



ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

**TRABAJO DE TITULACIÓN, PREVIO A LA OBTENCIÓN DEL TÍTULO
DE INGENIERO EN SISTEMAS E INFORMÁTICA**

**TEMA: “MODELO DE ANÁLISIS Y SELECCIÓN DE
HERRAMIENTAS DE CIBERSEGURIDAD PARA UN CSIRT
ACADÉMICO: CASO CSIRT-ESPE”**

**AUTORES: SALINAS CALLEJAS, EDWIN FERNANDO
MARIN ALQUINGA, EDISON DANIEL**

DIRECTOR: ING. RON EGAS, MARIO BERNABE

SANGOLQUÍ

2019

CERTIFICADO DEL DIRECTOR



DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN
CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

CERTIFICADO DEL DIRECTOR

Certifico que el trabajo de titulación, "**MODELO DE ANÁLISIS Y SELECCIÓN DE HERRAMIENTAS DE CIBERSEGURIDAD PARA UN CSIRT ACADÉMICO: CASO CSIRT-ESPE.**" fue realizado por los señores **SALINAS CALLEJAS EDWIN FERNANDO** y **MARIN ALQUINGA EDISON DANIEL**, el mismo que ha sido revisado en su totalidad, analizado por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Sangolquí, 8 de Julio del 2019

Ing. Mario Bernabe Ron Egas
C.C.: 1704229747
DIRECTOR

AUTORÍA DE RESPONSABILIDAD




DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN
CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

AUTORÍA DE RESPONSABILIDAD

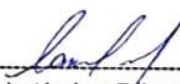
Nosotros, **SALINAS CALLEJAS EDWIN FERNANDO** y **MARIN ALQUINGA EDISON DANIEL**, declaramos que el contenido, ideas y criterios del trabajo de titulación: “**MODELO DE ANÁLISIS Y SELECCIÓN DE HERRAMIENTAS DE CIBERSEGURIDAD PARA UN CSIRT ACADÉMICO: CASO CSIRT-ESPE.**” es de nuestra autoría y responsabilidad, cumpliendo con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Consecuentemente el contenido de la investigación mencionada es veraz.

Sangolquí, 8 de Julio del 2019



Salinas Callejas Edwin Fernando
C.C.: 1716511868



Marin Alquina Edison Daniel
C.C.: 0503910903

AUTORIZACIÓN



DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN
CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

AUTORIZACIÓN

Nosotros, **SALINAS CALLEJAS EDWIN FERNANDO** y **MARIN ALQUINGA EDISON DANIEL**, autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **“MODELO DE ANÁLISIS Y SELECCIÓN DE HERRAMIENTAS DE CIBERSEGURIDAD PARA UN CSIRT ACADÉMICO: CASO CSIRT-ESPE.”** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de nuestra responsabilidad.

Sangolquí, 8 de Julio del 2019

Salinas Callejas Edwin Fernando
C.C.: 1716511868

Marin Alquina Edison Daniel
C.C.: 0503910903

DEDICATORIA

El presente trabajo lleva una dedicatoria muy especial a Dios, a nuestros padres y familiares que nos aportaron con motivación y esfuerzo a cumplir nuestras metas.

AGRADECIMIENTOS

Un agradecimiento a Dios por bendecirnos en cumplir nuestros sueños.

Nuestros padres y familiares por el apoyo y guía incondicional en nuestra vida académica.

Nuestro director de tesis el Ing. Mario Ron, por guiarnos en nuestro proyecto de grado.

Nuestros compañeros de la Universidad de las Fuerzas Armadas Espe, por brindarnos amistad en las aulas de nuestra institución.

A la Universidad de las Fuerzas Armadas Espe por formarnos como profesionales con sus docentes y personal, en valores y conocimientos, para hacer del Ecuador un país de desarrollo y tecnología.

ÍNDICE DE CONTENIDOS

CERTIFICADO DEL DIRECTOR.....	i
AUTORÍA DE RESPONSABILIDAD	ii
AUTORIZACIÓN	iii
DEDICATORIA.....	iv
AGRADECIMIENTOS	v
ÍNDICE DE CONTENIDOS	vi
ÍNDICE DE TABLAS	ix
ÍNDICE DE FIGURAS	xii
ABSTRACT	xiv
1. CAPITULO I	1
1.1. Antecedentes	2
1.2. Problemática	3
1.2.1. Contextualización del Problema	3
1.3. Formulación del Problema	4
1.4. Justificación	4
1.5. Objetivos	5
1.5.1 Objetivo General.....	5
1.5.2 Objetivos Específicos	6
1.6 Alcance.....	6
1.7 Marco Legal del Proyecto de Investigación.....	7
2. CAPITULO II	12
2.1. Introducción	12
2.2. La Ciberseguridad	14
2.2.1 Importancia de la Información en las Organizaciones.....	14
2.3. Principios de la seguridad de la información	15
2.4. Equipo de Respuesta ante Incidentes (CSIRT)	19
2.4.1. Definición.....	19
2.4.2. Funciones y Servicios de un CSIRT	19
2.4.2.1. Servicios Reactivos	20

2.4.2.2.	Servicios Proactivos	20
2.4.2.3.	Servicios de gestión de la calidad.....	21
2.4.3.	Clasificación de los CSIRT	21
2.5.	CSIRT Académico	22
2.6.	Herramientas de Ciberseguridad	25
2.6.1.	Herramientas de Monitoreo	25
2.6.2.	Herramientas de Evaluación de Seguridad.....	25
2.7.	Modelos de Calidad de Software	28
2.7.1.	Tipos de Modelos de Calidad de Software.....	29
2.8.	Método Empírico Analítico	29
2.8.1.	Método Empírico Analítico – Experimental	30
2.8.2.	Método Delphi	31
2.8.2.1.	Método Delphi - Juicio de Expertos	31
2.9.	Calidad del Producto Software	32
2.9.1.	Estándar General de Sistema de Gestión de Calidad.....	33
2.9.1.1.	ISO/IEC 9000: 9001	33
2.9.1.2.	Aseguramiento de la Calidad del Software	34
2.9.2.2.	ISO/IEC 9126	35
2.9.2.3.	ISO/IEC 14598 Métodos de Valoración y Evaluación de la Calidad del Producto Software	56
2.9.3.	Normas de Anticorrupción y Ética.....	59
2.10.	Priorización de Selección de Criterios de Evaluación	61
2.10.1.	Matriz de Priorización de Holmes o Matriz de Impacto	61
3.	CAPITULO III	63
3.1.	Introducción.....	63
3.2.	Definición de los Procesos de Evaluación	64
3.3.	Justificación la Adquisición (ISO 37001).....	66
3.4.	Proceso de Evaluación	67
3.4.1	Establecimiento de los requerimientos	69
3.4.2	Describir el Producto Software a Evaluar	74
3.4.3	Especificación de la evaluación	77

3.3.4.	Diseño de la Evaluación	92
3.3.5.	Ejecución de la Evaluación	108
3.3.6.	Conclusión de la Evaluación.....	108
4.	CAPITULO IV	110
4.1.	Introducción	110
4.2.	Justificación de la Adquisición	110
4.3.	Proceso de Evaluación	112
4.3.1	Establecimiento de Requerimientos por CSIRT-ESPE	112
4.3.2.	Descripción del Producto Software	113
4.3.3.	Ejecución de la Evaluación	117
4.4	Análisis de Resultados e Informe Final	158
4.5	Validación de Resultados	163
5.	CAPITULO V	164
5.1	Conclusiones	164
5.2	Recomendaciones.....	165
5.3	Bibliografía	166

ÍNDICE DE TABLAS

Tabla 1. <i>Niveles de Resultados Obtenidos en la Evaluación</i>	29
Tabla 2. <i>ISO 9126-2 Tabla de Métricas de Evaluación del Producto Software</i>	45
Tabla 3. <i>ISO/IEC 9126-2 Métricas Externas</i>	47
Tabla 4. <i>ISO/IEC 9126-3 Métricas Internas</i>	54
Tabla 5. <i>ISO/IEC 9126-4 Métricas de Calidad de Uso</i>	56
Tabla 6. <i>Matriz de Priorización de Holmes o Matriz de Impacto</i>	62
Tabla 7. <i>Características de calidad para aplicaciones de Ciberseguridad</i>	77
Tabla 8. <i>Matriz de Priorización de Características de Herramientas de Ciberseguridad y Coeficiente de Ponderación</i>	85
Tabla 9. <i>Propuesta de Métricas de Evaluación y Coeficiente de Ponderación</i>	89
Tabla 10. <i>Diseño de la Evaluación de Métricas y Métodos</i>	92
Tabla 11. <i>Detalle de Métrica: Cumplimiento de la Funcionalidad</i>	93
Tabla 12. <i>Detalle de Métrica: Fácil función de aprendizaje</i>	94
Tabla 13. <i>Detalle de Métrica: Consistencia Operacional de Uso</i>	96
Tabla 14. <i>Detalle de Métrica: Falsos Positivos</i>	97
Tabla 15. <i>Detalle de Métrica: Tiempo de Respuesta</i>	98
Tabla 16. <i>Detalle de Métrica: Consumo de Recursos</i>	99
Tabla 17. <i>Detalle de Métrica: Cumplimiento con Seguridad de Acceso</i>	101
Tabla 18. <i>Detalle de Métrica: Fácil de Implantación</i>	103
Tabla 19. <i>Detalle de Métrica: Grado de Coexistencia</i>	104
Tabla 20. <i>Matriz de Resultados y Comparación de Herramientas Evaluadas</i>	107
Tabla 21. <i>Evaluación de Métrica Cumplimiento de la Funcionalidad para la Herramienta Nessus</i>	117
Tabla 22. <i>Resultado de la Característica Funcionalidad para la Herramienta Nessus</i> 120	
Tabla 23. <i>Evaluación de Métrica Fácil función de aprendizaje para la Herramienta Nessus</i>	121
Tabla 24. <i>Evaluación de Métrica Consistencia operacional de uso para la Herramienta Nessus</i>	123

