboró</b>	<b>Revisó</b>	<b>Aprobó</b>	<b>Nro. de Páginas</b>
1	<b>Cargo:</b> Tesista <b>Nombre:</b> Maycol Pacha  <b>Firma:</b> 	<b>Cargo:</b> Tutor <b>Nombre:</b> Ing. Mario Ron MSc.  <b>Firma:</b>  <small>Firmado electrónicamente por:</small> <b>MARIO BERNABE RON</b>	<b>Cargo:</b> Director de Proyecto <b>Nombre:</b> Dr. Walter Fuertes D.  <b>Firma:</b>  <small>Firmado electrónicamente por:</small> <b>WALTER MARCELO FUERTES DIAZ</b>	4
	<b>Fecha:</b> 01-07-2022	<b>Fecha:</b> 03-08-2022	<b>Fecha:</b> 09-08-2022	

**CONTROL DE COPIAS DEL PROCESO**

<b>DEPARTAMENTO</b>	<b>FIRMA DE RECIBIDO</b>	<b>FECHA</b>
---------------------	--------------------------	--------------

<b>Nro. DE CAMBIO AL PROCESO</b>	<b>DESCRIPCIÓN DEL CAMBIO</b>
----------------------------------	-------------------------------

**Objetivo:**

- Establecer procedimientos clave para dar rentabilidad al observatorio.
- Agregar valor al cliente e instituciones.
- Apoyar a diferentes áreas de las instituciones cliente.

**Alcance:**

La gestión de operaciones y servicios ayuda a mantener satisfechos a los clientes y las instituciones a las que el CERT presta servicios mediante la gestión y el control efectivo de los recursos del observatorio. Para mantener su competitividad y viabilidad, el observatorio debe ser capaz de enfocar sus estrategias, ofertas y procedimientos operativos.

**Responsables:**

- Operadores ESPE-CERT.
- Analistas ESPE-CERT.
- Pasantes.
- Investigadores.
- Director ejecutivo ESPE-CERT.
- Consejo directivo ESPE-CERT.

**Base legal:**

LEY ORGANICA DE EDUCACION SUPERIOR, LOES:

**Art. 145 Principio de autodeterminación para la producción del pensamiento y conocimiento.** - Implica la creación de condiciones independientes para la educación, la creación y difusión del conocimiento en el marco del diálogo de saberes, la universalidad del pensamiento y los avances locales e internacionales de la ciencia y la tecnología.

**Art. 146 Garantía de la libertad de cátedra e investigativa.** - El derecho a la libertad de expresión está garantizado en las universidades y escuelas profesionales de política. Este derecho se entiende que permite al cuerpo docente de la institución y a sus instructores presentar los materiales del curso utilizando la dirección y las herramientas pedagógicas que estimen más adecuadas. Lo mismo se aplica a la libertad de investigación, que se define como la capacidad de la organización y de sus investigadores para buscar la verdad en los múltiples campos sin ningún tipo de barrera u obstrucción, con excepción de lo previsto en la Constitución. y la Ley vigente.

**Políticas:**

- Todos los procesos operativos deben ser evaluados mensualmente para fomentar la mejora de calidad en los servicios.
- Todos los procesos operativos se deben ajustar a políticas de aseguramiento de disponibilidad, confidencialidad e integridad de datos.
- Los datos que se obtengan en los procesos operativos son de uso exclusivo para el ESPE-CERT y sus investigaciones.
- Bajo ningún concepto se puede divulgar información obtenida en los procesos operativos, sin previa autorización.

**Definición:**

- **Operaciones:** un grupo de actividades destinadas a producir bienes o prestar servicios a los usuarios.
- **Servicios:** acciones destinadas a satisfacer una necesidad específica del cliente proporcionando un bien material y personalizado.

**Desarrollo:**

- Procedimiento CERT-02.01.01 Mesa de Servicios.
- Procedimiento CERT-02.01.02 Gestión de Incidentes.
- Procedimiento CERT-02.01.03 Análisis de vulnerabilidades.
- Procedimiento CERT-02.01.04 Monitoreo y alerta de primer nivel.
- Procedimiento CERT-02.01.05 Investigación Forense.
- Procedimiento CERT-02.01.06 Evaluación Técnica de Seguridad de la Información.
- Procedimiento CERT-02.01.07 Asesoramiento técnico y consultoría.
- Procedimiento CERT-02.01.08 Entrenamiento en el ámbito de la ciberseguridad y ciberdefensa.

**Indicadores de desempeño:**

- Indicadores basados en el procedimiento CERT-02.01.01 Mesa de Servicios.
- Indicadores basados en el procedimiento CERT-02.01.02 Gestión de Incidentes.
- Indicadores basados en el procedimiento CERT-02.01.03 Análisis de vulnerabilidades.
- Indicadores basados en el procedimiento CERT-02.01.04 Monitoreo y alerta de primer nivel.
- Indicadores basados en el procedimiento CERT-02.01.05 Investigación Forense.
- Indicadores basados en el procedimiento CERT-02.01.06 Evaluación Técnica de Seguridad de la Información.
- Indicadores basados en el procedimiento CERT-02.01.07 Asesoramiento técnico y consultoría.
- Indicadores basados en el procedimiento CERT-02.01.08 Entrenamiento en el ámbito de la ciberseguridad y ciberdefensa.

**CERT-02.01.01 MESA DE SERVICIOS.**

<b>Nro. de Proceso:</b> CERT-02.01.1	<b>Nro. de Hoja:</b> 14
<b>Elaboró:</b> Maycol Pacha	<b>NTE INEN- ISO 9001</b>
<b>Título:</b> Mesa de Servicios	

<b>Nro. de cambio al proceso</b>	<b>Elaboró</b> <b>Cargo:</b> Tesista <b>Nombre:</b> Maycol Pacha	<b>Revisó</b> <b>Cargo:</b> Tutor <b>Nombre:</b> Ing. Mario Ron MSc.	<b>Aprobó</b> <b>Cargo:</b> Director de Proyecto <b>Nombre:</b> Dr. Walter Fuertes D.	<b>Nro. de Páginas</b>
1	<b>Firma:</b> 	<b>Firma:</b>  <small>Firmado electrónicamente por:</small> <b>MARIO BERNABE RON</b>	<b>Firma:</b>  <small>Firmado electrónicamente por:</small> <b>WALTER MARCELO FUERTES DIAZ</b>	7
	<b>Fecha:</b> 01-07-2022	<b>Fecha:</b> 03-08-2022	<b>Fecha:</b> 09-08-2022	

**CONTROL DE COPIAS DEL PROCESO**

<b>DEPARTAMENTO</b>	<b>FIRMA DE RECIBIDO</b>	<b>FECHA</b>
<b>Nro. DE CAMBIO AL PROCESO</b>	<b>DESCRIPCIÓN DEL CAMBIO</b>	

**Objetivo:**

- Proveer a los usuarios un único punto de contacto mediante el cual se resuelvan y/o canalicen sus necesidades relativas al uso de servicios del ESPE-CERT.

**Alcance:**

El proceso de mesa de servicios es el principal y único punto de contacto entre clientes, empresas y socios con el ESPE-CERT. Centraliza las demandas e incidentes relacionados con TI en un solo lugar. Además, registra y monitorea todas las actividades con el objetivo de solucionarlas y evitar que se repitan.

**Responsables:**

- Analista ESPE-CERT.
- Operadores ESPE-CERT.

**Base legal:**

- **Reglamento para la Prestación de Servicios y Consultorías de la Universidad de las Fuerzas Armadas ESPE:** Documento que tiene por objeto regular las actividades de prestación de servicios y consultorías de la Universidad de las Fuerzas Armadas – ESPE.
- **Plan Estratégico ESPE- CERT:** Instrumento de gestión en el cual se define visión, misión, escenarios internos y externos, con las metas y objetivos institucionales claros, y medibles para alcanzar una situación futura en un período específico.
- **Normas de Control Interno de la Contraloría General del Estado:** Documento que detalla los controles internos sobre la tecnología de la información que aseguren la transparencia y la supervisión, así como la participación de la gerencia de alto nivel, de modo que las actividades y los procesos de tecnología de la información de la

organización deben estar bajo la supervisión de una unidad encargada de regular y estandarizar las normas institucionales. temas de tecnología.

- **Norma NTE INEN-ISO 9001:2015:** un estándar que hace referencia a la gestión de la calidad y ayuda a las organizaciones a cumplir con las expectativas y necesidades de sus clientes, así como a monitorear continuamente la eficiencia de todos los procesos.

#### **Políticas:**

- De protección de datos: El ESPE-CERT garantiza la protección de datos críticos de clientes y empresas.

Es responsabilidad del personal del ESPE-CERT el uso adecuado de los datos proporcionados por los clientes.

Los datos obtenidos por el ESPE-CERT son confidenciales y deben ser usados exclusivamente en las actividades propias del CERT.

- De revisión y registro de peticiones:
  - En caso de que el cliente no envíe toda la información necesaria para poder comenzar con la gestión del caso:

Se procederá a cerrarlo indicando que existe información faltante e invitando al cliente a que genere un nuevo caso con toda la información.

También es posible solicitar la información faltante, siempre y cuando el analista establezca cuánto tiempo puede esperar antes del vencimiento del caso.

- Creación de código de ticket:

El ESPE-CERT debe manejarse mediante códigos de tickets para la organización interna y documental del centro. Los códigos ayudan en la organización para:

— Búsqueda de información más rápida.

- Asignación inteligente de tareas.
- Comunicación más fluida.
- Mejor seguimiento de casos.
- Mejor organización en temas de auditoría.

El Código del ticket debe estar compuesto como se muestra en la figura 17:

**Figura 17**

*Estructura del código de ticket*



*Nota: La imagen representa la estructura estandarizada para registrar una solicitud.*

Códigos por servicios:

**Tabla 16**

*Código de servicios ofertados por el ESPE-CERT*

Servicio	Código	Procedimientos
Preventivo	SP	Análisis de vulnerabilidad. Investigación forense. Evaluaciones técnicas.
Reactivo	SR	Gestión de incidentes. Revisión de eventos.
Temas de Investigación	IDI	Gestión de desarrollo I+D+i.
Gestión de la Calidad	GC	Entrenamiento. Sensibilización. Soporte.

*Nota: Código de todos los servicios que oferta el ESPE-CERT*



**Definición:**

- **Mesa de servicio:** Principal y único punto de contacto entre clientes, empresas y socios, en donde se centralizan las demandas e incidentes relacionados con TI en un solo lugar.
- **Servicios:** una colección de actividades destinadas a satisfacer las necesidades de un cliente.

**Desarrollo:**

1. El cliente envía la petición mediante el Ingreso al Portal:  
<https://especare.freshdesk.com/support/home>
  - a. Generar ticket por el portal.
  - b. Registrar peticiones.
2. El cliente envía la petición mediante correo electrónico a la siguiente dirección:  
[espe-cert@espe.edu.ec](mailto:espe-cert@espe.edu.ec)
3. El analista examina el ticket: En esta actividad se verificará la validez de las peticiones y determinará a qué procedimiento corresponde la necesidad atendida, así como también, se excluirá aquellos casos en donde no se proporcione la información necesaria para el levantamiento del ticket, o que no se encuentre dentro de las categorías de servicios que oferta la organización.
4. El analista crea el caso: En esta actividad se crea el caso a ser atendido, para ello el código del ticket debe estar de acuerdo a la estructura establecida en las políticas del procedimiento en curso, además, es su responsabilidad adjuntar toda la información necesaria para su posterior gestión.
5. El analista prioriza una petición de acuerdo a parámetros como: fecha y hora de registro, disponibilidad de los operadores, criticidad de impacto, impacto actual e

impacto futuro, siendo de índole prioritaria la atención a miembros que conforman las diferentes áreas y departamentos de la Universidad de las Fuerzas Armadas "ESPE".

6. El analista seleccionará al agente: La asignación de operadores se realizará de acuerdo a la temática sobre la cual versa la necesidad del cliente, la carga de trabajo de los operadores y su experiencia en determinado tema.
7. Resolución de petición: De acuerdo con el análisis del ticket efectuado, el analista gestionará la petición desde los diferentes procedimientos definidos por el ESPE-CERT.

*Nota: Cada uno de los pasos expuestos son extractos de la Biblioteca de infraestructura de tecnología de la información V4 - Information Technology Infrastructure Library V4, adaptados a las necesidades actuales del ESPE-CERT.*

**Indicadores de desempeño:**

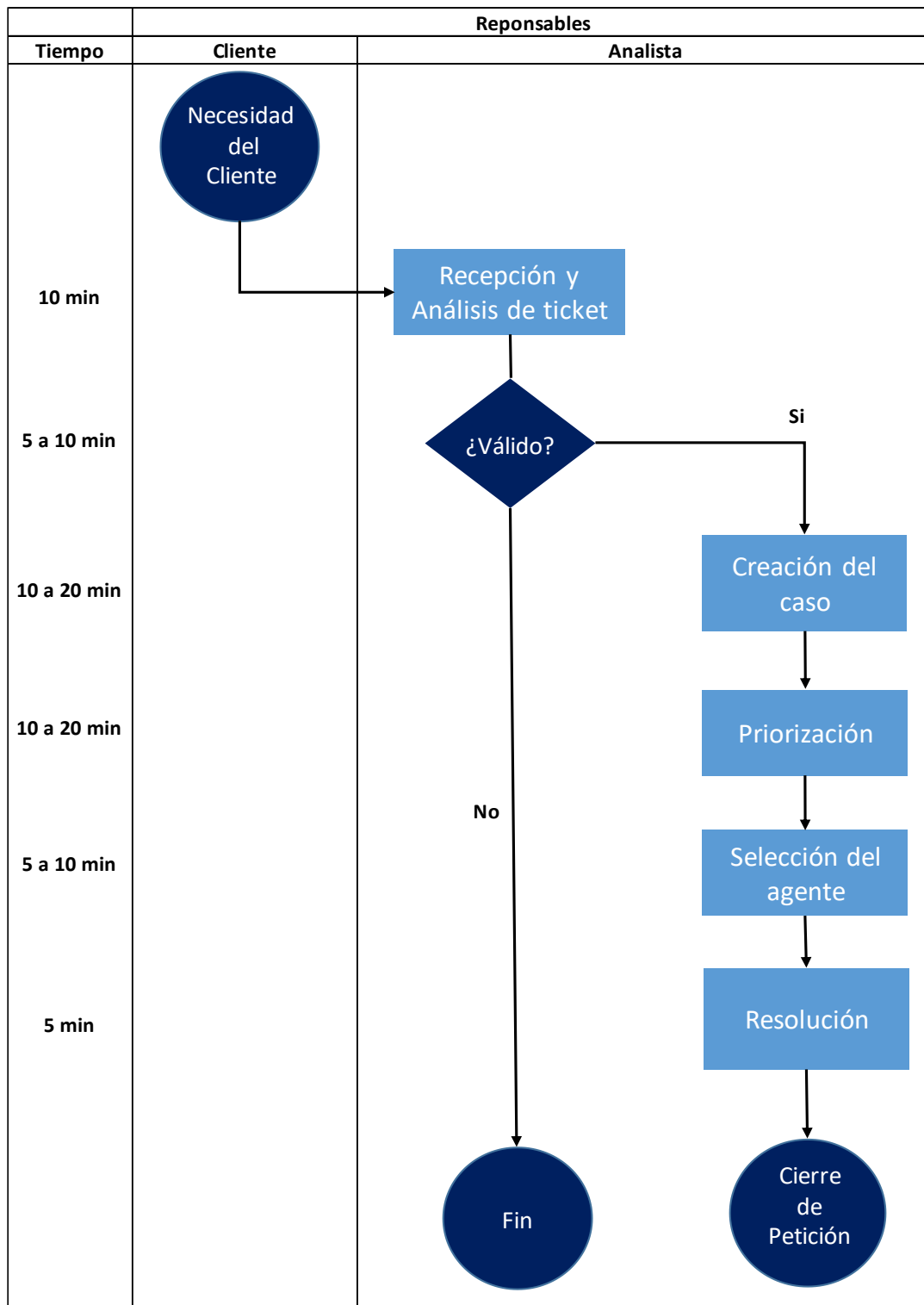
- Número de necesidades atendidas.
- Número de tickets resueltos.
- Tiempo de respuesta y tiempo de espera.