Tabla 25. <i>Resultado de la Característica Usabilidad para la Herramienta Nessus</i>	124
Tabla 26. <i>Evaluación de Métrica Falsos positivos para la Herramienta Nessus</i>	125
Tabla 27. <i>Resultado de la Característica Fiabilidad para Nessus</i>	126
Tabla 28. <i>Evaluación de Métrica Tiempo de respuesta para la Herramienta Nessus</i> ..	127
Tabla 29. <i>Evaluación de Métrica Consumo de recursos para la Herramienta Nessus</i> ..	128
Tabla 30. <i>Resultado de la Característica Eficiencia para Nessus</i>	130
Tabla 31. <i>Evaluación de Métrica Cumplimiento con seguridad de acceso para la Herramienta Nessus</i>	131
Tabla 32. <i>Resultado de la Característica Seguridad para Nessus</i>	132
Tabla 33. <i>Evaluación de Métrica Facilidad de implantación para Nessus</i>	133
Tabla 34. <i>Evaluación de Métrica Grado de coexistencia para la Herramienta Nessus</i>	135
Tabla 35. <i>Resultado de la Característica Portabilidad para la Herramienta Nessus</i>	136
Tabla 36. <i>Resultado General de la Herramienta Nessus</i>	137
Tabla 37. <i>Evaluación de Métrica Cumplimiento de la funcionalidad para la Herramienta Cisco Stealthwatch</i>	138
Tabla 38. <i>Resultado de la Característica Funcionalidad para la Herramienta Cisco Stealthwatch</i>	140
Tabla 39. <i>Evaluación de Métrica Fácil función de aprendizaje para la Herramienta Cisco Stealthwatch</i>	140
Tabla 40. <i>Evaluación de Métrica Consistencia operacional de uso para la Herramienta Cisco Stealthwatch</i>	143
Tabla 41. <i>Resultado de la Característica Usabilidad para la Herramienta Cisco Stealthwatch</i>	144
Tabla 42. <i>Evaluación de Métrica Falsos positivos para la Herramienta Cisco Stealthwatch</i>	145
Tabla 43. <i>Resultado de la Característica Fiabilidad para la Herramienta Cisco Stealthwatch</i>	146
Tabla 44. <i>Evaluación de Métrica Tiempo de respuesta para la Herramienta Cisco Stealthwatch</i>	147

Tabla 45. <i>Evaluación de Métrica Consumo de recursos para la Herramienta Cisco Stealthwatch</i>	148
Tabla 46. <i>Resultado de la Característica Eficiencia para la Herramienta Cisco Stealthwatch</i>	150
Tabla 47. <i>Evaluación de Métrica Cumplimiento con seguridad de acceso para la Herramienta Cisco Stealthwatch</i>	151
Tabla 48. <i>Resultado de la Característica Seguridad para la Herramienta Cisco Stealthwatch</i>	152
Tabla 49. <i>Evaluación de Métrica Facilidad de implantación para la Herramienta Cisco Stealthwatch</i>	153
Tabla 50. <i>Evaluación de Métrica Grado de coexistencia para la Herramienta Cisco Stealthwatch</i>	155
Tabla 51. <i>Resultado de la Característica Portabilidad para la Herramienta Cisco Stealthwatch</i>	157
Tabla 52. <i>Resultado General de la Herramienta Cisco Stealthwatch</i>	158
Tabla 53. <i>Cuadro comparativo del resultado de evaluación</i>	159
Tabla 54. <i>Niveles de resultados obtenidos en la evaluación</i>	160
Tabla 55. <i>Resultados de Matriz de Comparación</i>	163

ÍNDICE DE FIGURAS

Figura 1. Principios de la Seguridad de la Información	15
Figura 2. Tipos de CSIRT	21
Figura 3. Método Empírico	30
Figura 4. Método Delphi - Juicios de Expertos.....	32
Figura 5. ISO 9000/9001 Sistema de Gestión de Calidad Basado en Procesos	33
Figura 6. ISO 12207 Calidad del Producto Software	35
Figura 7. ISO/IEC 9126	36
Figura 8. ISO/IEC 9126-1 Calidad Interna y Externa junto a Calidad de Uso.....	37
Figura 9. Calidad Interna y Externa - Funcionalidad	39
Figura 10. Calidad Interna y Externa – Confiabilidad.....	40
Figura 11. Calidad Interna y Externa – Usabilidad.....	40
Figura 12. Calidad Interna y Externa – Eficiencia	41
Figura 13. Calidad Interna y Externa – Mantenibilidad.....	42
Figura 14. Calidad Interna y Externa – Portabilidad.....	43
Figura 15. ISO/IEC 9126-1 Gestión del Modelo de Calidad del Software	43
Figura 16. ISO/IEC 9126-1 Calidad de Uso	44
Figura 17. ISO/IEC 14598	58
Figura 18. ISO 37000: 37001 Anticorrupción y Ética	61
Figura 19. Proceso de Selección de Herramientas de Ciberseguridad para el CSIRT Académico ESPE.....	65
Figura 20. Procesos de Justificación ISO 37001 - CSIRT.....	67
Figura 21. Actividades del Proceso de Evaluación	68
Figura 22. Clasificación de servicios de un CSIRT	69
Figura 23. Clasificación de Características de la Calidad del Software de Ciberseguridad	74
Figura 24. Clasificación de Funcionalidades por Tipo de Software	75
Figura 25. Clasificación de funcionalidades por servicio del CSIRT.....	76
Figura 26. Niveles de Calificación de Evaluación	83

Figura 27. Procesos de selección ESPE - SERCOP	111
Figura 28. Propuesta de servicios iniciales CSIRT-ESPE.....	112
Figura 29. Propuesta de servicios de desarrollo CSIRT-ESPE	113
Figura 30. Logo del Software Nessus	113
Figura 31. Logo de Cisco Stealthwatch	114
Figura 32. Comparación de resultados obtenidos.....	160
Figura 33. Niveles de evaluación de la Herramienta Nessus	161
Figura 34. Niveles de evaluación de la Herramienta Cisco Stealthwatch.....	161
Figura 35. Ponderación de características de calidad.....	162

ABSTRACT

The purpose of this research work is to provide the Incident Response Team Group (CSIRT) at the La Universidad de las Fuerzas Armadas ESPE, a model that allows the optimal selection of cybersecurity tools, which cover all the requested requirements and the respective justification for specific functions of the CSIRT, the model will be composed of structures of good professional practices, ISO standards of software quality assurance and software quality models, detailed verification processes, flows, selection methods and graphs that allow making the right decisions within the functions specified by the academic CSIRT.

KEYWORD

- **COMPUTER SECURITY INCIDENT RESPONSE TEAM**
- **INFORMATION SECURITY**
- **ISO STANDARDS SOFTWARE**
- **ACADEMIC CSIRT**

1. CAPITULO I

El presente trabajo de investigación tiene como finalidad proporcionar al Grupo de Equipo de Respuesta antes Incidentes (CSIRT) de la Universidad de las Fuerzas Armadas ESPE, un modelo que permite la óptima selección de herramientas de ciberseguridad, que abarquen con la totalidad de los requerimientos solicitados y la justificación respectiva por funciones específicas del CSIRT, el modelo estará compuesto por estructuras de buenas prácticas profesionales, normas ISO de aseguramiento de la calidad del software y modelos de calidad del software, se detalla los procesos de verificación, flujos, métodos de selección y gráficas que permiten tomar decisiones acertadas dentro de las funciones que especifican el CSIRT académico.

1.1. Antecedentes

La información es el activo más importante de las organizaciones actualmente, por esta razón se han creado estándares, manuales de buenas prácticas y normas de aplicación que contienen actividades para garantizar que este activo se encuentre protegido de incidentes que impacten a los objetivos estratégicos de la organización. En este ámbito, actualmente se registran elevadas cifras de intrusiones en los sistemas de información de diversas instituciones, los cuales son llevados a cabo mediante la ejecución de ataques con denegación de servicios, robo o alteración de la información, entre otros.

Con la intención de minimizar el impacto de estas acciones delictivas e irregulares, muchas organizaciones han implementado CSIRT (Equipos de Respuesta ante Incidencias de Seguridad), que realizan el monitoreo constante de la infraestructura tecnológica de la organización, con la finalidad de detectar y prevenir actividades maliciosas y actuar con medidas oportunas en el caso de presentarse algún tipo de eventualidad o incidencia, de esta manera mitigar el impacto de riesgos que afectan a las infraestructuras críticas en las instituciones. (Incidentes, 2018).

Para conformar un CSIRT se deben tomar en cuenta varios factores y componentes, entre los cuales se encuentra la plataforma de ciberseguridad a utilizarse para el monitoreo y detección de vulnerabilidades en la infraestructura tecnológica de la organización, existen varias opciones en el mercado, pero habrá que analizar la mejor opción que se adapte al CSIRT académico. (Andrade R, 2013).

En este sentido, actualmente se encuentra en curso el desarrollo de un modelo para la implementación de un CSIRT académico en la Universidad de las Fuerzas Armadas ESPE. (De La Torre & Parra, 2018).

1.2. Problemática

1.2.1. Contextualización del Problema

El proceso de selección de herramientas de ciberseguridad y herramientas de software en general debe abarcar aspectos importantes, como el análisis minucioso de los requerimientos establecidos y las características de la calidad del software a adquirirse, esto con el propósito de que la decisión tomada sea la más acertada y completamente adaptable a los objetivos de las funciones para las que se va a emplear.

Los procesos de selección deben ser transparentes y garantizar que los resultados sean en función de los objetivos establecidos en la selección, sin favorecer a terceros, evitando casos de corrupción, una mala adquisición que no se adapte a las necesidades o una mala utilización de recursos.

Las herramientas o software de ciberseguridad en un CSIRT académico son de vital importancia, ya que permiten una exploración investigativa, tanto de las vulnerabilidades de seguridad de la información, análisis forense, monitoreo de recursos informáticos y todas las actividades desarrolladas en el CSIRT, sin embargo, al no contar con un marco definido de evaluación previa a la adquisición de este tipo de herramientas se tiende a que la herramienta a adquirirse no garantice la correcta realización de estas actividades.

Las respuestas ante incidentes de seguridad de la información deben ser óptimo, permitiendo mitigar el riesgo existente ante amenazas, como accesos no autorizados, denegación de servicios, entre otras; y a su vez se debe prevenir que estas amenazas se materialicen mediante el monitoreo continuo, análisis de vulnerabilidades, generación de reportes, entre otros. Esto constituye los servicios reactivos y proactivos de un CSIRT.