**Diagrama de flujo:**

- Diagrama De Flujo Espe-Cert, Código CERT-02.01.01

**Figura 18**

*CERT-02.01.01 Mesa de servicios*



**CERT-02.01.02 GESTIÓN DE INCIDENTES.**

<b>Nro. de Proceso:</b> CERT-02.01.02	<b>Nro. de Hoja:</b> 21
<b>Elaboró:</b> Maycol Pacha	<b>NTE INEN- ISO 9001</b>
<b>Título:</b> Gestión de Incidentes	

<b>Nro. de cambio al proceso</b>	<b>Elaboró</b>	<b>Revisó</b>	<b>Aprobó</b>	<b>Nro. de Páginas</b>
<b>1</b>	<b>Cargo:</b> Tesista <b>Nombre:</b> Maycol Pacha  <b>Firma:</b> 	<b>Cargo:</b> Tutor <b>Nombre:</b> Ing. Mario Ron MSc.  <b>Firma:</b>  <small>Firmado electrónicamente por:</small> <b>MARIO BERNABE RON</b>	<b>Cargo:</b> Director de Proyecto <b>Nombre:</b> Dr. Walter Fuertes D.  <b>Firma:</b>  <small>Firmado electrónicamente por:</small> <b>WALTER MARCELO FUERTES DIAZ</b>	<b>5</b>
	<b>Fecha:</b> 01-07-2022	<b>Fecha:</b> 03-08-2022	<b>Fecha:</b> 09-08-2022	

**CONTROL DE COPIAS DEL PROCESO**

<b>DEPARTAMENTO</b>	<b>FIRMA DE RECIBIDO</b>	<b>FECHA</b>
<b>Nro. DE CAMBIO AL PROCESO</b>	<b>DESCRIPCIÓN DEL CAMBIO</b>	

**Objetivo:**

- Reducir los posibles riesgos e impactos que pueda causar un incidente en la organización mediante las salvaguardas adecuadas como parte de la respuesta a tal incidente.

**Alcance:**

El proceso de gestión de incidentes se refiere a las actividades que realiza el ESPE-CERT para dar solución a un evento que puede afectar a la institución del cliente. El objetivo es minimizar el impacto negativo de la organización dando pronta solución al problema.

**Responsables:**

- Analista ESPE-CERT.
- Operadores ESPE-CERT.

**Base legal:**

- Acta de Reconocimiento N° 166 emitida por la Secretaría de la Función Pública de la Nación, por la cual se deroga formalmente el Esquema Gubernamental de Seguridad de la Información.
- Normas Técnicas Ecuatorianas NTE INEN- ISO /IEC 27000 para la Gestión de la Seguridad de la Información.
- Normas del National Institute of Standards and Technology (NIST) SP 800-61 (Referencial).

**Políticas:**

- De protección de datos: El ESPE-CERT garantiza la protección de datos críticos de clientes y empresas.

- Es responsabilidad del personal del ESPE-CERT el uso adecuado de los datos proporcionados por los clientes.
- Los datos obtenidos por el ESPE-CERT son confidenciales y deben ser usados exclusivamente en las actividades propias del CERT.
- Todo incidente de seguridad que sea reportado. La organización debe:
  - Realizar la gestión de cada incidente teniendo en cuenta todas las fases de su ciclo de vida, incluido el informe, la asignación, el tratamiento, la respuesta y el cierre.
  - El proceso de gestión de incidentes debe explicar de forma clara y concisa los procedimientos y métodos para la presentación de informes de incidentes de seguridad, así como la cantidad mínima de información que se debe proporcionar; manteniendo la confidencialidad de la información proporcionada por el denunciante, así como su anonimato.

**Definición:**

- **Incidente:** Intento de acceso, uso, divulgación, modificación o destrucción de información no autorizada.
- **Impacto:** Medida del alcance del daño potencial que el incidente puede causar.

**Desarrollo:****Registro:**

1. **El operador registra el incidente:** Todo evento catalogado como incidente será registrado en el sistema de gestión de tickets “Freshdesk”, para ello será responsabilidad del operador verificar la validez del incidente reportado.
2. **El operador prioriza los incidentes:** Un incidente tendrá una prioridad de atención de acuerdo a parámetros como: Criticidad de impacto, impacto actual e impacto futuro.

**Gestión del incidente:**

1. **El operador analiza el incidente:** En esta actividad se establecen los lineamientos iniciales para dar respuesta al incidente, para ello se verifica que dentro de la petición se haya especificado todos los datos críticos que permiten la identificación del incidente, caso contrario el operador se pondrá en contacto con el cliente para recabar con toda la información necesaria.
2. **El operador busca soluciones:** De acuerdo al tipo de prioridad se asignan los recursos destinados a dar una pronta respuesta al incidente registrado, siendo la prioridad Alta y Superior los que recibirán la máxima asignación de recursos, cabe señalar que las herramientas que apoyan esta actividad estarán disponibles en su totalidad.
3. **El operador elabora el informe:** Todas las especificaciones técnicas y recomendaciones referentes a la mitigación del incidente deberán ser registradas por parte del operador encargado en el formato: INST-01 MANUAL DE SERVICIOS PROACTIVOS.

*Nota: Cada uno de los pasos expuestos son extractos de la (NIST 800-61) Guía de seguridad para la Gestión de Incidentes - Computer Security Incident Handling Guide, adaptados a las necesidades actuales del ESPE-CERT.*

**Indicadores de desempeño:**

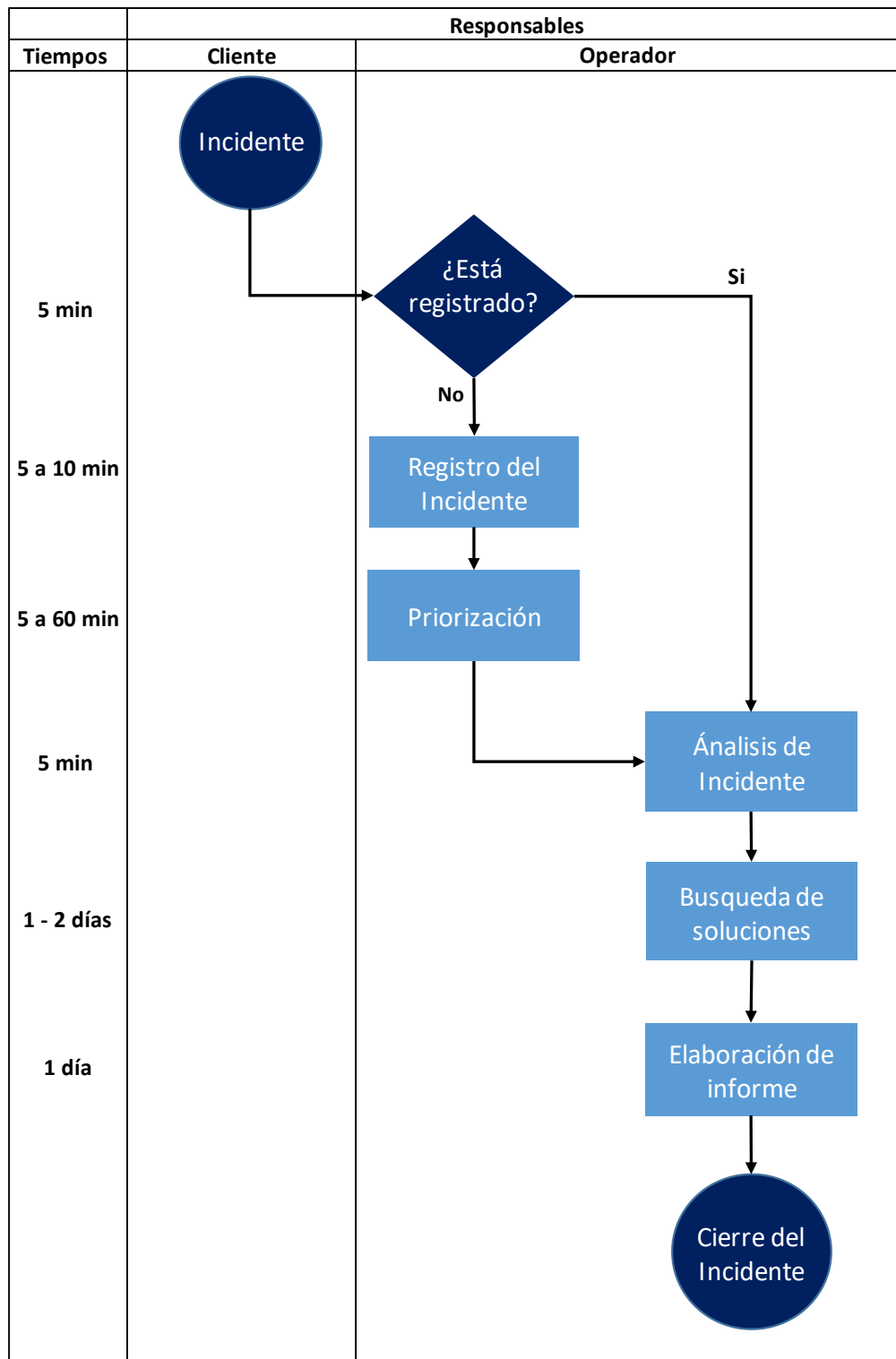
- Número de incidentes atendidos.
- Tiempo de respuesta y tiempo de espera.

**Diagrama de flujo:**

- Diagrama De Flujo Espe-Cert, Código CERT-02.01.02

**Figura 19**

*CERT-02.01.02 Gestión de Incidentes*





**CERT-02.01.03 ANÁLISIS DE VULNERABILIDADES.**


---

**Nro. de Procedimiento:** CERT02.01.03      **Nro. de Hoja:** 26

---

**Elaboró:** Juan Ruiz      **NTE INEN- ISO 9001**


---

**Título:** Análisis de vulnerabilidades
 

---

<b>Nro. de cambio al proceso</b>	<b>Elaboró</b> <b>Cargo:</b> Tesista <b>Nombre:</b> Juan Ruiz	<b>Revisó</b> <b>Cargo:</b> Tutor <b>Nombre:</b> Ing. Mario Ron MSc.	<b>Aprobó</b> <b>Cargo:</b> Director de Proyecto <b>Nombre:</b> Dr. Walter Fuertes D.	<b>Nro. de Páginas</b>
1	<b>Firma:</b> 	<b>Firma:</b>  <small>Firmado electrónicamente por:</small> <b>MARIO BERNABE RON</b>	<b>Firma:</b>  <small>Firmado electrónicamente por:</small> <b>WALTER MARCELO FUERTES DIAZ</b>	7
	<b>Fecha:</b> 03-07-2022	<b>Fecha:</b> 03-08-2022	<b>Fecha:</b> 09-08-2022	

---

**CONTROL DE COPIAS DEL PROCEDIMIENTO**

<b>DEPARTAMENTO</b>	<b>FIRMA DE RECIBIDO</b>	<b>FECHA</b>
---------------------	--------------------------	--------------

---

<b>Nro. DE CAMBIO AL PROCESO</b>	<b>DESCRIPCIÓN DEL CAMBIO</b>
----------------------------------	-------------------------------

---

**Objetivo:**

- Monitorear, identificar y clasificar las vulnerabilidades y/o debilidades presentes en los diferentes equipos, servidores, servicios, sistemas de la organización, optimizando las configuraciones de software de los activos, para aumentar la seguridad del entorno de trabajo evitando que se produzcan posibles ataques.

**Alcance:**

El procedimiento de análisis de vulnerabilidades identifica los sistemas en la red que tienen vulnerabilidades conocidas o identificadas, como explotaciones, fallas, brechas de seguridad, puntos de entrada no seguros y errores de configuración del sistema.

**Responsables:**

- Analista ESPE-CERT.
- Operadores ESPE-CERT.

**Base legal:**

RESOLUCIÓN No. 005-CCE-PLE-2021

“REGLAMENTO INTERNO DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN DE LA CORTE CONSTITUCIONAL”

- Norma técnica UNE-EN ISO/IEC 27001 Sistemas de Gestión de Seguridad de la Información.
- **Artículo 8 Responsabilidades de la delegada o delegado de Seguridad de la Información.** - La servidora o servidor público de la Gestión Interna de Infraestructura, Seguridades y Comunicaciones de la Dirección Nacional de Tecnologías de la Información y Comunicaciones, asumirá como delegada o delegado de Seguridad de la Información y, además de las funciones determinadas en su perfil de puesto, cumplirá

las siguientes responsabilidades dentro del seguimiento de la seguridad de la información:

- Ayudar al público en general y a los proveedores de servicios con la ejecución del estudio sobre la gestión de riesgos de seguridad de la información en muchas áreas.
- Crear un plan para monitorear y gestionar la implementación de acciones correctivas o medidas de mejora.
- Coordinar la elaboración del Plan de Continuidad de Seguridad de la Información.
- Orientar y desarrollar un procedimiento adecuado para el manejo de los incidentes de seguridad de la información que se presenten al interior de la institución.
- Verificar la implementación de las políticas, procedimientos y controles de seguridad institucional establecidos.

**Políticas:**

- De protección de datos:
  - El ESPE-CERT garantiza la protección de datos críticos de clientes y empresas.
  - Es responsabilidad del personal del ESPE-CERT el uso adecuado de los datos proporcionados por los clientes.
  - Los datos obtenidos por el ESPE-CERT son confidenciales y deben ser usados exclusivamente en las actividades propias del CERT.
- Todo incidente de seguridad que sea reportado. La organización debe:
  - Realizar la gestión de cada incidente teniendo en cuenta todas las fases de su ciclo de vida, incluido el informe, la asignación, el tratamiento, la respuesta y el cierre.
  - El proceso de gestión de incidentes debe explicar de forma clara y concisa los mecanismos y procedimientos para la presentación de informes de incidentes de seguridad, así como la cantidad mínima de información a proporcionar, manteniendo

la confidencialidad de la información proporcionada por el denunciante y su anonimato.

- Informar de forma completa e inmediata al responsable de Seguridad de la información la existencia de un potencial incidente de seguridad informática.

#### **Definición:**

- **Vulnerabilidad:** Fallo existente en el sistema que podría ser explotado por alguien con intenciones maliciosas de comprometer su seguridad.
- **Análisis de riesgo informático:** Proceso de identificación de las actividades informáticas, sus debilidades y amenazas, así como la probabilidad de que ocurran y sus efectos, con el fin de decidir las mejores medidas de seguridad para aceptar, reducir, transferir o prevenir la ocurrencia del riesgo.

#### **Desarrollo:**

1. **Identificación de activos.** - Primeramente, se deben conocer todos los activos de tecnología que forman parte de la infraestructura de la organización, como software y hardware. Con ese levantamiento, es posible tener una idea de donde se encuentran las principales vulnerabilidades y cuáles son las actividades críticas que deben ser tratadas.
2. **Planificar análisis.** - El operador encargado del ESPE-CERT, con actividades inmersas en Seguridad de la Información envía correos para planificar el análisis de vulnerabilidades, en la que se plantea un esquema y se identifican los elementos a los que se realizará el análisis. Si el análisis debe realizarse bajo demanda, el asunto del correo es para planificar las acciones a realizarse en torno al pedido realizado. El detalle del correo debe tener el siguiente detalle.

- a. Definir los activos que van a ser analizados y el alcance del análisis (aplicaciones, sistemas operativos, software y librerías, base de datos, entre otros).
- b. Definir información de vulnerabilidades.
- c. Priorización de las vulnerabilidades según grado de afectación.
- d. Definir el tiempo de cierre, de acuerdo a la prioridad.
- e. Planificar las actividades con cada dueño de los activos: Coordinar con los dueños de los activos la fecha y hora del análisis en base a las acciones que van a ser realizadas

**3. Realizar escaneo y analizar vulnerabilidades.** - El ESPE-CERT cuenta con herramientas que ayudan en el proceso de levantamiento de información; una de ellas es NNESSUS, el cual es un escáner de vulnerabilidades de varios sistemas operativos que muestra la información ordenada y precisa sobre los dispositivos analizados, si dentro del escáner se identifican incidentes informáticos, se continúa con el proceso de gestión de incidentes de lo contrario se cierra la petición y se informa al cliente que no se encontraron vulnerabilidades.

**4. Gestión del Incidente:** Si al realizar el análisis se detecta alguna vulnerabilidad se realizan las respectivas actividades que corresponden al procedimiento denominado Gestión de Incidentes, Código CERT-02.01.02, de lo contrario finaliza el procedimiento.

*Nota: Cada uno de los pasos expuestos son extractos de la (NIST 800-115) Guía técnica para la evaluación y pruebas de seguridad de la información, adaptados a las necesidades actuales del ESPE-CERT.*

### **Indicadores de desempeño**

- Número de falsos positivos / falsos negativos

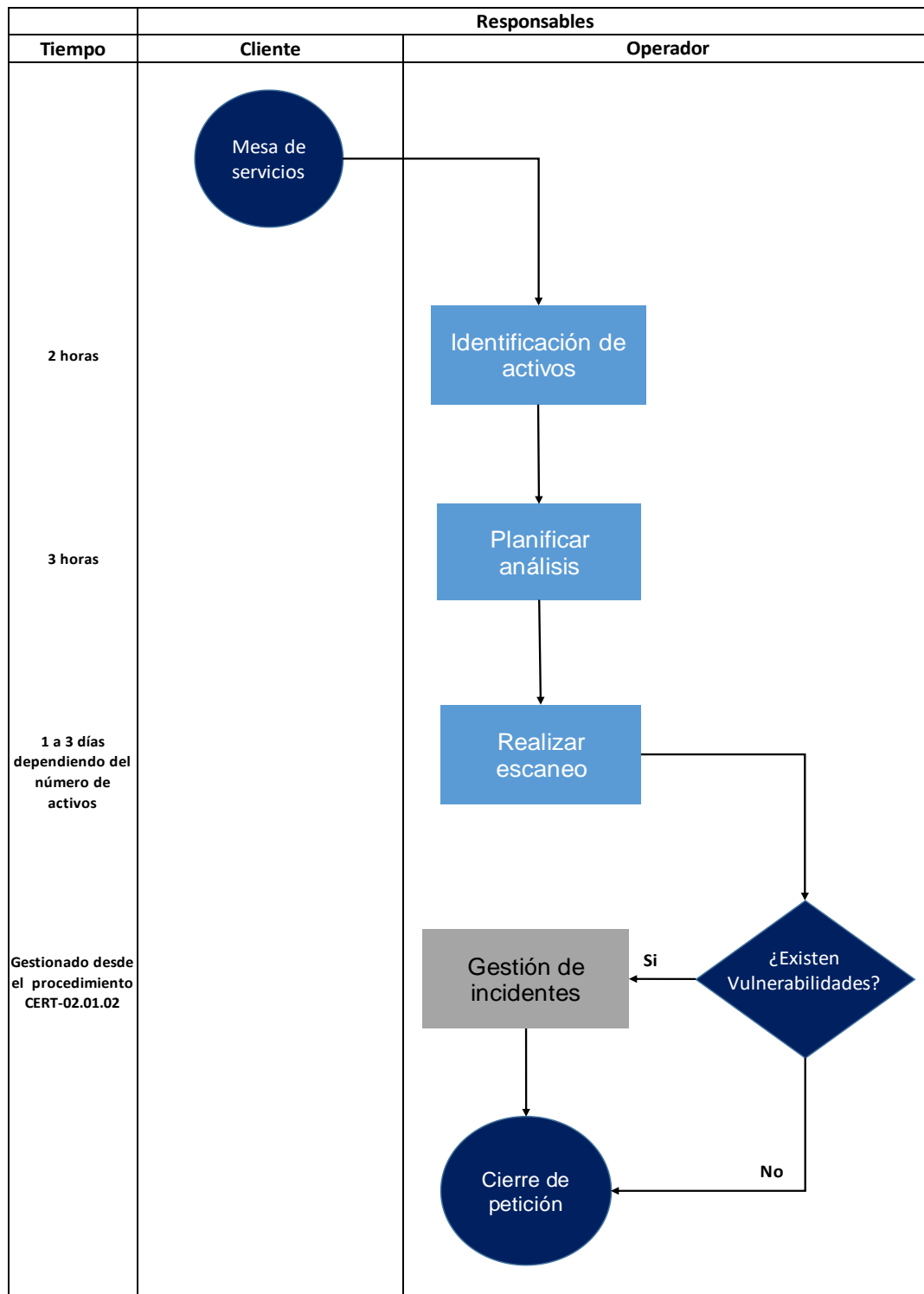
- Número de activos críticos que requieren otro tipo de análisis.

**Diagrama de flujo:**

- Diagrama De Flujo Espe-Cert, Código CERT-02.01.03



**Figura 20**

*CERT-02.01.03 Análisis de Vulnerabilidades*



**CERT-02.01.04 MONITOREO Y ALERTA DE PRIMER NIVEL.**

<b>Nro. de Procedimiento:</b> CERT02.01.04	<b>Nro. de Hoja:</b> 33
<b>Elaboró:</b> Juan Ruiz	<b>NTE INEN- ISO 9001</b>
<b>Título:</b> Monitoreo y Alerta de Primer Nivel	

<b>Nro. de cambio al proceso</b>	<b>Elaboró</b> <b>Cargo:</b> Tesista <b>Nombre:</b> Juan Ruiz	<b>Revisó</b> <b>Cargo:</b> Tutor <b>Nombre:</b> Ing. Mario Ron MSc.	<b>Aprobó</b> <b>Cargo:</b> Director de Proyecto <b>Nombre:</b> Dr. Walter Fuertes D.	<b>Nro. de Páginas</b>
1	<b>Firma:</b> 	<b>Firma:</b>  Firmado electrónicamente por: <b>MARIO BERNABE RON</b>	<b>Firma:</b>  Firmado electrónicamente por: <b>WALTER MARCELO FUERTES DIAZ</b>	5
	<b>Fecha:</b> 03-07-2022	<b>Fecha:</b> 03-08-2022	<b>Fecha:</b> 09-08-2022	

**CONTROL DE COPIAS DEL PROCEDIMIENTO**

<b>DEPARTAMENTO</b>	<b>FIRMA DE RECIBIDO</b>	<b>FECHA</b>
<b>Nro. DE CAMBIO AL PROCESO</b>	<b>DESCRIPCIÓN DEL CAMBIO</b>	



**Objetivo:**

- Informar a los usuarios de las nuevas vulnerabilidades y técnicas de intrusión detectadas, por medio de alertas, y notificaciones para proteger los sistemas de información de los nuevos riesgos de seguridad antes de que se materialicen.

**Alcance:**

El proceso consiste en revisar los logs y eventos que sucedan dentro de la red del cliente, junto con un análisis de los activos que están involucrados dentro de las conexiones de la institución.

**Responsables:**

- Analista ESPE-CERT.
- Operadores ESPE-CERT.

**Base legal:**

- La Norma Técnica NTE INEN-ISO/IEC 27002:2009 realizará las tareas de seguimiento y control del cumplimiento de la presente política, para lo cual se dará acceso a los registros de auditoría de las aplicaciones electrónicas, a la información contenida en los datos institucionales bases, y la información en poder de los funcionarios de la institución.

**Políticas:**

- ESPE-CERT acordará funciones y responsabilidades a los empleados encargados de monitorear y alertar dentro de la entidad.
- Es obligación de los operadores:

- Realizar monitoreos diarios para cumplir con los estándares de seguridad establecidos.
- Comunicar las alertas encontradas, máximo 2 horas después de haberlas detectado.

**Definición:**

- **Monitoreo:** La revisión y supervisión de todas las actividades realizadas a través de la infraestructura y el ecosistema de una organización constituye monitoreo.
- **Alerta:** El término "alerta" se refiere a los mensajes enviados a un usuario específico sobre eventos inminentes del sistema que requieren notificación. Lo mismo debe perdurar en todo el sistema hasta que se brinde una solución.

**Desarrollo:**

1. **Ingreso a la herramienta software.** - El operador o analista debe ingresar al portal <https://especare.freshdesk.com/support/home> para utilizar las herramientas instaladas para monitorear eventos, cada operador debe ingresar en su equipo y usuario designado.
2. **Revisión de eventos y logs.** - Para realizar la revisión, el operador debe determinar qué fuentes de registros están disponibles y qué herramientas automatizadas se pueden utilizar. Para ello, se realizará una copia de los registros y se trasladará a otra ubicación donde se puedan revisar sin cambiar el original, registros.
3. **Análisis de eventos.** - El operador realizará un análisis de los logs y eventos para identificar si se trata de un incidente. En el caso de ser positivo, pasa al procedimiento de gestión de incidente, en el caso contrario se cierra el monitoreo y se informa al cliente.

4. **Procedimiento de Gestión de Incidentes.** – Si se detecta algún incidente se realizan las respectivas actividades que corresponden al procedimiento denominado Gestión de Incidentes, Código CERT-02.01.02 de lo contrario finaliza el procedimiento.

*Nota: Cada uno de los pasos expuestos son extractos de la (NIST SP 800-61) Guía para el manejo de incidentes de seguridad informática, adaptados a las necesidades actuales del ESPE-CERT.*

**Indicadores de desempeño:**

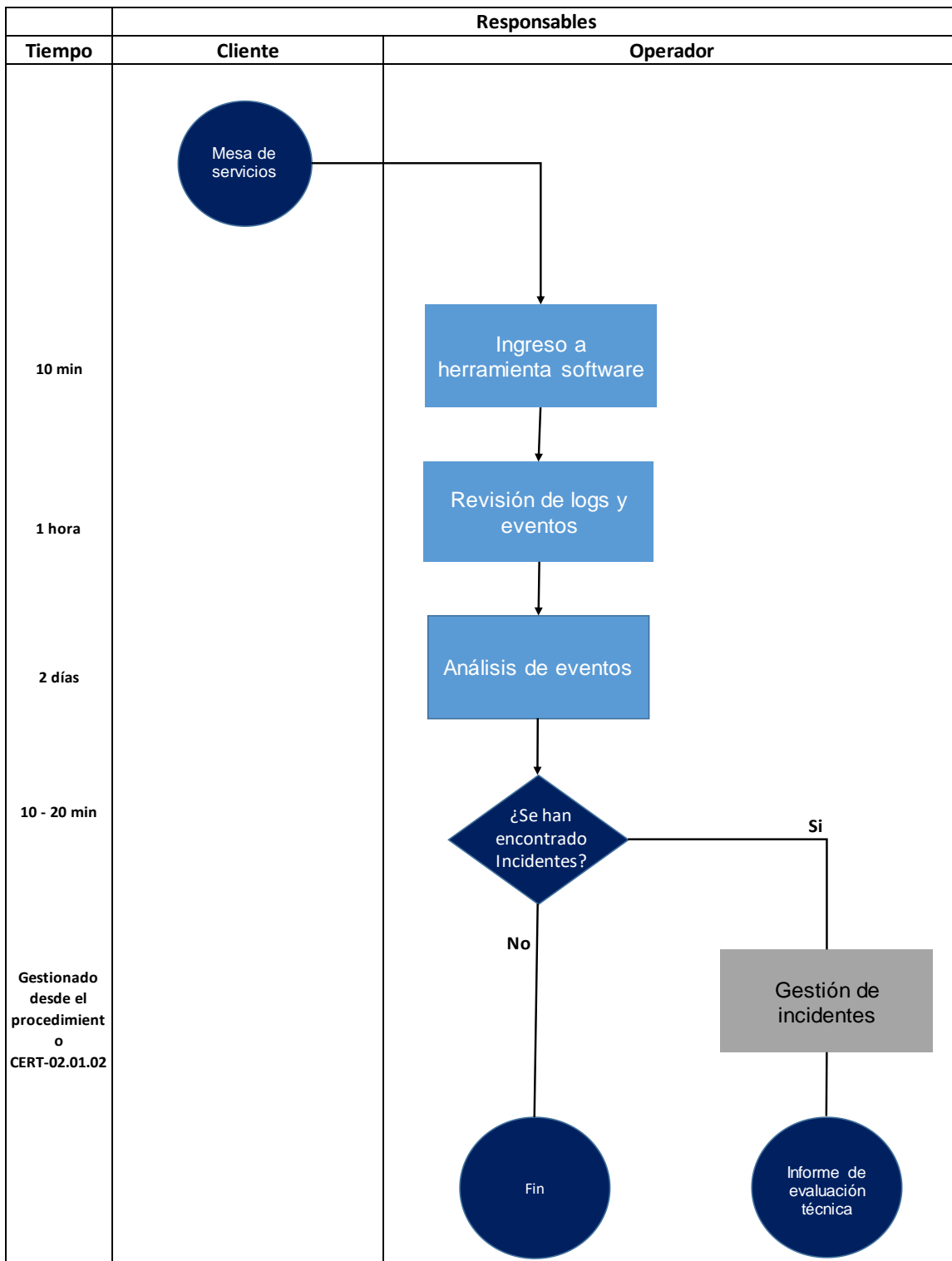
- Número de eventos que se identificaron y se lograron resolver con éxito en los tiempos establecidos.
- Número de vulnerabilidades conocidas por el ESPE – CERT.

**Diagrama de flujo:**

- Diagrama De Flujo Espe-Cert, Código CERT-02.01.04

**Figura 21**

*CERT-02.01.04 Monitoreo y alerta de primer nivel*



**CERT-02.01.05 INVESTIGACIÓN FORENSE.**

<b>Nro. de Proceso:</b> CERT-02.01.05	<b>Nro. de Hoja:</b> 38
<b>Elaboró:</b> Maycol Pacha	<b>NTE INEN- ISO 9001</b>
<b>Título:</b> Investigación Forense	

<b>Nro. de cambio al proceso</b>	<b>Elaboró</b> <b>Cargo:</b> Tesista <b>Nombre:</b> Maycol Pacha	<b>Revisó</b> <b>Cargo:</b> Tutor <b>Nombre:</b> Ing. Mario Ron MSc.	<b>Aprobó</b> <b>Cargo:</b> Director de Proyecto <b>Nombre:</b> Dr. Walter Fuertes D.	<b>Nro. de Páginas</b>
1	<b>Firma:</b> 	<b>Firma:</b>  Firmado electrónicamente por: <b>MARIO BERNABE RON</b>	<b>Firma:</b>  Firmado electrónicamente por: <b>WALTER MARCELO FUERTES DIAZ</b>	6
	<b>Fecha:</b> 01-07-2022	<b>Fecha:</b> 03-08-2022	<b>Fecha:</b> 09-08-2022	

**CONTROL DE COPIAS DEL PROCESO**

<b>DEPARTAMENTO</b>	<b>FIRMA DE RECIBIDO</b>	<b>FECHA</b>
---------------------	--------------------------	--------------

<b>Nro. DE CAMBIO AL PROCESO</b>	<b>DESCRIPCIÓN DEL CAMBIO</b>
----------------------------------	-------------------------------

**Objetivo:**

- Evitar que los delitos informáticos vuelvan a ocurrir, minimizando el riesgo futuro y preparando un caso sólido, contundente y con pruebas irrefutables para las acciones legales a que haya lugar.

**Alcance:**

El término " investigación forense " se refiere a un conjunto de métodos y procedimientos para identificar, recopilar, preservar, extraer, interpretar, documentar y presentar pruebas de equipo de cómputo para que sean aceptadas durante un proceso legal o administrativo ante un juez.

**Responsables:**

- Analista ESPE-CERT.
- Operadores ESPE-CERT.
- Investigador Forense ESPE-CERT.

**Base legal:**

- **Normas de Control Interno de la Contraloría General del Estado:** Documento que detalla los controles internos sobre la tecnología de la información que aseguren la transparencia y la supervisión, así como la participación de la gerencia de alto nivel, de modo que las actividades y los procesos de tecnología de la información de la organización deben estar bajo la supervisión de una unidad encargada de regular y estandarizar las normas institucionales. temas de tecnología.
- **Código Orgánico Integral Penal, COIP:** Además, el uso del mismo debe ser considerado como una guía del profesional del investigador en el uso de las ciencias de la prospectiva que permite aplicar adecuadamente el formato del cuestionario de

informe social y proyecta su aplicación a todas las consultas realizadas por la autoridad competente a nivel nacional.