Para que el CSIRT pueda llevar a cabo sus funciones es importante contar una plataforma de ciberseguridad, ya que esto permite un óptimo trabajo por parte del equipo, pero existe el riesgo de que la plataforma seleccionada no cumpla con las características de calidad requeridas y por ende sea un desperdicio de recursos, evitando que los objetivos se cumplan de manera correcta.

1.3. Formulación del Problema

¿Cómo crear un modelo que me permita seleccionar las herramientas de ciberseguridad de manera óptima y adecuada, para el CSIRT Académico en la Universidad de las Fuerzas Armadas ESPE?

1.4. Justificación

La Universidad de Las Fuerzas Armadas ESPE, cuenta con servicios en línea con la finalidad de facilitar los procesos académicos, administrativos y su funcionamiento en general. Esto aumenta los escenarios de riesgo de seguridad debido al creciente número de vulnerabilidades y la mayor frecuencia y sofisticación de los ciberataques, para prevenir estos riesgos es necesario contar con una plan de acción, lo que proporciona el CSIRT académico, el cual se deberá dotar de herramientas con el fin de monitorear de

manera eficiente la infraestructura de red de la Universidad de las Fuerzas Armadas ESPE, con la finalidad de detectar intrusiones que pongan en riesgo la seguridad de la información.

Los incidentes de seguridad que no son atendidos a tiempo provocan graves efectos en los sistemas de información, se realizan mediante accesos no autorizados que provocan pérdida de información, denegación de servicios y otras acciones que afectan el cumplimiento de los objetivos institucionales, por lo que es de vital importancia contar dentro del CSIRT con herramientas apropiadas para el constante monitoreo del estado de los sistemas de información e infraestructura en general.

Por tal motivo es importante diseñar una metodología que permita, con eficacia y eficiencia, establecer las mejores herramientas para identificar vulnerabilidades en la infraestructura tecnológica, mitigar el impacto de amenazas informáticas y aplicar adecuadamente procedimientos reactivos y proactivos ante incidentes informáticos (Andrade R, 2013).

1.5. Objetivos

1.5.1 Objetivo General

Diseñar un modelo de análisis y selección de herramientas de Ciberseguridad para un CSIRT Académico, mediante el uso de procesos y estándares de calidad que garantice una elección adecuada que se adapte a las necesidades establecidas.

1.5.2 Objetivos Específicos

- Establecer las características de las herramientas usadas en un CSIRT académico
- Determinar los estándares y procesos de calidad que permiten evaluar un producto Software.
- Estudiar la situación actual del CSIRT-ESPE, analizando sus servicios y funciones establecidas.
- Fijar etapas del proceso de evaluación y selección de herramientas de ciberseguridad para un CSIRT académico.
- Establecer métricas para las características de calidad tomadas en cuenta, así como métodos a utilizarse en la evaluación.
- Realizar la ejecución del modelo establecido utilizando el caso de estudio CSIRT-ESPE.
- Validar el modelo propuesto mediante la técnica Delphi.

1.6 Alcance

La propuesta para definir un modelo de análisis y selección de las herramientas de Ciberseguridad para un CSIRT Académico, caso CSIRT-ESPE, contempla el estudio de la situación actual, funciones y servicios que delimitan el alcance y actuación del CSIRT.

También cubre lo correspondiente al análisis de metodologías, estándares y normas relacionadas a la evaluación de las características de un producto software,

identificando sus atributos de calidad y adaptándolas a las particularidades de una plataforma de Ciberseguridad que permita operar un CSIRT Académico.

El alcance se extiende a la selección preliminar y evaluación de aquellas herramientas que permitan al CSIRT-ESPE cumplir con sus objetivos, con esta acción se aplicará la metodología diseñada, analizando los resultados obtenidos, para posteriormente mediante el método Delphi realizar la validación en base a las opiniones de expertos. Para obtener criterios basados en experiencias reales de desarrollo de CSIRT Académicos de Universidades e Instituciones Educativas e implantación de herramientas de Ciberseguridad.

Permitiendo en función de este análisis, obtener conclusiones y recomendaciones del modelo desarrollado, como parte del proceso de mejora de dicho modelo; a partir de la exploración de los datos obtenidos en la ejecución del caso práctico para el CSIRT-ESPE.

Finalmente, permitirá verificar si los resultados obtenidos a partir del método a desarrollarse están alineados a los objetivos planteados y pueden tomarse como válidos, para su futura implementación.

1.7 Marco Legal del Proyecto de Investigación

Adquisición de Software Libre

Actualmente en el Ecuador, rige la normativa que plantea la promoción del uso del software libre u Open Source. Bajo el Decreto Ejecutivo N. 1014, emitido el 23 de abril del 2008:

Artículo 1: “*Establecer como política pública para las entidades de la Administración Pública Central la utilización de software libre en sus sistemas y equipamientos informáticos*” (Decreto Ejecutivo 1014, 2008).

El en Código Orgánico de la Economía Social de los Conocimientos:

Artículo 144: “*Las instituciones del sistema nacional de educación y del sistema de educación superior, únicamente para su funcionamiento administrativo, deberán usar software siguiendo el esquema de prelación y criterios establecidos en el artículo 148.*” (Código Orgánico de la Economía Social de los Conocimientos, 2006).

Justificación de Adquisición de Software Propietario

Bajo los escenarios previstos, se analiza la factibilidad legal de la aplicación del proyecto, teniendo el respaldo legislativo, en el Código Orgánico de la Economía Social de los Conocimientos:

Artículo 144(B): “*... las instituciones del Sistema de Educación Superior no estarán obligadas a usar exclusivamente tecnologías digitales libres en el ejercicio de la libertad de cátedra y de investigación, pero deberá garantizarse una enseñanza holística de soluciones informáticas independientemente de su tipo de licenciamiento*” (Código Orgánico de la Economía Social de los Conocimientos, 2006).

Además, de acuerdo al artículo 148, el orden de prelación debe ser justificado teniendo en cuenta los siguientes criterios:

1. Sostenibilidad de la solución;

2. Costo y oportunidad;
3. Estándares de seguridad; y,
4. Capacidad técnica que brinde el soporte necesario para el uso del software.

Bajo ese contexto, el contratante deberá justificar la adquisición de un Software propietario en función de las necesidades por las que se va a adquirir. Como una base de justificación para este proyecto de investigación, se da importancia a la utilización de manuales de usabilidad, soporte técnico y ayuda web, estos datos son muy importantes para considerar como análisis de las herramientas de ciberseguridad, se puede identificar que estos atributos son propios del software propietario, de esta manera se descarta la posibilidad de utilizar software libre.

Ley de Accesos No Autorizados

Un CSIRT contempla servicios de monitoreo, para esto se tiene que acceder a infraestructuras informáticas, siendo este el contexto en el Ecuador se encuentra tipificado el acceso no autorizado. (Código Orgánico Integral Penal, 2014).:

Artículo 234.- “Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin

pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.” (Código Orgánico Integral Penal, 2014).

Ley de Protección de Datos

El proyecto de investigación genera información confidencial para el CSIRT-ESPE, estos datos contienen información de reportes o informes, que se generaron a través de las herramientas de ciberseguridad seleccionadas, esta información no debe ser expuesta a otros entornos, áreas o sectores, que pueden afectar a la seguridad de la información de la Universidad de las Fuerzas Armadas ESPE; esta información no puede ser divulgada sin autorización del CSIRT-ESPE, la información solo está sujeta al cumplimiento de funciones del CSIRT-ESPE, apoyándose en la Ley del Sistema Nacional de Registro de Datos Públicos, en los siguientes artículos:

Art. 23.- Sistema Informático. – “El sistema informático tiene como objetivo la tecnificación y modernización de los registros, empleando tecnologías de información, bases de datos y lenguajes informáticos estandarizados, protocolos de intercambio de datos seguros, que permitan un manejo de la información adecuado que reciba, capture, archive, codifique, proteja, intercambie, reproduzca, verifique, certifique o procese de manera tecnológica la información de los datos registrados” (Públicos, 2010).

Art. 26.- Seguridad. – “Toda base informática de datos debe contar con su respectivo archivo de respaldo, cumplir con los estándares técnicos y plan de contingencia que impidan la caída del sistema, robo de datos, modificación o cualquier otra circunstancia que pueda afectar la información pública” (Públicos, 2010).

Art. 27.- “Responsabilidad del manejo de las licencias. - Las Registradoras o Registradores y máximas autoridades, a quienes se autoriza el manejo de las licencias para el acceso a los registros de datos autorizados por la ley, serán las o los responsables directos administrativa, civil y penalmente por el mal uso de las mismas” (Públicos, 2010).

2. CAPITULO II

MARCO TEÓRICO

2.1. Introducción

En este capítulo se detalla los temas relevantes en el contexto de la ciberseguridad, focalizando la selección de herramientas para la gestión de un CSIRT académico, con el propósito de dar un marco referencial a través de un método propicio que permita la efectividad en la selección de herramientas como Nessus y Cisco Stealthwatch.

Además, de recalcar la importancia de la necesidad y obligación que tienen las organizaciones de proteger la información, servicios tecnológicos e infraestructura, debido a las actuales exigencias del mundo tecnológico. Por esta razón se han implementado varios mecanismos, estándares y metodologías que engloban a la calidad del producto software, su aplicación e importancia, por ejemplo, la familia de normas ISO/IEC 9126, definiciones de funciones del CSIRT, métricas de selección y modelos de calidad.

Ante la latente existencia de riesgos, vulnerabilidades y amenazas es esencial que la organización cuente con planes de contingencia para la mitigación, reducción y control de estos. La organización debe garantizar que sus partes interesadas, no tengan afectación debido al impacto que representa la presencia de una incidencia de seguridad de la información.

Los equipos de respuesta ante incidentes informáticos, mejor conocido como CSIRT, tienen como uno de sus principales objetivos la preservación de la seguridad de la información en la institución y por ende garantizar la confiabilidad, integridad y disponibilidad de servicios tecnológicos evitando denegación de servicios, robo de información, contribuyendo así al correcto desenvolvimiento de las actividades cotidianas de la Institución.

Un CSIRT es un grupo de personas totalmente especializadas en Ciberseguridad que prestan unos servicios a sus clientes de forma remota, desde unos centros de servicio (Moreno, 2015). Debido a esto un CSIRT académico debe permitir la formación y aprendizaje de los estudiantes sobre las metodologías, funciones y actividades de un centro de servicios, además de apoyar en la enseñanza del manejo de herramientas tecnológicas y software de seguridad de la información, con el propósito de obtener futuros profesionales capacitados en la gestión de un CSIRT.