**Políticas:**

- De protección de datos: El ESPE-CERT garantiza la protección de datos críticos de clientes y empresas.
  - Es responsabilidad del personal del ESPE-CERT el uso adecuado de los datos proporcionados por los clientes.
  - Los datos obtenidos por el ESPE-CERT son confidenciales y deben ser usados exclusivamente en las actividades propias del CERT.
- De destrucción de información: Política de destrucción de información, registros, activos, etc., para garantizar la protección de datos cuando algún servicio o dispositivo llegue a su fin.
  - El personal que cuente con información confidencial sin autorización deberá informar a la dirección para destruirla mediante los procesos establecidos para la destrucción de información.
- De acceso a información: Analiza los permisos de acceso del personal a la infraestructura TI y a la información crítica del ESPE-CERT, tomando en cuenta la comunidad a quien da sus servicios.
  - Es considerado un activo tecnológico cuando: el hardware, software, equipos informáticos, servidores, infraestructura de red consten en el inventario institucional de la ESPE.
  - Es propiedad de la Universidad de las Fuerzas Armadas toda información obtenida de dichos activos tecnológicos excluyendo la información personal de los trabajadores.

- Los usuarios y claves de acceso son intransferibles.

**Definición:**

- **Auditoría:** Examen crítico y de cumplimiento que realiza una persona o grupo de personas independientes.
- **Forense:** Significa adecuado para su uso en la corte. Para efectos prácticos el concepto de Forense es relativo a hechos ocurridos o consumados.
- **Investigación:** Actividad humana enfocada a adquirir nuevos conocimientos y aplicarlos a la resolución de dudas o consultas.
- **Investigación forense:** Concentre sus esfuerzos de búsqueda principalmente en la impugnación de la CMO, o aquellos elementos que fueron utilizados, manipulados, modificados o fabricados durante la comisión del delito.

**Desarrollo:**

1. El cliente realiza el pedido de la investigación forense.
2. El analista registra el caso en el depósito correspondiente con las características necesarias para la identificación del mismo y correlación con otros.
3. El analista realiza el análisis de infraestructura de TI, en esta etapa se busca información útil con relación a las evidencias, para ello se analizan dispositivos físicos, aplicaciones de software y servicios.
4. El investigador forense realiza las acciones de campo que pueden incluir:
  - a. Entrevistas exploratorias con los responsables de sus acciones u omisiones.
  - b. Entrevistas con el infractor o responsable directo para conocer su nivel de culpabilidad, dolo, confesión y restitución.



5. El investigador realiza una investigación forense, que incluye el análisis de documentos (documentos reales vs falsos) y análisis de sistemas (manipulación, fabricación, registros) para armar el caso de acuerdo con el tiempo, es decir, extraer y presentar todos los elementos que permitan determinar cómo el caso desplegado.
6. El investigador elabora el reporte final, el cual debe contener como mínimo:
  - a. **Antecedentes:** Cómo surge el caso, quién lo denuncia, etc.
  - b. **Estrategia:** pasos y etapas que se prepararon para reunir pruebas.
  - c. **Entrevistas:** presentando los conocimientos adquiridos por cada persona según su nivel de responsabilidad o conocimiento.
  - d. **Evidencias:** todos los factores que fueron investigados, examinados o descubiertos que fueron concluyentes e indiscutibles que contribuyeron a la comisión del hecho.
  - e. **Hallazgos:** derivar de la evidencia obtenida a través de entrevistas y evidencia.
  - f. **Conclusiones:** Con base en el proceso de investigación desarrollado, se identifican todos los actores y factores que posibilitaron la comisión del hecho y la sustentación de los elementos de investigación.

*Nota: Cada uno de los pasos expuestos son extractos de la Guía Técnica de Ciberataques presentados por el Instituto Nacional de Ciberseguridad (INCIBE) y adaptados a las necesidades actuales del ESPE-CERT.*

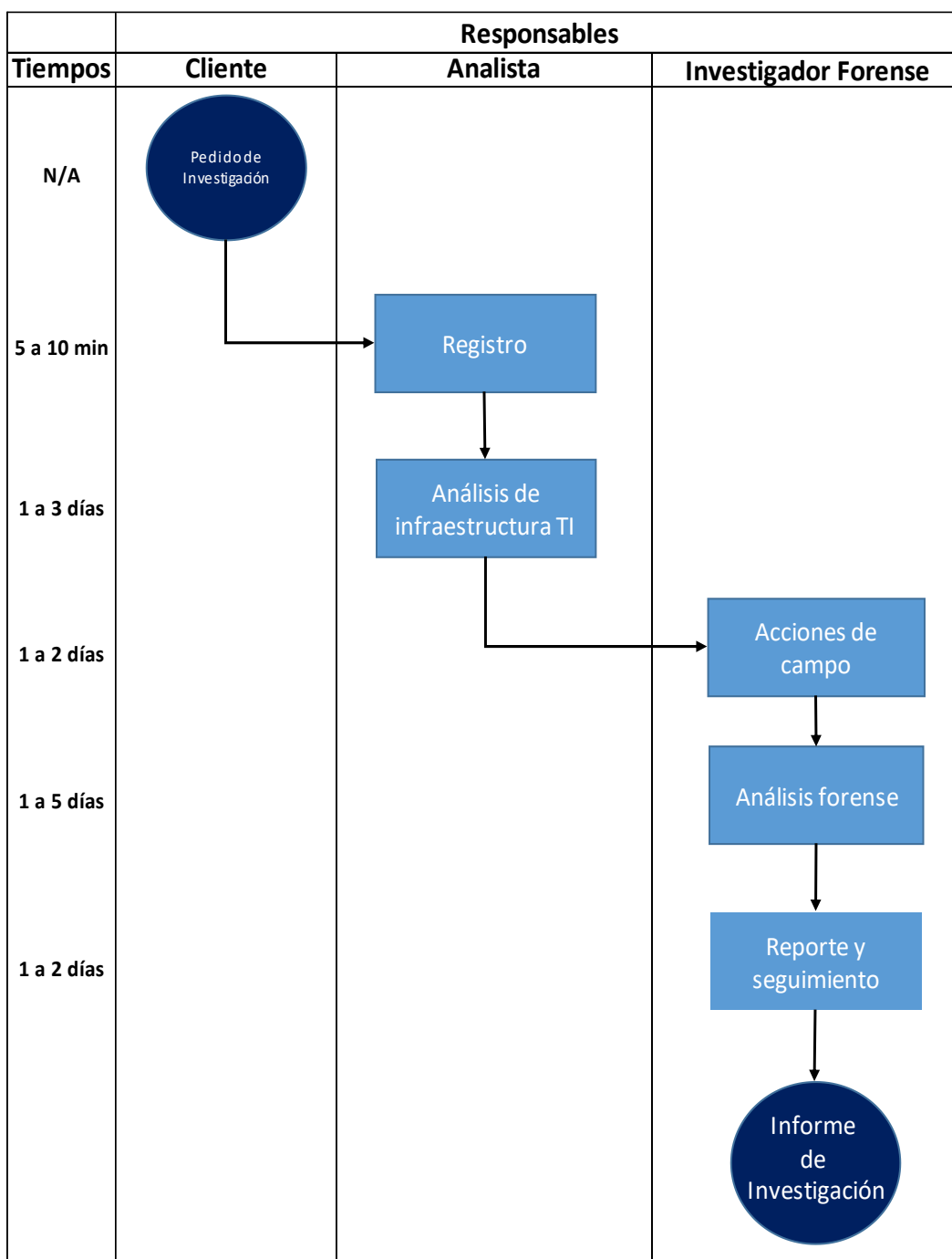
**Indicadores de desempeño:**

- Número de necesidades atendidas.
- Tiempo de respuesta y tiempo de espera.
- Número de fraudes descubiertos e investigados.

**Diagrama de flujo:** Diagrama De Flujo Espe-Cert, Código CERT-02.01.05

- Figura 22

*CERT-02.01.05 Investigación Forense*



**CERT-02.01.06 EVALUACIÓN TÉCNICA DE SEGURIDAD DE LA INFORMACIÓN.**

<b>Nro. de Procedimiento:</b> CERT02.01.06	<b>Nro. de Hoja:</b> 45
<b>Elaboró:</b> Juan Ruiz	<b>NTE INEN- ISO 9001</b>
<b>Título:</b> Evaluación Técnica de la Seguridad de la Información	

<b>Nro. de cambio al proceso</b>	<b>Elaboró</b>	<b>Revisó</b>	<b>Aprobó</b>	<b>Nro. de Páginas</b>
1	<b>Cargo:</b> Tesista <b>Nombre:</b> Maycol Pacha  <b>Firma:</b>   <b>Fecha:</b> 01-07-2022	<b>Cargo:</b> Tutor <b>Nombre:</b> Ing. Mario Ron MSc.  <b>Firma:</b>  <small>Firmado electrónicamente por:</small> <b>MARIO BERNABE RON</b>  <b>Fecha:</b> 03-08-2022	<b>Cargo:</b> Director de Proyecto <b>Nombre:</b> Dr. Walter Fuertes D.  <b>Firma:</b>  <small>Firmado electrónicamente por:</small> <b>WALTER MARCELO FUERTES DIAZ</b>  <b>Fecha:</b> 09-08-2022	6

**CONTROL DE COPIAS DEL PROCEDIMIENTO**

<b>DEPARTAMENTO</b>	<b>FIRMA DE RECIBIDO</b>	<b>FECHA</b>
<b>Nro. DE CAMBIO AL PROCESO</b>	<b>DESCRIPCIÓN DEL CAMBIO</b>	

**Objetivo:**

- Garantizar la protección de datos mediante la confidencialidad e integridad de la información, evitando acciones no autorizadas con ella, en particular, su uso, divulgación, distorsión, alteración, investigación y destrucción.

**Alcance:**

La evaluación técnica de seguridad de la información es un proceso de análisis de la madurez de las capacidades de ciberseguridad de la organización cliente que le proporcionará una comprensión de la eficacia de su defensa cibernética, ayudándole a obtener la confianza que necesita en su capacidad para gestionar los riesgos cibernéticos.

**Responsables:**

- Analista ESPE-CERT
- Operadores ESPE-CERT

**Base legal:**

RESOLUCIÓN No. 005-CCE-PLE-2021

“REGLAMENTO INTERNO DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN DE LA CORTE CONSTITUCIONAL”

- Que la Norma técnica UNE-EN ISO/IEC 27001 Sistemas de Gestión de Seguridad de la Información.
- **Artículo 8.- Responsabilidades de la delegada o delegado de Seguridad de la Información.** – La servidora o servidor público de la Gestión Interna de Infraestructura, Seguridades y Comunicaciones de la Dirección Nacional de Tecnologías de la Información y Comunicaciones, asumirá como delegada o delegado de Seguridad de la Información y, además de las funciones determinadas en su perfil de puesto, cumplirá

las siguientes responsabilidades dentro del seguimiento de la seguridad de la información:

- Verificar el cumplimiento de las políticas, procedimientos y controles de seguridad institucional establecidos;
- Informar al Comité de Seguridad de la Información sobre el estado de adopción de las políticas y estándares de Seguridad de la Información, así como de las advertencias que impidan su adopción.

### **Políticas:**

Para tener una adecuada gestión en seguridad de la información se debe tomar en cuenta:

- Asegurar que los datos y/o transacciones cumplan con los niveles de autorización correspondiente para su utilización y divulgación.
- Cada actividad o proceso de seguridad de la información debe tener una organización designada a cargo, y los detalles de esta organización deben estar documentados.
- Deben asegurarse de que nadie pueda acceder, modificar o usar actividades sin permiso o detección.

Para una adecuada administración de la seguridad de la información se debe tomar en cuenta:

- Obtener respaldos de Política de seguridad a través de miembros de la Universidad.
- Autorizar el manejo de la información confidencial a toda persona que lo requiera.

### **Definición:**

- **Confidencialidad de datos:** Evite la divulgación no autorizada de información confidencial.
- **Integridad:** Asegúrese de que la información no se cambie de forma no autorizada.

- **Accesibilidad:** Asegúrese de que la información esté disponible cuando los usuarios autorizados lo deseen.
- **Autenticidad:** capacidad de identificar exclusivamente al autor o fuente de información.

**Desarrollo:**

1. **Identificación de activos.** – Los operadores del ESPE-CERT deben conocer todos los activos de tecnología que forman parte de la infraestructura de la organización, como software y hardware. Con este levantamiento, es posible tener una idea de donde se encuentran las principales vulnerabilidades y cuáles son las actividades críticas que deben ser tratadas.
2. **Clasificación del tipo de activos.** – Los operadores del ESPE-CERT clasificarán los activos y se las hará de dos tipos, ya sean hardware o software y dependiendo del tipo se realizará la respectiva evaluación.
3. **Valoración de activos.** – La valoración de activos que hagan los operadores del ESPE-CERT nos servirá para determinar el estado actual en el que se encuentran los equipos de TI dentro y fuera de la organización.
4. **Evaluación de activos.** – Los activos serán evaluados por los operadores del ESPE en base a los parámetros establecidos en la valoración, y esto nos arrojará un informe con el rendimiento de cada activo evaluado.

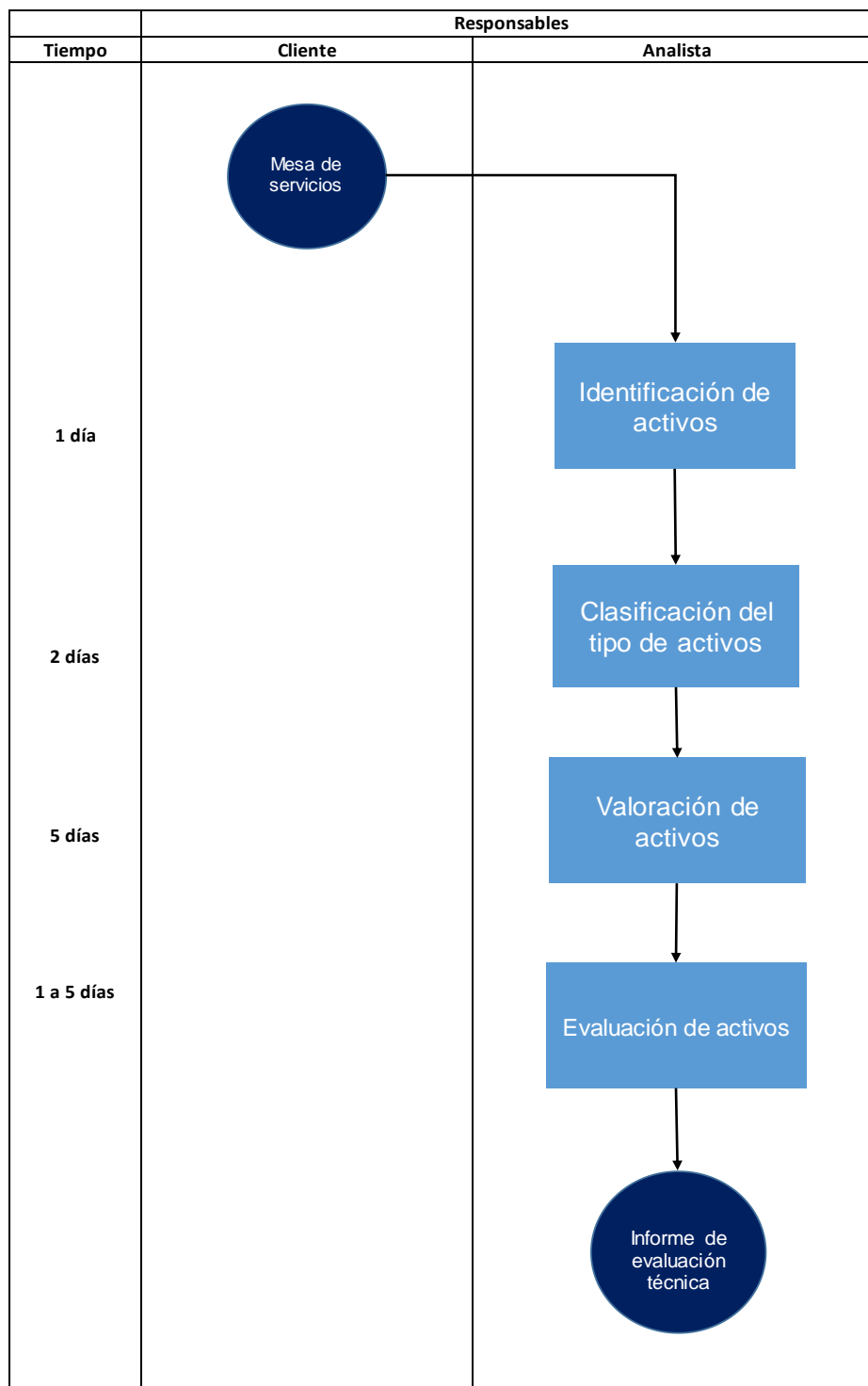
*Nota: Cada uno de los pasos expuestos son extractos de la (NIST SP 800-30) Guía para la gestión y el análisis de riesgo en seguridad de la información, adaptados a las necesidades actuales del ESPE-CERT.*

**Indicadores de desempeño:**

- Número de puertos de comunicación abiertos durante un período de tiempo.
- Frecuencia de accesos de terceros hacia el sitio web del ESPE-CERT.