Actualmente la Universidad de las Fuerzas Armadas ESPE, cuenta con un proyecto para la creación de un CSIRT Académico, este proyecto permitirá adecuar y contribuir con la formación de alumnos en el área de seguridad de la información, análisis forense y gestión de riesgos. Para ello es indispensable contar con un proceso de selección de herramientas de Ciberseguridad, como herramientas de monitoreo, gestión de incidentes, análisis forense, entre otras.

2.2. La Ciberseguridad

Según ISACA (Information Systems Audit and Control Association), La ciberseguridad es la “Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados” (ISACA, 2017).

Como se menciona anteriormente, la Ciberseguridad se enfoca en brindar protección a los activos de información en los sistemas de información, los activos de información comprenden todos los elementos que constan en la base de conocimientos de una organización, como archivos, contratos, bases de datos, manuales, entre otros. En otras palabras, los activos de información según la definición de la norma ISO 27001, se entiende como el consolidado de conocimientos o datos que tiene un determinado valor para la organización, mientras que los sistemas de información se refieren a la tecnología que permite la gestión de la información.

La Ciberseguridad se relaciona con la seguridad informática al enfocarse en la información en formato digital y los sistemas de información que la gestionan mediante el procesamiento, almacenamiento y transmisión de la misma.

2.2.1 Importancia de la Información en las Organizaciones

Todas las organizaciones actualmente se componen por un conjunto de procesos sinérgicos interconectados, que procesan información de forma cooperativa y que dependen de la disponibilidad, integridad y confidencialidad de la misma para que las

actividades de la organización se efectúen con éxito, por esta razón se percibe a la información como el activo más esencial de toda empresa, por lo que se debe implementar mecanismos óptimos para salvaguardarla.

2.3. Principios de la seguridad de la información

Los principios fundamentales de la seguridad de la información son conocidos como, La confidencialidad, Integridad y Disponibilidad deben garantizarse al igual que el no repudio, autenticidad y trazabilidad de esta en todos los procedimientos en los cuales esté relacionada (Krutz & Vines, 2002).

La efectividad de los controles usados para las medidas de riesgo de la seguridad de la información se debe medir en los principios mencionados anteriormente.



Figura 1. Principios de la Seguridad de la Información

Fuente: ISACA

Además de los principios más importantes, se tienen otros aspectos que se toman en cuenta dentro de la definición de la seguridad de la información tales son:

Confidencialidad

Se refiere a que solo las personas autorizadas a cierta información la conozcan, mediante el establecimiento de privilegios a determinadas cuentas de usuarios u otros mecanismos para gestionar los accesos a la información.

Integridad

Este principio se basa principalmente en que la información pueda ser alterada solamente en el proceso legítimo en un lapso de tiempo establecido, por el personal y sitio autorizado. Toda alteración en distintas condiciones no puede estar permitida.

Disponibilidad

Se entiende como la garantía de que la información esté accesible por las personas que estén autorizados en el momento en que la requieran. También existen características secundarias, cuya función es hacer uso de procedimientos que aportan con el aseguramiento de la información:

No Repudio

Permite establecer que los responsables que participan en las transacciones, no puedan renunciar sus actividades en el proceso.

Trazabilidad

Se interpreta como un servicio que permite el registro constante del flujo de la información a través de los componentes que la procesan, en el que se deben propiciar los detalles y el tiempo que permitan reconstruir un hecho.

Autenticación

Tiene como objetivo identificar los roles que se les otorga a los individuos, abarcando privilegios que tiene sobre un proceso en el cual esté implicado un activo de información.

2.3.2. Principales riesgos relacionados con la tecnología emergente

La tecnología es la herramienta clave para el tratamiento eficaz de la información, sin embargo, existen innumerables riesgos en el contexto tecnológico debido a que los sistemas de gestión de los activos de la información son un conjunto de componentes distribuidos, por ejemplo, en una arquitectura cliente-servidor, se tienen elementos principales que son: el cliente, servidor y los protocolos de comunicación, como TCP/IP, FTP, SMTP, HTTP, entre otros.

El número de elementos involucrados hace más susceptible a fallos de seguridad debido a que un intruso tiene mayor superficie de ataque. (Manadhata, 2018), es decir a mayor número de componentes es mayor la probabilidad de que cuenten con vulnerabilidades explotables lo que implica que una amenaza puede aprovecharse y por ende el riesgo es mayor, y su impacto afectaría en un grado alto en la labor diaria de la institución.

Actualmente la superficie de ataque en las instituciones u organizaciones está aumentando cada vez más, debido a las exigencias del mundo globalizado, según Cisco Systems, cada año se evidencia el crecimiento exponencial de la superficie de ataque debido a la integración de nuevas tecnologías como IoT (Internet of things), que incorpora nuevos endpoints como DVRs, cámaras IP, SmartTVs y otros componentes relacionados con la domótica y smartcities que requieren el uso de nuevos protocolos de comunicación que aún no han alcanzado su grado de madurez, sin embargo pese a todas las vulnerabilidades existentes el usuario final es categorizado como la principal causa de las intromisiones de seguridad en las organizaciones. (Cisco Systems, 2017)

Todo apunta a que las organizaciones opten con mayor responsabilidad la implementación de controles efectivos que permitan de cierta manera gestionar el riesgo, existen varios mecanismos abordados en la actualidad

Principales riesgos de seguridad

- Spamming
- Search Poisoning
- Botnets
- Denial of Service (DoS)
- Phishing
- Malware
- Website Threats

(Mahmood & Afzal, 2013)

2.4. Equipo de Respuesta ante Incidentes (CSIRT)

2.4.1. Definición

Se conoce como CSIRT a un Equipo de Respuesta a Incidentes de Seguridad Informática, que se conforma por un conjunto de expertos que son encargados de la gestión de los incidentes de seguridad de la información, mediante la prevención, identificación y tratamiento de los mismos, además de proveer medidas, estrategias y planes para la mitigación de riesgos y la recuperación ante incidentes de la seguridad de la información detectadas (De La Torre & Parra, 2018).

2.4.2. Funciones y Servicios de un CSIRT

Uno de los aspectos esenciales a tomar en cuenta, al momento de constituir un CSIRT, es sin duda alguna la definición de funciones o servicios que se va a realizar, analizando la capacidad y recursos con los que se cuentan. Estableciendo así el alcance que va a cumplir, estableciendo las actividades para la detección, análisis y tratamiento de las incidencias de seguridad de la información en la institución.

Según (Van Der Heide, 2017). Los servicios que presta un CSIRT se clasifican en tres grupos definidos:

- Servicios Reactivos
- Servicios Proactivos
- Servicios de gestión de calidad de seguridad

2.4.2.1. Servicios Reactivos

Son aquellos que se diseñan con el propósito de brindar asistencia a incidentes generados a partir de notificaciones, detecciones mediante monitoreo, entre otros. Además, se plantean con el propósito de reportar estos incidentes de una manera oportuna para su posterior tratamiento, estos incidentes están relacionados usualmente con amenazas o ataques, como equipos comprometidos, malware, vulnerabilidades u otro tipo de incidentes similares (Van Der Heide, 2017).

- Alertas y Advertencias
- Manejo de incidentes
- Manejo de la vulnerabilidad
- Manejo de artefactos

2.4.2.2. Servicios Proactivos

Son aquellos servicios que se constituyen con el propósito de prevenir que la incidencia tenga una afectación o impacto real en los componentes de la arquitectura de la organización. Normalmente se realizan actividades como:

- Anuncios
- Monitoreo continuo
- Auditorias de Seguridad / Pentests
- Desarrollo de herramientas Detección de intrusión
- Difusión de Inteligencia de amenazas

2.4.2.3. Servicios de gestión de la calidad

Son servicios que no se enfocan en el tratamiento de incidentes en particular, sino de manera general proporcionan lineamientos de mejora de la seguridad de la información de la organización. Mediante la retroalimentación en la prestación de servicios proactivos y reactivos, se adquiere conocimiento, con el propósito de brindar recomendaciones en base a la experiencia que va adquiriendo el CSIRT, las actividades que se tienen en esta clasificación, entre otras son:

- Análisis de riesgo
- Planificación Continuidad del negocio y Recuperación ante desastres
- Conciencia de seguridad Formación (De La Torre & Parra, 2018).

2.4.3. Clasificación de los CSIRT

Dependiendo de su ámbito de implementación los CSIRT se clasifican,

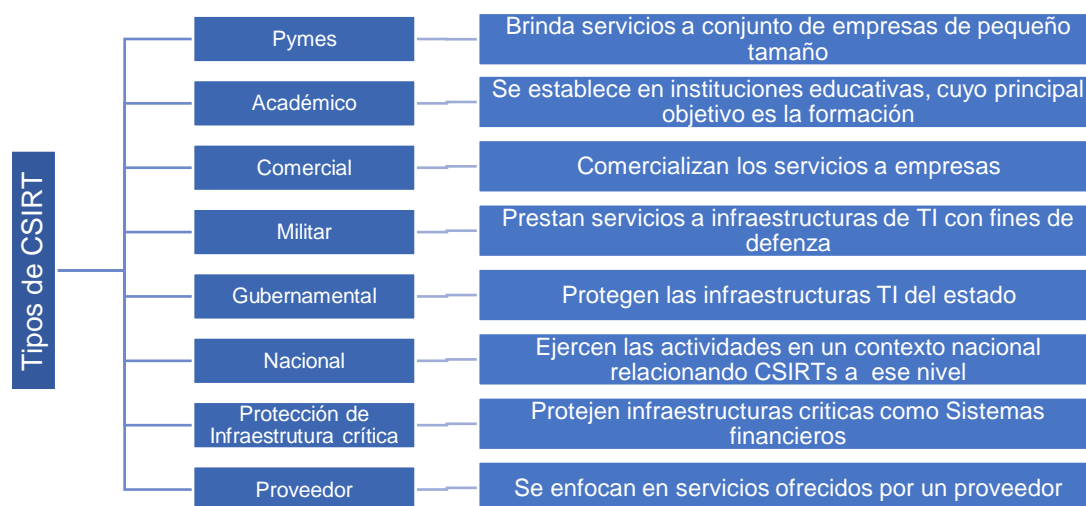


Figura 2. Tipos de CSIRT

Fuente: (De La Torre & Parra, 2018)

Como se puede apreciar hay un catálogo de clasificación de CSIRT, varían es sus características como esquema organizacional, ámbito de aplicación y sobre todo en los servicios que estos ofrecen, sin embargo, en este proyecto se focalizará principalmente en el análisis y descripción de un CSIRT Académico.

2.5. CSIRT Académico

Los CSIRT Académicos no se basan solamente en los servicios relacionados en la gestión de incidentes de la seguridad informática, sino que además propician de entornos favorables para la formación e investigación en la institución educativa.

Además, uno de los servicios del CSIRT académico se centra en la formación, que proporciona un plan de capacitación que se fija como objetivos:

- Dar a conocer el funcionamiento interno del CSIRT
- Mejorar y ejercitar las habilidades técnicas de todo el personal
- Mantenerse al tanto de los avances tecnológicos en materia de Ciberseguridad mediante la constante investigación

2.4.5. CSIRT Académicos en la Formación en Herramientas de Ciberseguridad

En un CSIRT académico unos de los objetivos que priman es la formación y entrenamiento, el personal debe adquirir la destreza y conocimiento profundo de las capacidades de las herramientas de Ciberseguridad a utilizarse mediante:

- Capacitación por parte del proveedor
- Ejercicios continuos y explotación al máximo de funcionalidades

- Revisar documentación y prestar atención exhaustiva de todas sus características
- Si la herramienta contiene un lenguaje de scripting u otro complemento, es importante explorar a profundidad la característica.

Tomando en cuenta estas recomendaciones se busca que el personal desarrolle el grado de expertos requerido para entender infraestructuras de TI complejas que se complementa con el uso adecuado de determinada herramienta con el objetivo final de generar resultados que aporten con la disminución de vulnerabilidades.

Como se menciona previamente, la función de formación y capacitación del CSIRT académico, provee un excelente entorno en el cual el personal junior, como estudiantes, pasantes y personal con poca experiencia desenvuelva actividades de entrenamiento bajo la supervisión de evaluadores con experiencia, utilizando las herramientas que se hayan seleccionado, estos evaluadores a su vez deberán tener muy claro el funcionamiento mecánico de las herramientas y el criterio de su utilización, para formar al personal con el juicio necesario para que ejerzan las actividades de manera efectiva.

2.4.6. Herramientas de Ciberseguridad para un CSIRT Académico

Hoy en día existe un sinnúmero de herramientas tanto libres como propietarias que tienen características que permiten evaluar, reportar, gestionar y explotar vulnerabilidades en infraestructuras de TI, sin embargo, es muy importante que el CSIRT establezca un conjunto de herramientas elegidas con criterio conforme a sus necesidades, debido a que esta herramienta se deberá ajustar a las necesidades y

cumplir con las condiciones del entorno del CSIRT. A continuación, (Wyk, 2007), recomienda la siguiente lista de particularidades que una herramienta debe poseer para ser seleccionada:

- **Visibilidad:** Se refiere a que las actividades realizadas y los informes generados por la herramienta deben ser completamente visibles y entendibles por el equipo, en medida de lo posible hay que evitar las herramientas que ocultan la información con fines comerciales.
- **Extensibilidad:** Se trata de que se debe enfocarse en las herramientas que son flexibles a personalización, permitiendo adaptar la herramienta al uso que se le desee dar en las circunstancias dadas, por ejemplo, aquellas herramientas que tengan la capacidad de adaptar plug-in o scripting, que se adaptan al uso que se le pueda dar.
- **Configurabilidad:** Debe permitir alta configuración en función de los parámetros que se desee evaluar dentro de la actividad llevada a cabo.
- **Documentación:** Es muy importante contar con explicación, guías de uso o manuales de configuración para explotar al máximo sus funcionalidades.

Adicionalmente, se deberá tener en cuenta otros criterios de selección como presupuesto, facilidad de uso, apoyo del proveedor (si la herramienta es propietaria) y entre otras características que estudiadas más adelante con el propósito de brindar un marco referencial para la implantación de herramientas en un CSIRT académico. Cabe mencionar que se debe contar con un juicio de expertos para la correspondiente validación del conjunto de herramientas seleccionado, para tener una mayor garantía de

que este sea el indicado, tanto para la formación del personal como para la gestión de incidentes de Ciberseguridad.

2.6. Herramientas de Ciberseguridad

En esta sección se proporciona una introducción, categorización y visión general a las herramientas comúnmente usadas en la realización de actividades en un CSIRT como herramientas de monitoreo, forenses, alertas y gestión de incidentes, entre otras.

2.6.1. Herramientas de Monitoreo

Para poder detectar intrusiones en la infraestructura de TI, se requiere una continua observación de los componentes de la misma, escaneando y visualizando los canales por donde el flujo de activos de información se transporta.

2.6.2. Herramientas de Evaluación de Seguridad

Las Herramientas de Evaluación de Seguridad, están diseñada para ayudarle a identificar y abordar los riesgos de seguridad de su entorno informático. La herramienta utiliza un enfoque integral para medir el nivel de seguridad y cubre aspectos tales como usuarios, procesos y tecnología. Sus conclusiones incluyen orientaciones y recomendaciones para mitigar los esfuerzos además de enlaces a información adicional sobre cuestiones propias del sector si ello es necesario. Estos recursos pueden informarle sobre las herramientas y métodos específicos que mejor le pueden ayudar a modificar la situación de la seguridad en su entorno tecnológico (Microsoft, 2017).

2.5.2.1. Escáneres de puerto

Las herramientas de escaneo de puertos permiten recompilar información sobre una ubicación de red remota, localizando los servicios de red que están disponibles en cada host de destino, se realiza una comprobación uno a uno de los puertos designados o predeterminados en el componente de destino.

2.5.2.2. Análisis de vulnerabilidad

Los análisis de vulnerabilidad pretenden explotar las vulnerabilidades conocidas en los componentes de una infraestructura de TI, a diferencia que los escáneres de puertos que obtienen inventarios de los servicios disponibles, los escáneres de vulnerabilidad generan un informe de las potenciales y comunes falencias de seguridad.

2.5.2.3. Herramientas de Alertas y reportes

Detectan afectaciones a la seguridad en la infraestructura tecnológica, redes y en la información que compromete a ocasionar a una vulnerabilidad en riesgo, de esta manera emiten reportes que permiten tomar decisiones a tiempo sin ocasionar daños o consecuencias futuras.

2.5.2.4. Herramientas Forenses

Permiten descubrir o interpretar datos electrónicos, colaboran con investigaciones estructuradas, validando la originalidad y la privación de la información. Utilizan procesos de recuperación de datos y análisis en reportes en datos recogidos.

2.5.2.5. Plataformas HoneyNet

Son herramientas de investigación para detección de intrusos que comprometen la seguridad de la red y conocer todas las estrategias que estos intrusos atacan o intervienen con la red, se podría decir son herramientas de trampa, adoptan sistemas compuestos muy creíbles para captar la atención de los intrusos, generalmente se encuentran en sistemas operativos de servidores.

2.5.2.6. Sistema de inteligencia de amenazas cibernéticas

Son conocimientos basados en evidencias que utilizan estrategias de seguridad que permiten a las organizaciones o instituciones analizar y tomar decisiones de defensas a ataques fortaleciendo y eliminando vulnerabilidades y mitigando riesgos.

2.5.2.7. Feeds

Son sistemas que permiten recoger entradas de blogs, estos blogs pueden estar en diferentes medios cargados en una misma web y visualizar actualizaciones de nuevos artículos de interés seleccionado por el usuario web.

2.5.2.8. Análisis de código

Son herramientas que utilizan un conjunto de tecnologías en el análisis el código fuente, detectando vulnerabilidades que compromete al código a ser atacado. Se analiza el funcionamiento en todo el ciclo de vida del software, y permite prevenir un escenario donde el software sea la responsable de un fallo de ciberseguridad.

2.5.2.9. Advertencias y avisos

Son herramientas de ciberseguridad que permiten convertir a las vulnerabilidades en alertas en tiempo real al personal con responsabilidad de gestionar el área a tratar de esta manera las vulnerabilidades no se convierte de vulnerabilidades a riesgos, y en el caso de alertar un riesgo, permite mitigar el riesgo.

2.6. Plataformas de Ciberseguridad Existentes en el Mercado

Debido a la demanda actual de herramientas que permitan el control y administración de incidentes de Ciberseguridad, debido a la creciente presencia de amenazas en el entorno digital, a la par se van teniendo ofertas en el mercado de plataformas que faciliten esta labor.

El principal enfoque que tienen es reducir el riesgo mediante el monitoreo continuo de los activos de activos de la información, gestión de incidentes y análisis de datos, esto permite dar una clara visión de lo que ocurriendo en los sistemas de información de la organización.

Dentro de las alternativas ofrecidas por el mercado, se va a estudiar las siguientes:

2.7. Modelos de Calidad de Software

Se denomina modelo a una representación conceptual, gráfica y matemática, de sistemas o procesos con el objetivo de realizar su análisis y estudio que permite generar informes y salidas predeterminadas, que permiten predecir los resultados obtenidos y tomar decisiones. Los modelos de calidad del software definen el grado de un sistema

cumple los requerimientos especificados y necesidades a expectativas del cliente o usuario.

Los modelos de procesos tradicionales por experiencia o recomendaciones, en algunos casos se podría decir por propuestas llamativas en tiempo de entrega y costo, pueden generar una gran probabilidad de adquirir errores a las selecciones de herramientas de software que cumplan efectivamente todos los requerimientos necesarios.

2.7.1. Tipos de Modelos de Calidad de Software

Tabla 1.
Niveles de Resultados Obtenidos en la Evaluación

<i>Área</i>	<i>Modelo de Calidad</i>
<i>Ciclo de Vida del Software</i>	CMMI
	ISO 12207
<i>Gobierno de TI (Organización)</i>	ISO 9000 / 9001
	COBIT
<i>Procesos del Fabricante</i>	PMBOOK
	ITIL
<i>Producto Software Final</i>	ISO 14598

2.8. Método Empírico Analítico

Para la realización de este proyecto se toma en cuenta el tipo de investigación a realizar, en este caso se realizará una investigación aplicada, ya que se fundamenta en

la aplicación o utilización de los conocimientos que se han adquirido luego de implementar y sintetizar la práctica basada en la investigación, esto se entiende como el manejo de los conocimientos en la práctica para aplicarlos en beneficio de aquellos grupos que participan en los diferentes procesos y en la sociedad en general.