**Diagrama de flujo:** Diagrama De Flujo Espe-Cert, Código CERT-02.01.06 Figura 23

***CERT-02.01.06 Evaluación técnica de la seguridad de la información***



**CERT-02.01.07 ASESORAMIENTO TÉCNICO Y CONSULTORÍA.**

<b>Nro. de Procedimiento:</b> CERT02.01.07	<b>Nro. de Hoja:</b> 51
<b>Elaboró:</b> Juan Ruiz	<b>NTE INEN- ISO 9001</b>
<b>Título:</b> Asesoramiento Técnico y Consultoría	

<b>Nro. de cambio al proceso</b>	<b>Elaboró</b> <b>Cargo:</b> Tesista <b>Nombre:</b> Juan Ruiz	<b>Revisó</b> <b>Cargo:</b> Tutor <b>Nombre:</b> Ing. Mario Ron MSc.	<b>Aprobó</b> <b>Cargo:</b> Director de Proyecto <b>Nombre:</b> Dr. Walter Fuertes D.	<b>Nro. de Páginas</b>
1	<b>Firma:</b> 	<b>Firma:</b>  <small>Firmado electrónicamente por:</small> <b>MARIO BERNABE RON</b>	<b>Firma:</b>  <small>Firmado electrónicamente por:</small> <b>WALTER MARCELO FUERTES DIAZ</b>	6
	<b>Fecha:</b> 03-07-2022	<b>Fecha:</b> 03-08-2022	<b>Fecha:</b> 09-08-2022	

**CONTROL DE COPIAS DEL PROCEDIMIENTO**

<b>DEPARTAMENTO</b>	<b>FIRMA DE RECIBIDO</b>	<b>FECHA</b>
<b>Nro. DE CAMBIO AL PROCESO</b>	<b>DESCRIPCIÓN DEL CAMBIO</b>	



**Objetivo:**

- Ofrecer a los clientes el máximo valor por los servicios de consultoría y asesoramiento implementando soluciones enfocadas en aumentar la productividad y competitividad dentro del ESPE-CERT aprovechando los recursos existentes.

**Alcance:**

Cuando su organización enfrenta algún problema relacionado con la administración, organización, políticas o procedimientos, los empresarios, directores de empresas y servidores públicos recurren a los servicios profesionales de empresas de asistencia técnica y consultoría.

**Responsables:**

- Analista ESPE-CERT
- Operadores ESPE-CERT

**Base legal:**

LEY DE CONSULTORÍA, CODIFICACION. Codificación 24, Registro Oficial 455 de 5 de noviembre del 2004.

- **Art. 3.-** La consultoría será ejercida por las siguientes personas naturales o jurídicas a quienes para efectos de este reglamento se las denominará indistintamente consultor o consultores:
  - Consultoras nacionales o asociaciones de ellas.
  - Universidades, escuelas técnicas y centros de transferencia tecnológica de universidades y escuelas técnicas que sean reconocidas por ley bajo la Ordenanza de Educación Superior.
  - Órganos y entidades del sector público facultados por ley para ejercer la consulta.

- **Art. 6.-** Los consultores individuales, nacionales o extranjeros, deben cumplir con los siguientes requisitos para poder realizar actividades de consultoría: a) Estar en posesión de un título profesional otorgado por una institución de educación superior ecuatoriana o extranjera, en cuyo caso deberá ser convalidado en el país de conformidad con la ley; y, b) Cumplir con las leyes pertinentes que rigen la actividad profesional. Los consultores extranjeros individuales que sean contratados por firmas consultoras extranjeras o nacionales deben demostrar su calibre.

#### **Políticas:**

- Las personas que sean seleccionadas para dar un asesoramiento o consultoría dentro del ESPE-CERT deben tener un título de tercer nivel.
- El analista siempre debe actuar con transparencia basándose en los valores que tiene el ESPE-CERT, respetando las opiniones de los clientes que necesitan estos servicios y teniendo especial cuidado en el manejo confidencial de las informaciones.
- El tiempo establecido para ofrecer asesoría en el ESPE-CERT está determinado por el tiempo disponible por el analista.

#### **Definición:**

- **Asesoría:** Trabajo realizado por un profesional o empresa para el desempeño de diversas funciones de asesoramiento, dirección y supervisión de la actividad económica de una persona física o jurídica que contrate sus servicios en el ámbito económico y jurídico.
- **Consultoría:** Servicio profesional que ofrece propuestas y recomendaciones concretas a los empresarios para abordar los problemas prácticos que están experimentando en sus organizaciones, depositando su total confianza en los profesionales internos o externos de la empresa.

**Desarrollo:**

1. **Planificación.** – Dado que las próximas fases estarán fuertemente influenciadas por el trabajo conceptual realizado y el tipo de relaciones que el consultor establezca con su cliente desde el inicio, el analista en esta fase sienta las bases de todo lo que vendrá después. En esta fase preliminar, también es posible que no se prepare una propuesta completa a satisfacción del cliente o que el cliente solicite propuestas de varios consultores, de los cuales se elegirá a uno para completar la tarea.
2. **Valoración de la problemática.** – El consultor tiene una amplia gama de opciones, especialmente si el cliente participa activamente en esta fase.
3. **Plan de acción.** – En la tercera fase, el objetivo de los analistas es encontrar la solución del problema. Incluye investigar varias soluciones, evaluar opciones, desarrollar un plan para implementar cambios y presentar ideas al cliente para que pueda elegir. El consultor tiene una amplia gama de opciones, especialmente si el cliente participa activamente en esta fase.
4. **Puesta en marcha.** – La cuarta fase de la consultoría, la del analista, sirve como prueba definitiva de la pertinencia y viabilidad de las sugerencias realizadas por el consultor en colaboración con el cliente. Los cambios propuestos comienzan a convertirse en una realidad.

*Nota: Cada uno de los pasos expuestos son extractos de la (ISO-27001) Guía para sistemas de gestión de la seguridad de la información, adaptados a las necesidades actuales del ESPE-CERT.*

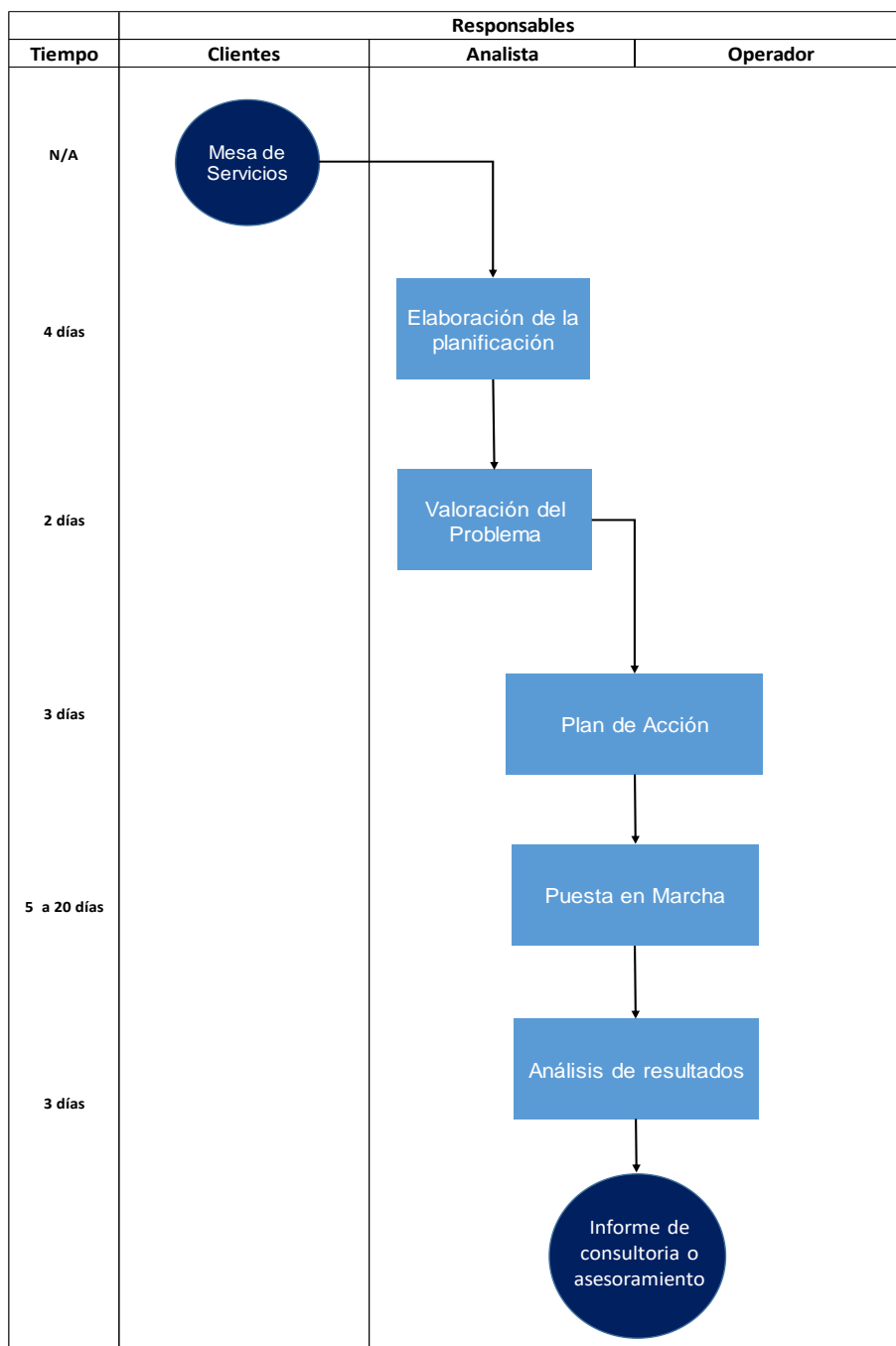
**Indicadores de desempeño**

- Número de problemas resueltos/ problemas no resueltos.
- Tiempo real en resolver el problema/ tiempo estimado en resolver el problema.

**Diagrama de flujo:** Diagrama De Flujo Espe-Cert, Código CERT-02.01.07

**Figura 24**

*CERT-02.01.07 Asesoramiento Técnico y Consultoría*



**CERT-02.01.08 ENTRENAMIENTO EN EL ÁMBITO DE LA CIBERSEGURIDAD Y  
CIBERDEFENSA**

<b>Nro. de Proceso:</b> CERT-02.01.08	<b>Nro. De Hoja:</b> 57
<b>Elaboró:</b> Maycol Pacha	<b>NTE INEN- ISO 9001</b>
<b>Título:</b> Entrenamiento en el Ámbito de Ciberseguridad y Ciberdefensa	

<b>Nro. de cambio al proceso</b>	<b>Elaboró</b>	<b>Revisó</b>	<b>Aprobó</b>	<b>Nro. de Páginas</b>
<b>1</b>	<b>Cargo:</b> Tesista <b>Nombre:</b> Maycol Pacha  <b>Firma:</b> 	<b>Cargo:</b> Tutor <b>Nombre:</b> Ing. Mario Ron MSc.  <b>Firma:</b>  Firmado electrónicamente por: <b>MARIO BERNABE RON</b>	<b>Cargo:</b> Director de Proyecto <b>Nombre:</b> Dr. Walter Fuertes D.  <b>Firma:</b>  Firmado electrónicamente por: <b>WALTER MARCELO FUERTES DIAZ</b>	<b>6</b>
	<b>Fecha:</b> 01-07-2022	<b>Fecha:</b> 03-08-2022	<b>Fecha:</b> 09-08-2022	

**CONTROL DE COPIAS DEL PROCESO**

<b>DEPARTAMENTO</b>	<b>FIRMA DE RECIBIDO</b>	<b>FECHA</b>
<b>Nro. DE CAMBIO AL PROCESO</b>	<b>DESCRIPCIÓN DEL CAMBIO</b>	

**Objetivo:**

- Coadyuvar en el desarrollo de habilidades o destrezas, por medio de capacitaciones en los ámbitos de ciberseguridad y ciberdefensa.

**Alcance:**

El proceso de capacitación en ciberseguridad es una parte fundamental del desarrollo del personal interno y externo al observatorio. El entrenamiento y capacitación permite dar a conocer a las personas buenas prácticas de seguridad para reducir la posibilidad de un ataque cibernético. Cuando se capacitan de manera efectiva, los beneficiarios constituyen una importante primera línea de defensa contra posibles incidentes de seguridad.

**Responsables:**

- Capacitador
- Director Ejecutivo
- Consejo Directivo

**Base legal:**

- **Norma técnica del subsistema de formación y capacitación:** Documento por el que se establecen los mecanismos normativos y técnicos que permitan a las Unidades Administradoras de Recursos Humanos organizar, ejecutar, evaluar y mejorar los programas de capacitación y fortalecimiento de capacidades tendientes a adquirir, desarrollar y potenciar los conocimientos, destrezas, habilidades y comportamientos necesarios para el desempeño de sus funciones, trabajos.
- Normas del National Institute of Standards and Technology (NIST) SP 800-61 (Referencial).

**Políticas:**

- Será responsabilidad del cliente de la institución solicitante, informar a los empleados sobre los cursos requeridos y/ o disponibles para su puesto. Será responsabilidad del empleado programar, asistir y aprobar los cursos requeridos de acuerdo con su puesto.
- De obligaciones y derechos de los participantes: Todos los miembros del personal de la Institución tienen derecho a participar en los programas de capacitación, siempre que el contenido se relacione con sus funciones y cuente con la aprobación previa de su superior inmediato.

Además, cumplir con las siguientes obligaciones:

- Llegar a tiempo a las sesiones de trabajo para las que han sido programadas.
- Revisar los materiales de consulta para desarrollar las evaluaciones de conocimientos que utilizará el capacitador.
- Respetar tanto a los instructores como a los demás participantes del curso de acuerdo con las normas básicas de urbanidad; mantener una actitud consistente hacia los estándares y opiniones de otras personas; abstenerse de comentarios que puedan afectar negativamente al lugar de trabajo o sus compañeros de trabajo. De obligación de los capacitadores: Una medida de la calidad de un instructor es qué tan bien se adhiere a los estándares internos, como:
  - Presentar el material didáctico relacionado con la materia por lo menos 15 días antes de la fecha prevista para el desarrollo del curso.

Cumplir a tiempo con el desarrollo de las capacitaciones y completar el tiempo del programa.

Establecer procedimientos de evaluación que se utilizarán en los participantes del curso para evaluar su nivel de participación.

Eliminar comportamientos o modos de expresión que afecten la sensibilidad de los participantes o pongan en duda su nivel de cultura, humanidad o moralidad.

**Definición:**

- **Ciberseguridad:** Protección de las actividades de procesamiento de información a través de la mitigación de amenazas a la información que es procesada, almacenada y transportada por los sistemas de información conectados.
- **Ciberdefensa:** Conjunto de acciones de tipo activo, pasivo, proactivo, preventivo y reactivo que se aplican para asegurar el uso propio del ciberespacio y negarlo al enemigo o a otras inteligencias en oposición.
- **Entrenamiento:** Conjunto de procedimientos y actividades realizadas para aumentar las habilidades o destrezas, desarrollando las cualidades de un individuo o grupo de personas de la forma más adecuada y en función de las circunstancias.
- **Capacitador:** Profesional que asume el papel de dirección y guía, o facilitador, dentro del proceso de entrenamiento.

**Desarrollo:**

1. **Diseño:** El Capacitador determinará el contenido y profundidad de la capacitación en base a la evaluación de necesidades, así como también, Los hallazgos de la evaluación brindarán la justificación requerida para que la alta gerencia proporcione los recursos necesarios para llevar a cabo el plan de trabajo. Posteriormente, se procede con la elaboración del plan, el cual debe contener entre otros los elementos que se presentan a continuación:
  - a. Alcance del plan.
  - b. Objetivos del plan.
  - c. Roles y Responsabilidades.



- d. Temas y frecuencias de cada sesión.
  - e. Evaluación y renovación del material.
2. El director ejecutivo aprueba el plan de entrenamiento, de acuerdo al análisis del diseño del mismo.
  3. **El capacitador desarrollará el material:** El desarrollo del material de capacitación, debe garantizar que las habilidades o destrezas que se requieren aprender y aplicar, sean contempladas en su totalidad. La idea fundamental del desarrollo de este material es que el grupo objetivo entienda que la seguridad de la información es una responsabilidad compartida y que todos son importantes en esa labor.
  4. Determinar el contenido del material del programa de capacitación antes de desarrollarlo es una de las consideraciones, una forma de lograr el cumplimiento de los objetivos planteados es obtener diverso material para el desarrollo del plan de diferentes fuentes confiables como se presentan a continuación:
    - a. Revistas científicas.
    - b. Conferencias de seguridad.
    - c. Asociaciones profesionales
    - d. Proveedores de seguridad de la información.
  5. El Consejo Ejecutivo aprueba el material, de acuerdo al análisis del desarrollo del mismo.
  6. **El capacitador dará inicio con la implementación del programa:** Para ello, el primer paso debe ser discutir el plan de formación con la alta dirección de la organización, ya que de esta forma se asegurará el apoyo para su ejecución y por tanto el pistoletazo de salida a la implementación. La implementación se llevará a cabo según lo establecido en la fase de diseño, es importante mencionar que, si por alguna situación se decide cambiar con dicha estructura, se deberá reestructurar el plan desde la etapa de diseño.

**7. El capacitador realizará la evaluación y seguimiento del plan de entrenamiento:** La fase final se enfoca en mantener y monitorear el plan. Los métodos efectivos de retroalimentación pueden incluir, por nombrar algunos, revisiones, grupos de interés y procedimientos de prueba de referencia. Sin saber primero cómo se está desempeñando dentro de la organización, no se puede mejorar un plan de capacitación; por lo tanto, es necesario buscar métodos que demuestren la efectividad del programa. Los métodos más comunes son:

- a. Evaluaciones o cuestionarios.
- b. Foros abiertos con usuarios que recibieron la capacitación.
- c. Entrevistas selectivas o entrevistas grupales

*Nota: Cada uno de los pasos expuestos son extractos de la (NIST 800-50) Guía de Creación de conciencia y capacitación sobre la seguridad de la tecnología de la información, ISO/IEC 27001 Seguridad de la Información e ISO/IEC 27002 Buenas prácticas para gestión de la seguridad de la información, adaptados a las necesidades actuales del ESPE-CERT.*

**Indicadores de desempeño:**

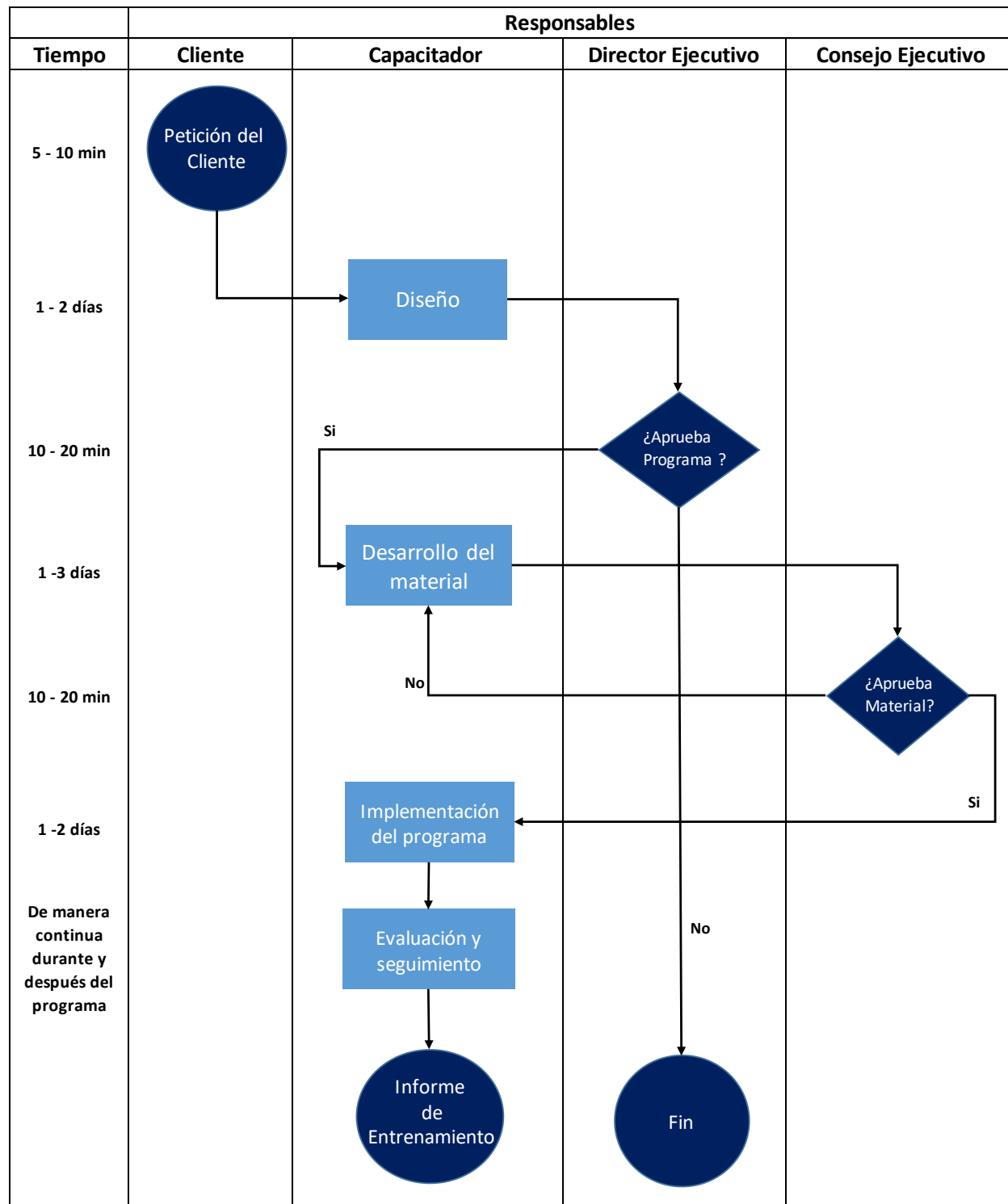
- Número de participantes que aprueban el entrenamiento.
- Número de participantes que asistieron al curso.
- Nivel de satisfacción del entrenamiento recibido.

**Diagrama de flujo:**

- Diagrama De Flujo Espe-Cert, Código CERT-02.01.08




**Figura 25**

*CERT-02.01.08 Entrenamiento en el Ámbito de Ciberseguridad y Ciberdefensa*



**CERT-02.02. GESTIÓN DE I+D+I**

<b>Nro. de Proceso:</b> CERT-02.02.	<b>Nro. Hoja:</b> 64
<b>Elaboró:</b> Juan Ruiz	<b>NTE INEN- ISO 9001</b>
<b>Título:</b> Gestión de I+D+I	

<b>Nro. de cambio al proceso</b>	<b>Elaboró</b> <b>Cargo:</b> Tesista <b>Nombre:</b> Juan Ruiz	<b>Revisó</b> <b>Cargo:</b> Tutor <b>Nombre:</b> Ing. Mario Ron MSc.	<b>Aprobó</b> <b>Cargo:</b> Director de Proyecto <b>Nombre:</b> Dr. Walter Fuertes D.	<b>Nro. de Páginas</b>
1	<b>Firma:</b> 	<b>Firma:</b>  <small>Firmado electrónicamente por:</small> <b>MARIO BERNABE RON</b>	<b>Firma:</b>  <small>Firmado electrónicamente por:</small> <b>WALTER MARCELO FUERTES DIAZ</b>	4
	<b>Fecha:</b> 03-07-2022	<b>Fecha:</b> 03-08-2022	<b>Fecha:</b> 09-08-2022	

**CONTROL DE COPIAS DEL PROCESO**

<b>DEPARTAMENTO</b>	<b>FIRMA DE RECIBIDO</b>	<b>FECHA</b>
---------------------	--------------------------	--------------

<b>Nro. DE CAMBIO AL PROCESO</b>	<b>DESCRIPCIÓN DEL CAMBIO</b>

**Objetivos:**

- Adquirir conocimientos nuevos para formular hipótesis, leyes y teorías nuevas acerca de la ciberseguridad.
- Realizar investigación aplicada para obtener objetos y artefactos para desarrollar prototipos.

**Alcance:**

La investigación y el desarrollo (I+D+i) es el proceso de investigación del conocimiento científico y técnico con el objetivo de desarrollar tecnologías para producir nuevos bienes, materiales o procedimientos.

**Responsables:**

- Director ejecutivo ESPE-CERT.
- Consejo directivo ESPE-CERT.
- Investigadores

**Base legal:**

- **El Art. 350** De acuerdo con la Constitución de la República del Ecuador, “El Sistema de Educación Superior tiene como finalidad la formación de académicos y profesionales con perspectiva científica y humanista; la investigación científica y tecnológica; la innovación, la promoción, el desarrollo y la difusión del conocimiento y la cultura; y la construcción de soluciones a los problemas nacionales en relación con las metas del régimen de desarrollo.”

LEY ORGANICA DE EDUCACION SUPERIOR, LOES:

- **Art. 6.1.- Deberes de las y los profesores e investigadores:** Son deberes de los educadores e investigadores de conformidad con la Constitución y esta Ley: a) realizar

actividades relacionadas con el conocimiento, con la investigación y conexas, de acuerdo con los estándares y lineamientos establecidos por los organismos reguladores del sistema y de sus propias instituciones; b) Ejercer tu derecho al catedrático respetando los derechos legales y constitucionales del sistema y de tus propias instituciones; c) promover los derechos consagrados en la Constitución y las leyes vigentes; d) Mantener un proceso continuo de capacitación y actualización para asegurar la aplicación del principio de calidad y la actualización permanente del plan de estudios; e) Participar periódicamente en los procesos de evaluación; y, f) cumplir con la normativa vigente así como con las políticas internas del colegio, si se trata de estudiantes de una institución de educación superior.

- **Art. 28.- Fuentes complementarias de ingresos y exoneraciones tributarias.** - Para aumentar su capacidad académica, las instituciones de educación superior pueden desarrollar fuentes de ingresos complementarias. Estas fuentes pueden incluir inversiones en investigación, otorgamiento de becas y ayudas financieras, formación de doctorados, programas de posgrado, inversiones en infraestructura, promoción y la difusión cultural, entre otros, dentro de los límites que determine la normativa aplicable.

#### **Políticas:**

- Fomentar un entorno propicio para el desarrollo de la investigación y fortalecer una comunidad capaz de realizar investigaciones científicas, innovar y desarrollar tecnologías.
- Se incentivará la creación de productos derivados de las investigaciones, su posterior difusión y transferencia a la sociedad.
- Se impulsará la obtención de recursos internos para la investigación al igual que los datos e información que necesite el investigador para su desarrollo.

**Definición:**

- **La investigación científica:** Proceso dinámico que se caracteriza por la rigidez y conduce a la adquisición de nuevos conocimientos. Su propósito es describir, aclarar, comprender, controlar y predecir eventos, fenómenos y comportamientos.
- **El artículo científico:** Texto de carácter académico que muestra el cumplimiento de normas específicas tanto en su estructura general como en su contenido.

**Desarrollo:**

1. Proceso CERT-02.02.01 Investigación, Desarrollo e implementación (I+D+i) de artefactos.
2. Proceso CERT-02.02.02 Análisis de sensibilización y elaboración de materiales.

**Indicadores de desempeño:**

- Indicadores basados en el procedimiento CERT-02.02.01 Investigación, Desarrollo e implementación (I+D+i) de artefactos.
- Indicadores basados en el procedimiento CERT-02.02.02 Análisis de sensibilización y elaboración de materiales.

**CERT-02.02.01 INVESTIGACIÓN, DESARROLLO E IMPLEMENTACIÓN (I+D+i) DE ARTEFACTOS**

<b>Nro. de Proceso:</b> CERT 02.02.01	<b>Nro. de Hoja:</b> 68
<b>Elaboró:</b> Juan Ruiz	<b>NTE INEN- ISO 9001</b>
<b>Título:</b> Investigación, Desarrollo e Implementación (I+D+i) de Artefactos	

<b>Nro. de cambio al proceso</b>	<b>Elaboró</b> <b>Cargo:</b> Tesista <b>Nombre:</b> Juan Ruiz	<b>Revisó</b> <b>Cargo:</b> Tutor <b>Nombre:</b> Ing. Mario Ron MSc.	<b>Aprobó</b> <b>Cargo:</b> Director de Proyecto <b>Nombre:</b> Dr. Walter Fuertes D.	<b>Nro. de Páginas</b>
1	<b>Firma:</b> 	<b>Firma:</b>  Firmado electrónicamente por: <b>MARIO BERNABE RON</b>	<b>Firma:</b>  Firmado electrónicamente por: <b>WALTER MARCELO FUERTES DIAZ</b>	7
	<b>Fecha:</b> 03-07-2022	<b>Fecha:</b> 03-08-2022	<b>Fecha:</b> 09-08-2022	

**CONTROL DE COPIAS DEL PROCEDIMIENTO**

<b>DEPARTAMENTO</b>	<b>FIRMA DE RECIBIDO</b>	<b>FECHA</b>
<b>Nro. DE CAMBIO AL PROCESO</b>	<b>DESCRIPCIÓN DEL CAMBIO</b>	



**Objetivo:**

- Desarrollar e incorporar nuevas tecnologías y procesos que permitan obtener nuevos productos, a través de la investigación científica, desarrollo tecnológico e innovación, para solucionar problemas de la sociedad en materia de ciberseguridad y ciberdefensa.

**Alcance:**

El procedimiento de Investigación, Desarrollo e Implementación I+D+i Incluye estructura organizativa, planificación de actividades, responsabilidades, prácticas, procedimientos, procesos y recursos para desarrollar, implementar, evaluar y mantener artefactos, prototipos, modelos, e investigación dentro de la institución.

**Responsables:**

- Consejo Directivo ESPE-CERT
- Director Ejecutivo ESPE-CERT
- Investigadores ESPE-CERT

**Base legal:**

- **Artículo 350** de la Constitución de la República del Ecuador, establece que "El sistema de educación superior tiene como finalidad la formación académica y profesional con una visión científica y humanista; la investigación científica y tecnológica; la innovación, promoción, desarrollo y difusión de los saberes y las culturas; la construcción de soluciones."
- **Artículo 388** de la Constitución de la República del Ecuador, prescribe que: "sujeto al presupuesto de la institución, asigna recursos para la investigación científica, el desarrollo tecnológico y la innovación. Una parte de estos recursos financiará proyectos

a través de concursos. Las organizaciones financiadas con fondos públicos están sujetas a contabilidad y supervisión estatal".

**Políticas:**

- El ESPE-CERT sujeto al presupuesto de la institución, asigna recursos para la investigación científica, el desarrollo tecnológico y la innovación.
- **Propiedad Intelectual:** Todos los productos generados en ESPE-CERT y/o proyectos (I+D+i), serán susceptibles de registro ante el Instituto Ecuatoriano de Propiedad Intelectual, respetando los porcentajes de participación establecidos en la normativa emitida para cada caso; el procedimiento de registro deberá ser iniciado por la entidad beneficiada en coordinación con los Directores de cada programa y/o proyecto o sus delegados, antes de proceder con la suscripción del Acta de finiquito referida.

**Definición:**

- **Investigación:** Actividad humana que se centra en adquirir nuevos conocimientos y aplicarlos a problemas o preguntas.
- **Desarrollo:** Toda actividad que trata de aprovechar los conocimientos aprendidos en la investigación para desarrollar nuevos productos o procesos productivos.
- **Innovación:** Consiste en crear algo nuevo, o mejorar lo que ya existe para hacerlo mejor.
- **Proyecto:** Actividades que buscan cumplir objetivos previamente identificados de investigación y desarrollo tecnológico durante un periodo de tiempo definido y respetando un presupuesto establecido.