2.8.1. Método Empírico Analítico – Experimental

Se seleccionó la investigación basada en la experimentación o la observación evidencias o resultados obtenidos a partir de la experimentación, pruebas u observación, todo aporte en este proyecto de investigación debe ser empírico, lo que significa que es basado en la evidencia y debe comprobarse mediante la observación y los análisis correspondientes en su selección aplicada en herramientas de ciberseguridad.

Durante su desarrollo se debe capturar datos contextuales priorizando su complejidad, analizar e identificar la experiencia de expertos, confirmar y promover los conceptos prácticos y teóricos de ciberseguridad, nos permitirá estar en un ambiente real y de mejor comprensión, combinando una amplia investigación con un estudio de caso detallado y analítico.

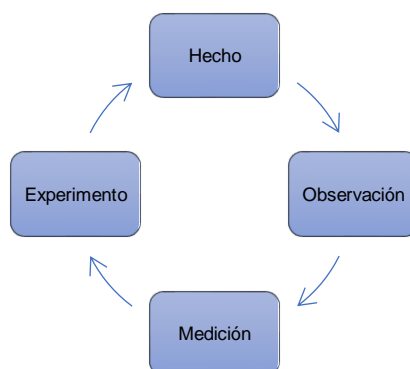


Figura 3. Método Empírico

2.8.2. Método Delphi

Es una técnica basada en la prospectiva y predicción en base a un panel de expertos en el tema a tratar o investigar, obtiene información cualitativa y prácticamente precisa de considerar en resultados obtenidos.

Busca un debate de opiniones de expertos es decir utiliza Juicios de Expertos, considerando las respuestas planteadas en un cuestionario entregado, este método posee principios como:

- Anonimato de expertos o participantes
- Retroalimentación de opiniones
- Respuesta estadística

2.8.2.1. Método Delphi - Juicio de Expertos

Es un proceso de actividades ordenado para lograr adquirir información de un panel de expertos seleccionados para tratar un tema en base a conocimiento y experiencias probadas, que nos permitirá tomar decisiones o nos orientaran en la elaboración de proyectos de investigación, las tareas son las siguientes:

- Establecer el tema de investigación.
- Selección del panel de expertos.
- Informar al panel de expertos la información que se desea obtener como objetivo.

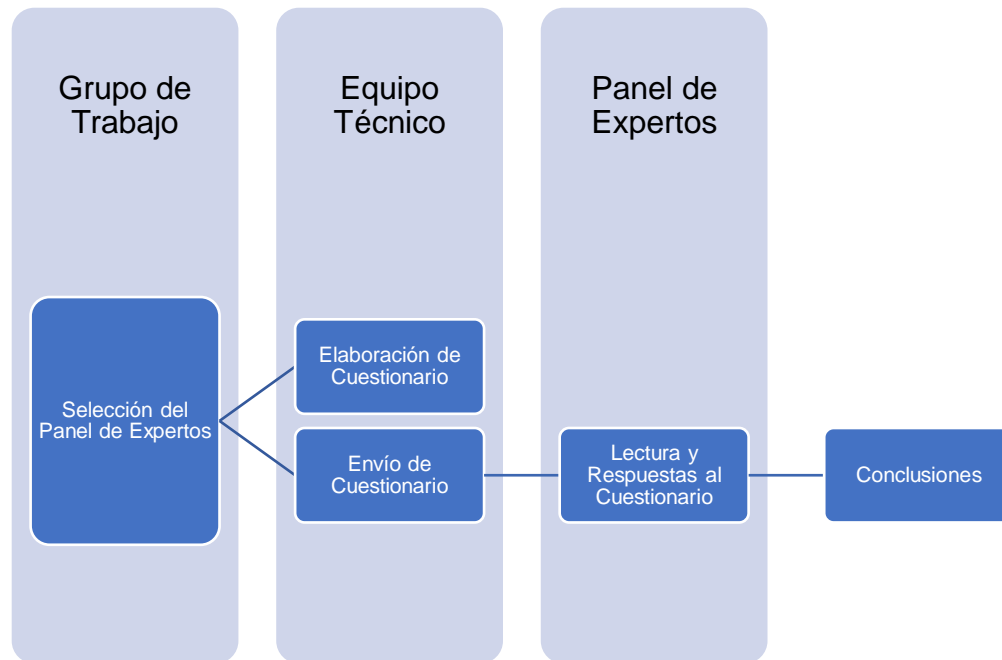


Figura 4. Método Delphi - Juicios de Expertos

2.9. Calidad del Producto Software

Las normas ISO (Organismo Internacional de Estandarización) utilizan varios conceptos, guías, métricas y parámetros de calidad, que nos permiten analizar y calificar procesos, servicios y productos ofertados y creados por las empresas u organizaciones.

Los estándares de calidad del software son bases fundamentales de la ingeniería de software, de esta manera se puede identificar efectividad en los procesos de desarrollo del software.

2.9.1. Estándar General de Sistema de Gestión de Calidad

2.9.1.1. ISO/IEC 9000: 9001

Nos permite conocer, evaluar o analizar la calidad de servicios o de un producto final de manera general en medición, de esta manera se puede otorgar credibilidad en el uso de calidad por parte de la empresa a ofertar y adquirir el producto software, al utilizar la norma ISO 9000 / 9001 nos permite evaluar:

- Reputación e imagen general de la empresa
- Nivel de satisfacción de los clientes o usuarios finales
- Ventaja competitiva de utilizar o adquirir productos o servicios
- Si posee calidad en los procesos internos que permiten cumplir con el objetivo
- Gestión de riesgos
- Calidad en infraestructura
- Mejora continua



Figura 5. ISO 9000/9001 Sistema de Gestión de Calidad Basado en Procesos

2.9.1.2. Aseguramiento de la Calidad del Software

Es un conjunto de actividades sistemáticas que permiten dar confianza al adquirente del software que cumple con requisitos de calidad como producto desarrollado por un fabricante, consta de las siguientes características:

- Métodos y herramientas de análisis.
- Inspecciones técnicas en todos los procesos de ciclo de vida del software.
- Control de documentación.
- Procedimientos de ajuste a estándares de calidad.
- Métricas de software de control.
- Gestión de configuración del software
- Auditorias e informes.

2.9.2. Estándares Específicos de la Calidad del Producto Software

2.9.2.1. ISO/IEC 12207

Es un estándar específico para el ciclo de vida del software en una organización, comprende de 17 procesos clasificados en 3 categorías:

- Principales
- Apoyo
- Organización

Este estándar nos permite identificar los procesos totales en el cumplimiento de requisitos de calidad desde la creación hasta la finalización y entrega del producto

software, una empresa o casa de software que tenga la norma ISO 12207 nos garantiza que sus procesos son garantizados en el desarrollo de software, garantizándonos:

- Análisis y recopilación de requerimientos adecuados del cliente.
- Calidad en el desarrollo de software.
- Entrega, Implantación y Capacitación adecuada del producto software.

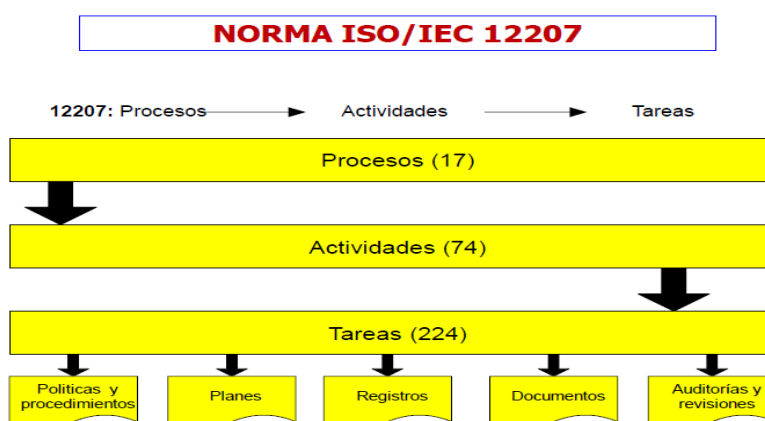


Figura 6. ISO 12207 Calidad del Producto Software

2.9.2.2. ISO/IEC 9126

Este estándar nos permite identificar la calidad en un producto software finalizado considerando su uso como principal característica a evaluar, se puede mencionar:

- **Funcionalidad.** Nivel de satisfacción en el cumplimiento de los requerimientos especificados al contraer el producto software por parte del cliente.
- **Fiabilidad.** Nivel de seguridad, tolerancia a fallos, recuperación y efectividad en la ejecución del software.

- **Usabilidad.** Nivel de facilidad de uso considerando comprensión, interfaz amigable y operatividad del software.
- **Eficiencia.** Nivel operatividad del software en tiempo adecuado en el uso de recursos del sistema.
- **Portabilidad.** Nivel de facilidad del software en que se pueda implantar y trasladar en diferentes entornos, ambientes y arquitecturas de hardware.

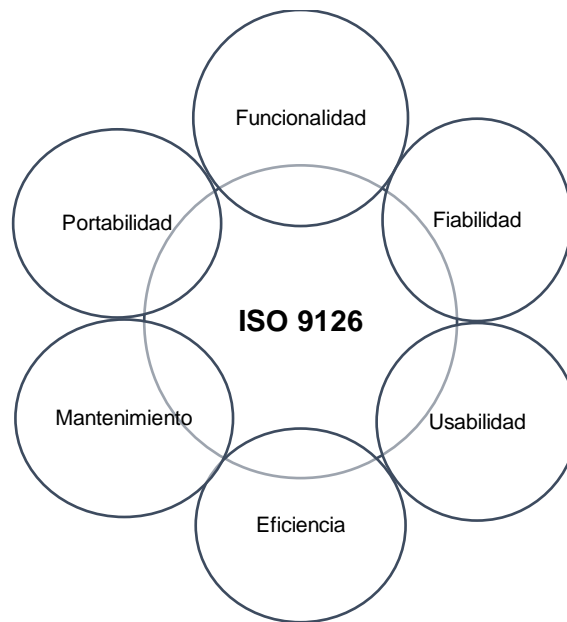


Figura 7. ISO/IEC 9126

La familia de la norma ISO 9126 consta de cuatro categorías:

- ISO/IEC 9126-1 Gestión de Modelo de Calidad del Software
- ISO/IEC 9126-2 Métricas Externas
- ISO/IEC 9126-3 Métricas Internas
- ISO/IEC 9126-4 Métricas de Calidad de Uso

La familia de la norma ISO 9126 garantiza calidad internacional en la comercialización del producto software, al tratar de incorporar herramientas de Ciberseguridad con proveedores internacionales, permite conocer al CSIRT acreditación de calidad internacional.

2.9.2.2.1. ISO/IEC 9126-1 Gestión del Modelo de Calidad del Software

La norma ISO/IEC 9126-1 permite evaluar la calidad del software tomando en cuenta aspectos de adquisición, requerimientos, soporte, uso y evaluación del software. El modelo está dividido en dos categorías:

- Calidad Interna y Externa
- Calidad de Uso

Se considera que la Usabilidad tiene un enfoque de análisis a nivel profesional-técnico con su propia interpretación a diferencia que la calidad de uso tiene un enfoque de un usuario final al software con criterio de experiencia e interacción.



Figura 8. ISO/IEC 9126-1 Calidad Interna y Externa junto a Calidad de Uso

2.9.2.2.1.1. Calidad Interna y Externa

Utiliza atributos medibles que incluyen en la calidad del software, se establecen cualidades de calidad interna y externa del software y subcategorías, y estas pueden ser medibles por sus capacidades en contenido del software.

Funcionalidad

Se describe como la capacidad de efectividad en las funciones establecidas de cumplimiento del software, y cubrir las necesidades de los usuarios, tiene cinco criterios:

- **Adecuación.** Es la capacidad del software de cumplir funciones específicas a un seleccionado grupo de usuarios.
- **Precisión.** es la capacidad del software para realizar procesos solicitados y obtener resultados precisos.
- **Interoperabilidad.** es la capacidad del software de poder interactuar con otros entornos de software.
- **Seguridad.** es la capacidad del software de protección a la información y accesos denegados.
- **Cumplimiento funcional.** es la capacidad del software en relación al cumplimiento de estándares de funcionalidad.

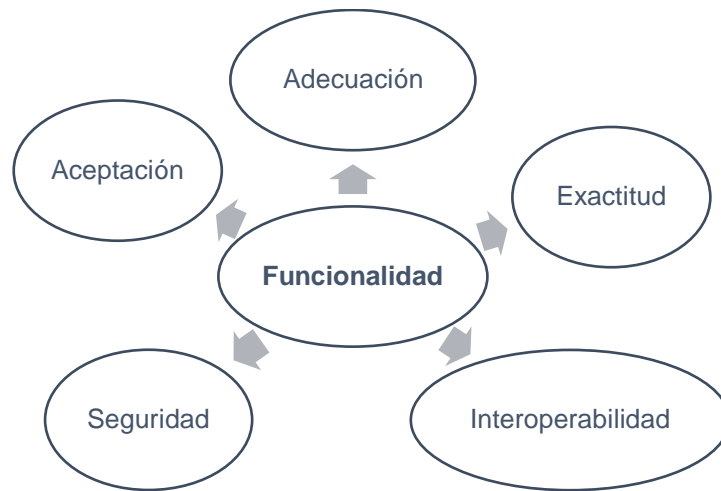


Figura 9. Calidad Interna y Externa - Funcionalidad

Confiabilidad

Es la confianza en el funcionamiento del software en cualquier área de análisis a evaluar su cumplimiento, tiene cuatro criterios:

- **Madurez.** Es la capacidad del software de solución a errores detectables.
- **Tolerancia a fallos.** Es la capacidad del software de estabilidad en su funcionamiento al detectar errores en su ejecución.
- **Recuperación.** Es la capacidad del software en no afectar su rendimiento y recuperación de datos al detectar errores en su ejecución.
- **Fiabilidad.** Es la capacidad del software en el cumplimiento con estándares de calidad.

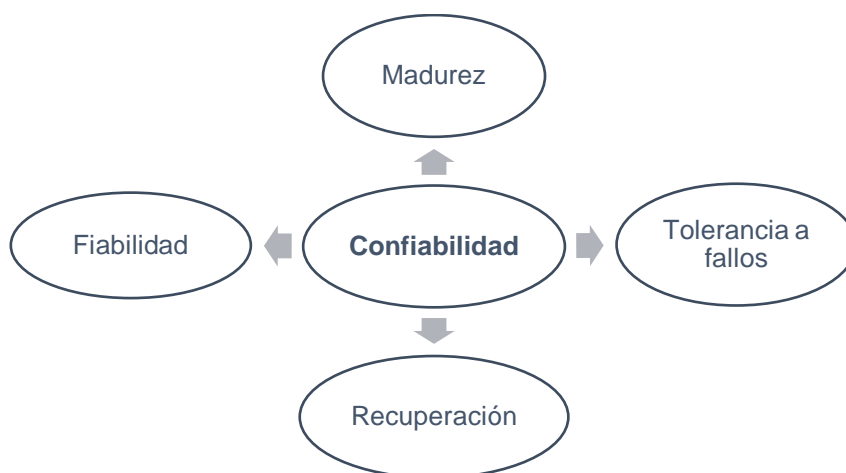


Figura 10. Calidad Interna y Externa – Confiabilidad

Usabilidad

Comprende a la medida de experiencia y la capacidad de ser entendido, comprendido y usado por el usuario final y los profesionales ingenieros y técnicos en su gestión, posee 2 criterios de evaluación:

- **Entendido.** Es la capacidad del software de ser fácil en su interacción con el usuario en su capacitación de uso.
- **Operación.** Es la capacidad del software que relaciona al usuario y los procesos de ejecución.



Figura 11. Calidad Interna y Externa – Usabilidad

Eficiencia

Es una característica muy importante en la evolución del producto software y comprende al desempeño adecuado y correcto analizado del software, tiene relación con los recursos necesarios con especificaciones establecidas por evaluación y posee dos criterios considerando su comportamiento:

- **Tiempo.** Es la capacidad del software en analizar la respuesta y procesamiento de funciones y procesos con condiciones establecidas.
- **Recursos.** Es la capacidad del software en usar solo los recursos necesarios al procesar funciones determinadas.

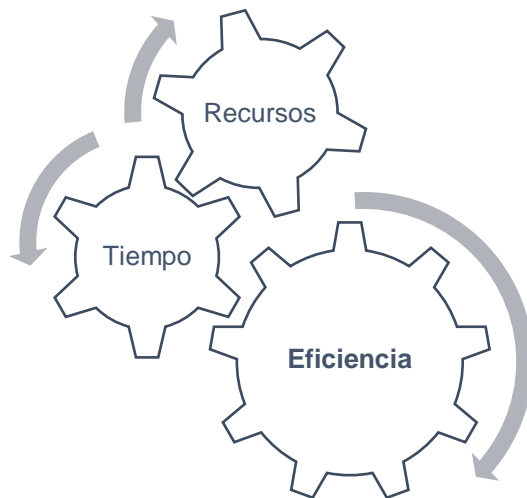


Figura 12. Calidad Interna y Externa – Eficiencia

Mantenibilidad

Se comprende a la facilidad de poder editar, modificar y corregir errores detectados en el software, proveer una mejora, documentación adecuada en información necesaria

para la modificación del software en el caso de ser necesario por peticiones de usuarios, posee cuatro criterios considerando su facilidad:

- **Análisis.** Es la capacidad del software para ser detectar fallos o errores y sus causas.
- **Estabilidad.** Es la capacidad del software en relación con riesgos y los efectos de correcciones previamente realizadas.
- **Cambio.** Es la capacidad del software en modificaciones para corcones de fallos o errores detectados.
- **Pruebas.** Es la capacidad del software para ser analizado a modificaciones y determinar su aprobación.

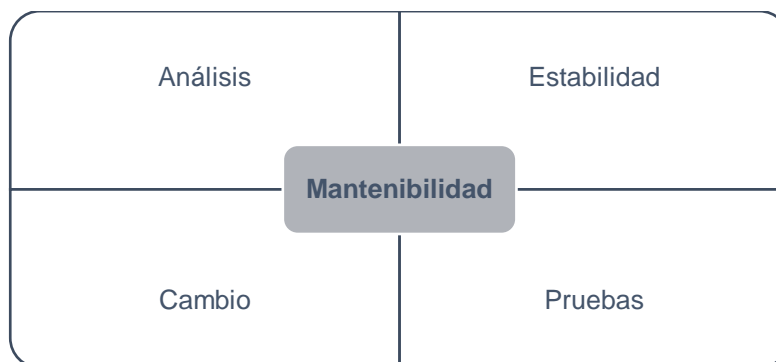


Figura 13. Calidad Interna y Externa – Mantenibilidad

Portabilidad

Se entiende a la capacidad del software de ser adaptado a otro entorno o ambiente, y su funcionamiento no sea afectado por su traslado, posee dos criterios de evaluación:

- **Adaptabilidad.** Es la capacidad del software para ser implantado en otro entorno o ambiente y no se vea afectado en su funcionamiento, no necesita de acciones adicionales para lograr su correcto funcionamiento en su transferencia.
- **Reemplazamiento.** Es la capacidad del software en poder ser reemplazado por otro software y cumplir el mismo propósito.