**Desarrollo:**

1. **Designar responsables y funciones.** - El director ejecutivo asignará roles y responsabilidades, de modo que los miembros del equipo sepan quién está trabajando en tareas estrechamente relacionadas. Pueden revisar la lista de tareas pendientes, ver quién está trabajando en la tarea y pedir opiniones o preguntas según sea necesario.
2. **Objetivos del proyecto.** - El consejo directivo plantea los objetivos de la investigación la cual corresponde a la aspiración o el propósito que se desea alcanzar y en él se exponen de manera clara y precisa los resultados que se quieren obtener.
3. **Impacto e innovación del proyecto.** - Los investigadores (profesores, alumnos, miembros del ESPE-CERT) analizarán el impacto de un proyecto con sus efectos, positivos y negativos, intencionales o no, directos e indirectos,
4. **Planificación.** - Los investigadores (profesores, alumnos, miembros del ESPE-CERT) ayudarán estableciendo la prioridad de cada actividad y una mejor gestión del tiempo para un proyecto exitoso.
5. **Gestión de riesgos.** - Los investigadores (profesores, alumnos, miembros del ESPE-CERT) identificarán, analizarán y cuantifican pérdidas y efectos secundarios de los desastres, así como medidas preventivas, correctivas y reductivas correspondientes que deben emprenderse.
6. **Presupuesto y recursos.** - Los investigadores (profesores, alumnos, miembros del ESPE-CERT) se encargarán de estimar un presupuesto y los recursos necesarios que se necesiten y así poder completar un proyecto durante un período específico para obtener los resultados esperados.
7. **Desarrollo.** - Los investigadores (profesores, alumnos, miembros del ESPE-CERT) integrarán una serie de procedimientos y actividades utilizando una metodología

definida para lograr los objetivos de manera eficiente y eficaz.

- 8. Control de documentación.** - Los investigadores (profesores, alumnos, miembros del ESPE-CERT) realizarán el control de documento, que consiste en un sistema de gestión cuyo propósito es hacer cumplir los procesos y prácticas para la creación, revisión, modificación, emisión, distribución y accesibilidad de los documentos.
- 9. Seguimiento.** - Los investigadores (docentes, estudiantes, integrantes de la ESPE-CERT) monitorearán y evaluarán el avance e impacto del proyecto, establecerán la viabilidad de sus objetivos, identificarán y anticiparán los problemas, permitiendo a la comunidad y al agente de desarrollo tomar las medidas necesarias para evitarlos o abordarlos. El proceso de seguimiento y evaluación está vinculado a la toma de decisiones: permite a la comunidad redefinir sus objetivos y ajustar sus actividades según sea necesario.
- 10. Control de cambios.** - Los investigadores (profesores, alumnos, miembros del ESPE-CERT) realizarán un control de cambios que les permita llevar a cabo de una manera planificada, organizada y controlada con el fin de satisfacer las necesidades de los clientes.
- 11. Implementación.** - Los investigadores (profesores, alumnos, miembros del ESPE-CERT) realizarán la implementación la cual permite a la organización mejorar las conexiones, combinaciones e interacciones del sistema.
- 12. Análisis de resultados.** - Los investigadores (profesores, alumnos, miembros del ESPE-CERT) realizarán el análisis de resultados con el fin de procesar toda la información relacionada con el estudio, con el objetivo de presentarla de manera ordenada y comprensible, para finalmente, llegar a conclusiones basadas en datos.

*Nota: Cada uno de los pasos expuestos son extractos de la (ISO [9001/20000/27001])*

*Sistemas para gestión de la calidad, gestión del servicio y sistemas de gestión de seguridad de la información, adaptados a las necesidades actuales del ESPE-CERT.*

### **Indicadores de desempeño**

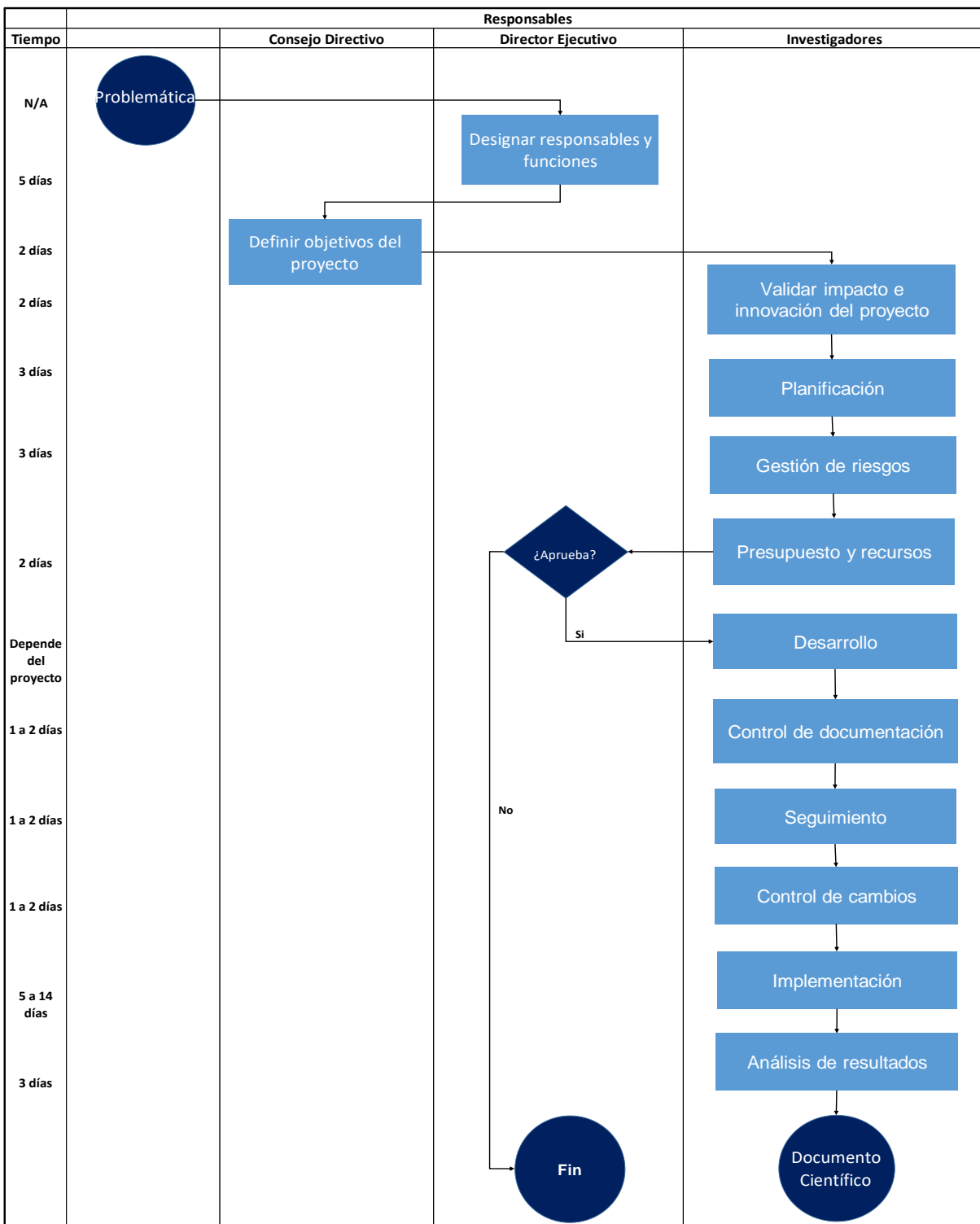
- Número de falsos positivos / falsos negativos
- Numero de activos críticos que requieren otro tipo de análisis.

### **Diagrama de flujo:**

- Diagrama De Flujo Espe-Cert, CERT-02.02.01

**Figura 26**

*CERT-02.02.1 Investigación, Desarrollo e Investigación (I+D+i) de Artefactos*



**CERT-02.02.02 SENSIBILIZACIÓN Y ELABORACIÓN DE MATERIALES**

<b>Nro. de Proceso:</b> CERT-02.02.02	<b>Nro. de Hoja:</b> 75
<b>Elaboró:</b> Maycol Pacha	<b>NTE INEN- ISO 9001</b>
<b>Título:</b> Procedimiento Sensibilización y Elaboración de materiales	

<b>Nro. de cambio al proceso</b>	<b>Elaboró</b>	<b>Revisó</b>	<b>Aprobó</b>	<b>Nro. de Páginas</b>
1	<b>Cargo:</b> Tesista <b>Nombre:</b> Maycol Pacha  <b>Firma:</b> 	<b>Cargo:</b> Tutor <b>Nombre:</b> Ing. Mario Ron MSc.  <b>Firma:</b>  <small>Firmado electrónicamente por:</small> <b>MARIO BERNABE RON</b>	<b>Cargo:</b> Director de Proyecto <b>Nombre:</b> Dr. Walter Fuertes D.  <b>Firma:</b>  <small>Firmado electrónicamente por:</small> <b>WALTER MARCELO FUERTES DIAZ</b>	6
	<b>Fecha:</b> 01-07-2022	<b>Fecha:</b> 03-08-2022	<b>Fecha:</b> 09-08-2022	

**CONTROL DE COPIAS DEL PROCESO**

<b>DEPARTAMENTO</b>	<b>FIRMA DE RECIBIDO</b>	<b>FECHA</b>
---------------------	--------------------------	--------------

<b>Nro. DE CAMBIO AL PROCESO</b>	<b>DESCRIPCIÓN DEL CAMBIO</b>
----------------------------------	-------------------------------

**Objetivo:**

- Sensibilizar al personal interno y externo para que asuman la responsabilidad personal de proteger la información de la organización, por medio del desarrollo y elaboración de materiales.

**Alcance:**

El proceso se refiere a la sensibilización y concientización del personal interno y externo de las instituciones clientes. El proceso intenta realizar un análisis de la situación actual del personal y desarrollar estrategias que permitan concientizar sobre temas de ciberseguridad a las personas.

**Responsables:**

- Analista ESPE-CERT.
- Operadores ESPE-CERT.
- Consejo Ejecutivo ESPE-CERT.
- Director Ejecutivo ESPE-CERT.

**Base legal:**

- **Norma técnica del subsistema de formación y capacitación:** Documento que establece los mecanismos normativos y técnicos de las Unidades de Gestión del Talento, organizar, ejecutar, evaluar y mejorar los programas de capacitación y desarrollo para adquirir, desarrollar y maximizar los conocimientos, destrezas, habilidades y actitudes relacionados con el trabajo.
- Normas del National Institute of Standards and Technology (NIST) SP 800-61 (Referencial).



**Políticas:**

- Será responsabilidad del cliente de la institución solicitante, informar a los empleados (as) sobre los programas de sensibilización de acuerdo a sus puestos de trabajo.
- De obligaciones y derechos de los participantes: Todos los colaboradores de la institución tienen derecho a participar en programas de sensibilización siempre y cuando el tema tenga relación con su función y cuente con la aprobación previa de su jefe inmediato superior.

Además, cumplir con las siguientes obligaciones:

- Revisar el material de consulta para desarrollar las evaluaciones de conocimientos que aplicará el operador.
- Respetar tanto a operadores como a compañeros, de acuerdo con las normas básicas de urbanidad.
- De obligación de los operadores: La calidad de los materiales realizados, también se mide por el nivel de cumplimiento de las normas internas, tales como:
  - Presentar el contenido del curso al menos 15 días antes de la fecha de inicio del curso.
  - Días de Sensibilización Puntual y Horario del Programa.
  - Establecer métodos de evaluación de los participantes del curso para medir su aprendizaje.
  - Evitar actitudes o expresiones que afecten la sensibilidad de los participantes o cuestionen su calidad cultural o humana.

**Definición:**

- **Sensibilización:** La sensibilización tiene por objetivo la concienciación de las personas y, para ello, se pueden realizar acciones de diversa índole: charlas, conferencias, exposiciones, talleres, formación de grupos, concursos, juegos, mercadillos, eventos deportivos o acciones directas en la calle.
- **Material didáctico:** El material didáctico consta de contenidos y recursos metodológicos y didácticos para ayudar al aprendizaje. Ayuda a los estudiantes a desarrollar habilidades y conocimientos.

**Desarrollo:**

1. **Análisis técnico de situación actual:** El Analista evalúa las necesidades actuales de la organización solicitante, donde se realizará un estudio de todos los incidentes informáticos que la empresa se ha visto expuesta, determinando de esta manera las áreas críticas dentro de la organización y posibles temas puntuales que abordará el plan de sensibilización. Por otro lado, si el cliente que representa la organización solicitante tiene claro el tema puntual de sensibilización, se emitirá el paso correspondiente al análisis técnico, en cuyo caso se evaluará la factibilidad para realizar la elaboración de materiales solicitados.
2. El Director Ejecutivo aprueba el plan de sensibilización, de acuerdo al análisis técnico de la situación actual.
3. **El Analista diseña el plan de sensibilización:** Una vez que se identifican todas las fallas organizacionales, se debe crear una estrategia que incluya, entre otras cosas, soluciones. que se detallan a continuación:
  - a. Alcance del plan.
  - b. Objetivos del plan.

- c. Roles y responsabilidades.
  - d. Temas para la elaboración de materiales.
  - e. Evaluación y renovación del material.
4. El Consejo Ejecutivo aprueba el diseño del plan de sensibilización, de acuerdo al análisis del mismo.
5. **El Analista desarrolla el material:** Una pregunta que surge al desarrollar el plan de concientización de una empresa es: ¿Qué requiere conocer el personal de la organización en materia de seguridad de la información? Se pueden incluir argumentos extensos en un plan de sensibilización, por tal motivo se debe dar prioridad a los temas definidos en la etapa de diseño. Por otro lado, la norma NIST 800-50 “Creación de un programa de concientización sobre seguridad en TI”, recomienda a los Equipos de Respuesta, la creación de planes de sensibilización que aborden los temas que se detallan a continuación:
- a. Uso y administración de contraseñas.
  - b. Protección contra virus, troyanos y otros códigos maliciosos.
  - c. Uso de la web: permitido vs prohibido.
  - d. Ingeniería social.
6. **El Analista dará inicio con la puesta en marcha del programa de sensibilización:** Este paso dirige los roles de comunicación y sensibilización efectiva. Como primer paso, consulte con la alta dirección de la organización para asegurar el apoyo necesario para la implementación. A continuación, Se describen algunas técnicas para difundir o comunicar información; el método elegido depende de los recursos y la tecnología de la organización, algunos ejemplos son:
- a. Posters con mensajes o checklist sobre que debe y que no debe hacerse.
  - b. Screensavers con mensajes de sensibilización.

- c. Boletines vía email.
  - d. Eventos relacionados con seguridad, concursos etc.
7. El Analista realizará la evaluación y seguimiento del plan de sensibilización: Un plan de sensibilización, No se puede mejorar sin saber cómo se está desempeñando la organización, por lo que es necesario encontrar indicadores de efectividad del programa. Los métodos comunes para evaluar las campañas de concientización incluyen:
- a. Evaluaciones o cuestionarios.
  - b. Foros Abiertos con usuarios que recibieron la sensibilización.
  - c. Entrevistas selectivas o entrevistas grupales.
  - d. Uso de “benchmarking”, que indica comparar el método que se ha implementado con el de otras empresas similares, para así mejorar el modelo implementado.

*Nota: Cada uno de los pasos expuestos son extractos de la (NIST 800-50) Guía de Creación de conciencia y capacitación sobre la seguridad de la tecnología de la información, ISO/IEC 27001 Seguridad de la Información e ISO/IEC 27002 Buenas prácticas para gestión de la seguridad de la información, adaptados a las necesidades actuales del ESPE-CERT.*

**Indicadores de desempeño:**

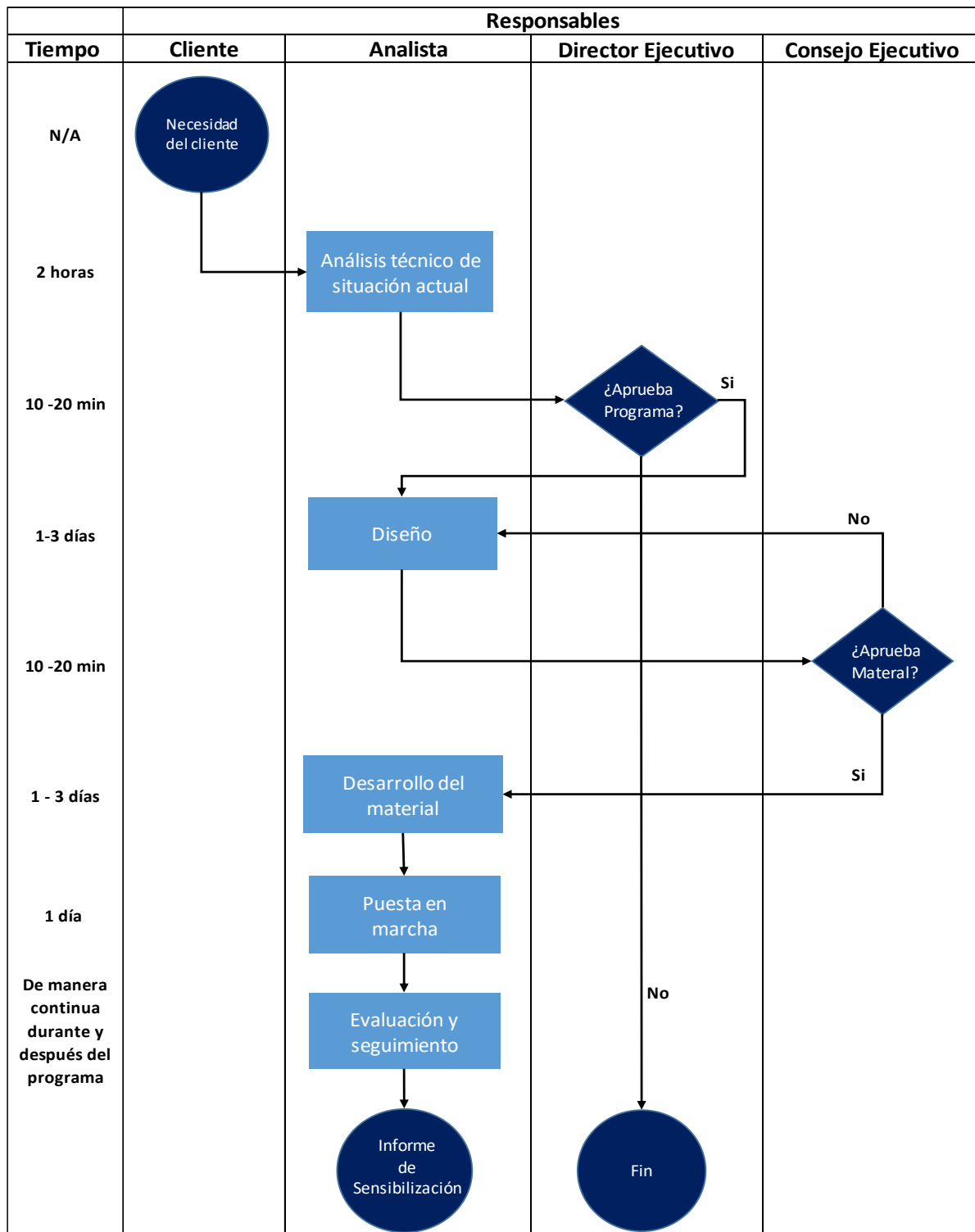
- Número de participantes que adquieren el material de sensibilización.
- Número de incidentes reportados en la organización.

**Diagramas de flujo:**

- Diagrama De Flujo Espe-Cert, Código CERT-02.02.02

**Figura 27**

*CERT-02.02.02 Procedimiento Sensibilización y Elaboración de materiales*



### ***Disposiciones generales***

**Primera 1** El presente manual tiene por objeto establecer una cultura aplicable a los servicios que oferta el ESPE-CERT.

**Segunda 2** Los procesos generadores de valor son aquellos definidos como operativos y fundamento de los servicios del ESPE-CERT.

**Tercera 3** Las definiciones de los términos técnicos son las establecidas en las referencias normativas.

### ***Disposiciones transitorias***

**Primera:** El presente manual de procesos operativos entrará en vigencia a partir de su aprobación por parte del organismo normativo o de la Universidad de las Fuerzas Armadas.

**Segunda:** Al expedir una nueva versión del manual de procesos operativos, quedará sin efecto la versión anterior y entrará en vigencia el nuevo manual el cual será aprobado por parte del organismo normativo o de la Universidad de las Fuerzas Armadas.

**Tercera:** Las autoridades del ESPE-CERT, designaran las personas encargadas de la revisión del manual a partir de su entrega completa, así como también de sus actualizaciones.

**Cuarta:** El Director del Proyecto se encargará de la aprobación del manual a partir de su entrega completa, así como también de sus actualizaciones.

### ***Aprobación y legalización***

La aprobación y legalización del Manual de Procesos Operativos, después de efectuar todas las correcciones y sugerencias de mejora en su desarrollo, la realiza el Director del Proyecto Dr. Walter Marcelo Fuertes Diaz , el día martes 09 de agosto del 2022, para su constancia se adjunta las firmas que respaldan el debido proceso.

**ELABORA:**



---

Maycol Jonathan Pacha Morales

**ELABORA:**



---

Ruiz Vega Juan José

**REVISAR:**



Firmado electrónicamente por:  
**MARIO  
BERNABE RON**

---

Ing. Mario B. Ron Egas MSc

**APRUEBA**



Firmado electrónicamente por:  
**WALTER MARCELO  
FUERTES DIAZ**

---

Dr. Walter Marcelo Fuertes Diaz  
Director del Proyecto

## Capítulo V

### Conclusiones y recomendaciones

#### Conclusiones

- Se desarrolló un manual de procesos operativos para el CERT académico de la Universidad de las Fuerzas Armadas “ESPE”, utilizando estándares a nivel internacional mediante una racionalización de procesos, para contribuir a la eficacia y eficiencia de la gestión de operaciones del CERT coadyuvando en la mejora de los servicios ofertados a la comunidad universitaria.
- La identificación y revisión sistemática de estudios relacionados con la operación de un equipo de respuesta ante incidentes informáticos, buenas prácticas y estándares a nivel internacional, permitió formar una base de diseño adecuada del manual de procesos del ESPE-CERT.
- La selección de los procesos operativos de los servicios proactivos y reactivos ofertados por el ESPE-CERTS, así como su racionalización, permitió la elaboración de las normas de procedimiento de manera técnica y sistemática, incluyendo el diseño de los diagramas de flujo de acuerdo a las actividades identificadas, en concordancia con buenas prácticas y normativa internacional relacionada.
- La rúbrica de evaluación y la matriz de priorización de parámetros diseñadas para evaluar el trabajo realizado, resultó muy objetiva para el uso de los evaluadores y los diseñadores del manual, quienes utilizaron los resultados de este proceso de evaluación para realizar mejoras al documento elaborado.



## Recomendaciones

- Realizar la implementación de los procesos y procedimientos identificados de acuerdo a los servicios ofertados por el ESPE-CERT, en concordancia con los cargos definidos y las responsabilidades establecidas en el manual elaborado.
- Utilizar el presente trabajo de titulación para conseguir la certificación del ESPE - CERT por parte del Forum of Incident Response and Security Teams (FIRST), como se contempla entre los objetivos del proyecto de investigación relacionado.
- Emplear la rúbrica elaborada en evaluaciones posteriores y cíclicas de los procesos de mejora del manual elaborados y por consiguiente de la mejora u optimización de los procesos operativos del ESPE-CERT.
- Como trabajo futuro es necesario también elaborar las normas de procedimiento de los procesos de dirección estratégica y de apoyo del ESPE-CERT.

## Bibliografía

9001. (26 de Agosto de 2016). *Caso de Uso: automatizar la gestión por procesos según ISO 9001*. Obtenido de ISOTools EXCELLENCE: <https://www.isotools.org/2016/08/26/caso-de-uso-automatizar-la-gestion-por-procesos-segun-iso-9001/>
- Academy Cisco Networking*. (2020). Obtenido de Introducción a la Ciberseguridad: [www.netacad.com/es/courses/cybersecurity/introduction-cybersecurity](http://www.netacad.com/es/courses/cybersecurity/introduction-cybersecurity)
- Agudelo, L. F. (2007). *Gestión por Procesos*. Medellín: ICONTEC 2008.
- Ahmad, R. A., & Hashim, M. S. (2011). *The Organisation of Islamic Conference — Computer Emergency Response Team(OIC-CERT): Answering cross border cooperation*. 2011 Second Worldwide Cybersecurity Summit (WCS), 1-5.
- Alvarado, J. (2020). ANÁLISIS DE ATAQUES CIBERNÉTICOS HACIA EL ECUADOR. *ITSJBA*, 10.
- Antonucci, I. (10 de Marzo de 2021). *Mejora Continua: ¿Qué es y cómo se implementa? | Método Kaizen*. Obtenido de Atlas Consultora: <https://www.atlasconsultora.com/mejora-continua/>
- Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (Agosto de 2012). *Guía de manejo de incidentes de seguridad informática (SP 800-61 Rev. 2)*. Obtenido de CENTRO DE RECURSOS DE SEGURIDAD INFORMÁTICA NIST: <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>
- Dentzel, Z. (2013). *El impacto de internet en la vida diaria*. Obtenido de OpenMind BBVA: <https://www.bbvaopenmind.com/articulos/el-impacto-de-internet-en-la-vida-diaria/>
- Endicott-Popovsky, B., & Frincke, D. (2005). *Adding the fourth "R" [CERT's model for computer security strategies]*. Proceedings from the Fifth Annual IEEE SMC Information Assurance Workshop, 2004.

- González, S. A. (2018). *Reputación corporativa. Estudio del concepto y las metodologías para su medición*. Obtenido de <https://eprints.ucm.es/id/eprint/47772/1/T39956.pdf>
- Haller, J., Merrell, S. A., Butkovic, M. J., & Willke, B. J. (Abril de 2011). *Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability, Version 2.0*. Obtenido de Carnegie Mellon University: <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9999>
- Hurtado, F. (27 de Febrero de 2018). *¿Qué es y cómo hacer un manual de procedimientos?* Obtenido de Softgrade: <https://softgrade.mx/manual-de-procedimientos/>
- INCIBE. (2020). *GUÍA NACIONAL DE NOTIFICACIÓN Y GESTIÓN DE CIBERINCIDENTES*. ESPAÑA. Obtenido de [https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia\\_nacional\\_notificacion\\_gestion\\_ciberincidentes.pdf](https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf)
- INCIBE-CERT. (1 de Octubre de 2018). *El Centro de Respuesta a Incidentes de Seguridad para ciudadanos y empresas pasa a denominarse INCIBE-CERT*. Obtenido de INCIBE: <https://www.incibe.es/sala-prensa/notas-prensa/incibe-cert-es-el-centro-respuesta-incidentes-seguridad-ciudadanos-y-empresas>
- Ioannou, M., Stavrou, E., & Bada, M. (2019). *Cybersecurity Culture in Computer Security Incident Response Teams: Investigating difficulties in communication and coordination*. International Conference on Cyber Security and Protection of Digital Services (Cyber Security), 1-4.
- ITIL. (2019). *Gestión Operativa y su incidencia en la calidad de Atención al Cliente*. Obtenido de [https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/4248/Julio\\_Leon\\_Trabajo\\_de\\_Investigacion\\_2017.pdf?sequence=1&isAllowed=y](https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/4248/Julio_Leon_Trabajo_de_Investigacion_2017.pdf?sequence=1&isAllowed=y)
- Kijewski, P., & Kozakiewicz, A. (2011). *Security Research at NASK: Supporting the Operational Needs of a CERT Team and More*. 2011 First SysSec Workshop, 96-99.

- Kitchenham, B., Budgen, D., & Brereton, P. (2015). *Evidence-Based Software Engineering and Systematic Reviews*. (1st Edition ed.). Chapman and Hall/CRC.
- López, P. L. (2011). *Cómo hacer el Manual de Calidad según la nueva ISO 9001:2008* (Primera ed.). FC Editorial.
- Marcasco. (25 de Noviembre de 2021). *6 formas de agilizar los procesos empresariales y los flujos de trabajo*. Obtenido de Historiadelaempresa.com.:  
<https://historiadelaempresa.com/racionalizar-los-procesos-y-los-flujos-de-trabajo>
- Mendoza, M. Á. (18 de Mayo de 2015). *Welivesecurity.com*. Obtenido de  
<https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/>
- Mooi, R. D., & Botha, R. A. (2016). *A Management Model for Building a Computer Security Incident Response Capability*. SAIEE Africa Research Journal .
- Mooi, R., & Botha, R. A. (2016). *Context for the SA NREN Computer Security Incident Response Team*. 2016 IST-Africa Week Conference 1-9.
- Mosquera, J. (2007). *RACIONALIZACION DE LOS PROCESOS Y PROCEDIMIENTOS DE LAS AREAS OPERATIVAS DE LA UNIDAD ESTRATEGICA DEL NEGOCIO DE TELECOMUNICACIONES DE EMCALI*. Edu.Co. . Santiago de Cali.
- Moyle, E. (2 de Julio de 2019). *CERT vs. CSIRT vs. SOC: ¿Cuál es la diferencia?* Obtenido de ComputerWeekly.es; TechTarget.: <https://www.computerweekly.com/es/consejo/CERT-vs-CSIRT-vs-SOC-Cual-es-la-diferencia>
- Organización de los Estados Americanos. (Abril de 2016). *Buenas prácticas para establecer un CSIRT nacional*. Obtenido de [www.oas.org/cyber/](http://www.oas.org/cyber/)
- Paz, A. (30 de Mayo de 2017). *BPM Gestión de Procesos de Negocio*. Obtenido de Título del sitio: <https://andrepazalejandro.wordpress.com/2017/05/30/bpm-gestion-de-procesos-de-negocio/>

- Pazmiño, C., Serrano, A., & González, M. (2020). Las Tics como herramienta para la gestión de riesgos. *Mundo de la investigación y el conocimiento*. Obtenido de [https://doi.org/10.26820/recimundo/4.\(1\).esp.marzo.2020.173-181](https://doi.org/10.26820/recimundo/4.(1).esp.marzo.2020.173-181)
- Pérez, J. (2010). *Gestión por Procesos* (Cuarta ed.). Esic Editorial.
- Petersen, K., Feldt, R., Mujtaba, S., & Michael, M. (2008). Systematic Mapping Studies in Software Engineering. *12th International Conference on Evaluation and Assessment in Software Engineering*. Obtenido de [https://www.researchgate.net/publication/228350426\\_Systematic\\_Mapping\\_Studies\\_in\\_Software\\_Engineering](https://www.researchgate.net/publication/228350426_Systematic_Mapping_Studies_in_Software_Engineering)
- Rocha, C. (5 de Septiembre de 2011). La Seguridad Informática. *Revista Ciencia Unem*, 26-33.
- Romero, J. A. (15 de Septiembre de 2020). *Diferencia entre proceso y procedimiento en ISO 9001 - ISO 9001:2015*. Obtenido de Cambios Clave NUEVA ISO 9001:2015 : <https://www.nueva-iso-9001-2015.com/2020/09/diferencia-entre-proceso-y-procedimiento-segun-iso-9001/>
- Ron Egas, M., Vásques Cañas, R., Lanfranco, M., Macia, N., & Diaz, J. (2017). *Practical Guide To Implement An Academic Computing Security Incident Response Team (Academic CSIRT)*.
- Sejzer, R. (12 de Abril de 2017). *Implementación de Six Sigma con DMAIC por Raúl Sejzer*. Obtenido de QUALITY ROAD.: <https://qualityway.wordpress.com/2017/04/12/implementacion-de-six-sigma-con-dmaic-por-raul-sejzer/>
- Steinke, J., Bolunmez, B., Fletcher, L., Wang, V., Tomassetti, A. J., Repchick, K. M., . . . Tetrick, L. E. (2015). *Improving Cybersecurity Incident Response Team Effectiveness Using Teams-Based Research*. *IEEE Security & Privacy*, 20-29.

Toro, R. (5 de Mayo de 2015). *¿Cómo es un mapa de procesos basado en la norma ISO 9001*

*2015?* Obtenido de Cambios clave NUEVA ISO 9001:2015: <https://www.nueva-iso-9001-2015.com/2016/05/como-es-un-mapa-procesos-basado-norma-iso-9001-2015/>

UIT, C. (2018). *GUÍA PARA LA ELABORACIÓN DE UNA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD, PARTICIPACIÓN ESTRATÉGICA EN LA CIBERSEGURIDAD.*

Ginebra: CC BY 3.0 IGO.

Valladares, P., Fuertes, W., Tapia, F., Toulkeridis, T., & Pérez, E. (2017). *Dimensional data*

*model for early alerts of malicious activities in a CSIRT.* 2017 International Symposium

on Performance Evaluation of Computer and Telecommunication Systems (SPECTS), 1-

8.