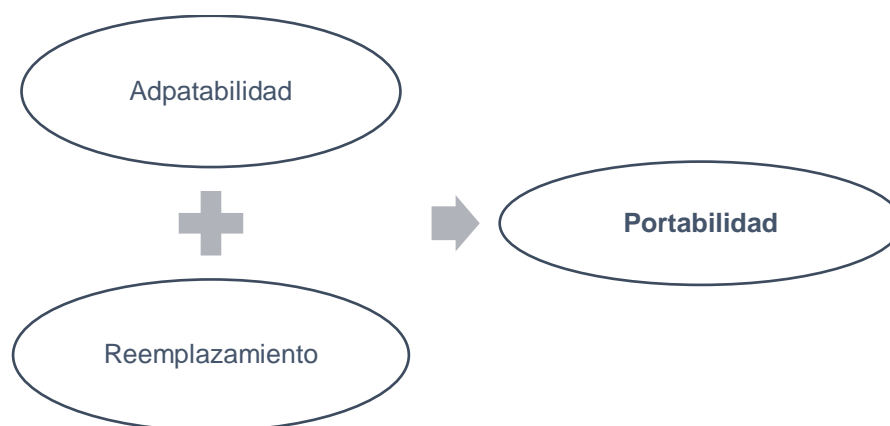


Figura 14. Calidad Interna y Externa – Portabilidad

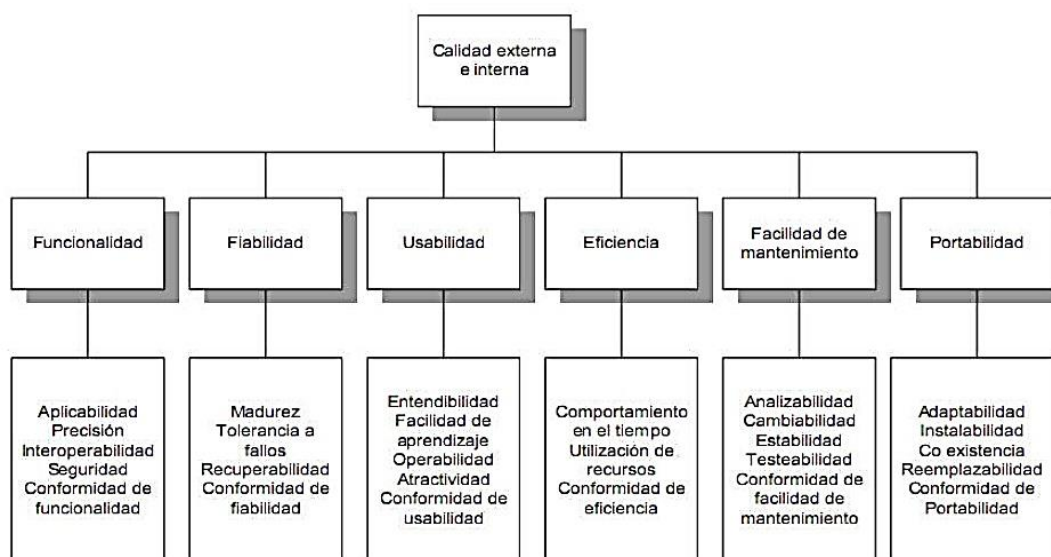


Figura 15. ISO/IEC 9126-1 Gestión del Modelo de Calidad del Software

2.9.2.2.1.2. Calidad en Uso

Utiliza atributos que miden la aceptación por parte del usuario final y su experiencia en el uso del software, posee cuatro atributos:

Eficacia. Relaciona el cumplimiento de los objetivos especificados por el software establecido en los requerimientos por parte del usuario final.

Productividad. Establece una relación de las tareas del usuario final con la medición en grado de rendimiento de cumplimiento esperado por el software.

Satisfacción. Es la capacidad del software en cumplir los propósitos del usuario final al ejecutar los procesos y funciones establecidas para su análisis.



Figura 16. ISO/IEC 9126-1 Calidad de Uso

2.9.2.2.2. ISO/IEC 9126-2 Métricas Externas

En esta familia de la ISO 9126 se puede hacer uso de las métricas consideradas en la evaluación, de esta manera se puede especificar más detalladamente métricas


propias a considerar en el estudio de herramientas de software, se debe clasificar y subclasificar las métricas dependiendo el caso de estudio a evaluar, dentro de la clasificación las métricas deben ser priorizadas dependiendo como se desea obtener los resultados más relevantes en la medición objetiva, a continuación se detalla cómo está estructurada la tabla de métricas:

Tabla 2.

ISO 9126-2 Tabla de Métricas de Evaluación del Producto Software

Tabla de Métricas de Evaluación del Producto Software

Detalle de la Métrica	Significado
Nombre	Nombre propio de la métrica.
Propósito	Se describe el motivo de selección de la métrica.
Método de aplicación	Se describe el perfil de la métrica en su aplicación
Medición y calculo	Se describe la forma de calcular y medición de métricas a utilizar.
Interpretación del valor medio	Se describe el rango y los valores a evaluar la métrica.
Tipo de escala	Se describe a la medición de asignar el valor a una variable de un elemento en observación.

CONTINÚA 


Tipo de media	Se describe el tipo de medida a utilizar en el análisis de la métrica en relación al tipo de escala definido.
Entradas de medición	Se describe los datos información utilizados para medir.
Referencia ISO/IEC 12207	Detalla la información a utilizar en evaluación de procesos de calidad del ciclo de vida del software y donde se puede considerar las métricas a medir.
Usuarios designados	Se describe y define a los usuarios escogidos para analizar las métricas seleccionadas.

Las métricas externas detalladas en la ISO 9126-2 nos permite categorizar en las evaluaciones a estudiar e identificar la calidad en los procesos de selección del producto software a seleccionar.


Tabla 3.
ISO/IEC 9126-2 Métricas Externas

ISO/IEC 9126-2 Métricas Externas


Categoría Principal	Subcategoría	Métrica
Métricas de Funcionalidad	Métricas de Adecuación	Adecuada funcionalidad
		Completa implementación funcional
		Implementación de cobertura funcional
		Especificación de estabilidad funcional
	Métricas de Exactitud	Expectativa de exactitud
		Exactitud computacional
		Precisión
	Métricas de Interoperabilidad	Intercambio de datos (Datos reseteados de la base)
		Intercambio de datos (Acceso de los usuarios a la base)
	Métricas de Seguridad de Acceso	Acceso auditable
Control de acceso		

CONTINÚA 

		Prevención de datos erróneos
	Métricas de Cumplimiento de Funcionalidad	Cumplimiento de la funcionalidad
		Cumplimiento de las normas de estandarización de interfaces
Métricas de Fiabilidad	Métricas de Madurez	Estimar el efecto de la densidad más reciente
		Defectos de densidad contra casos de pruebas
		Falla de densidad
		Falla removida
		Tiempo significativo entre fallas
		Prueba de cobertura
		Prueba de madurez
	Métricas de Tolerancia a fallos	Evitar bajas del producto software
		Evitar fracaso de procesos
		Evitar errores operacionales

CONTINÚA 

	Métricas de Capacidad de Recuperación	Disponibilidad Tiempo bajo de ejecución Tiempo medio de recuperación Restablecimiento Restauración Restauración efectiva
	Métricas de Cumplimiento de Fiabilidad	Cumplimiento de fiabilidad
	Métricas de Usabilidad	Métricas de Capacidad para ser Entendido
	Métricas de Capacidad para ser Aprendido	Fácil función de aprendizaje

CONTINÚA 

Métricas de Capacidad
para ser Operado

Fácil aprendizaje en tareas
de ejecución

Correcta Documentación
del software a personal
técnico

Correcta Documentación
del software a personal
usuarios

Ayuda de accesibilidad


Ayuda frecuente

Cumplimiento de
expectativas de operación
de los usuarios

Capacidad de control
Apropiada tarea de
operación


Guía de descripción
Errores tolerantes de
operación

Individualización apropiada
Interacción atractiva

CONTINÚA 

	Métricas de Capacidad de Atracción	Interfaz de apariencia personalizada
	Métricas de Cumplimiento de la Usabilidad	Cumplimiento de usabilidad
Métricas de Eficiencia	Métricas de Comportamiento Temporal	Tiempo de respuesta Transferencia del proceso Tiempo de cambio
	Métricas de Utilización de Recursos	Utilización de recursos de dispositivos de entrada y salida Utilización de recursos de memoria Utilización de recursos de transmisión
	Métricas de Cumplimiento de la Eficiencia	Cumplimiento de eficiencia
Métricas de Mantenibilidad	Métricas de Capacidad de ser Atendido	Capacidad para realizar auditorías Soporte en función de diagnóstico Capacidad de análisis de fallas

	Eficiencia de análisis de fallas
	Capacidad de estado de monitoreo
Métricas de Capacidad para ser Cambiado	Eficiencia en el ciclo de cambio
	Lapsos de tiempo en cambios de implementación
	Complejidad en la información
	Modificación de parámetros
	Capacidad de control en cambio de software
Métricas de Estabilidad	Proporción satisfactoria de cambio
	Localización de impacto de modificación
Métricas de Capacidad para ser Probado	Disponibilidad de la función incorporada de prueba
	Eficiencia de nueva prueba
	Prueba de restauración

CONTINÚA 

Métricas de Portabilidad	Métricas de Cumplimiento de Mantenibilidad	Cumplimiento de mantenibilidad
	Métricas de Adaptabilidad	Capacidad de adaptación de datos e información
		Capacidad de adaptación del hardware a un ambiente
		Capacidad de adaptación en un entorno
		Amigable al usuario
		Capacidad de adaptación a un ambiente de software
	Métricas de Instalabilidad	Fácil instalación
		Fácil configuración
	Métricas de Coexistencia	Coexistencia disponible
	Métricas de Capacidad para ser Reemplazado	Continuidad en el uso de datos
Integración de funciones		
Consistencia funcional en el soporte a usuarios		
Métricas de Cumplimiento de Portabilidad	Cumplimiento de portabilidad	

2.9.2.2.3. ISO/IEC 9126-3 Métricas Internas

Esta familia de la norma ISO/IEC 9126 nos permite conocer las métricas internas a evaluar en el producto software, es decir considera atributos internos, utilizan flujos y diagramas como representación gráfica de estado en resultados analizados, las métricas internas utilizan números y rangos para ser evaluados con el objetivo asegurar la calidad interna del producto software, a continuación, se plantea la categorización las métricas especificando la medición en uso:

Tabla 4.
ISO/IEC 9126-3 Métricas Internas

ISO/IEC 9126-3 Métricas Internas

Categoría	Métricas
Métricas de Funcionalidad	Métricas de Adecuación
	Métricas de Exactitud
	Métricas de Interoperabilidad
	Métricas de Seguridad
	Métricas de Cumplimiento de la Funcionalidad
Métricas de Fiabilidad	Métricas de Madurez
	Métricas de Tolerancia a Fallos
	Métricas de Capacidad de Recuperación
	Métricas de Cumplimiento de Fiabilidad
Métricas de Usabilidad	Métricas de Capacidad para ser Entendido

CONTINÚA 

	Métricas de Capacidad para ser Aprendido
	Métricas de Capacidad para ser Operado
	Métricas de Capacidad de Atracción
	Métricas de Cumplimiento de Usabilidad
Métricas de Eficiencia	Métricas de Comportamiento Temporal
	Métricas de Utilización de Recursos
	Métricas de Cumplimiento de Eficiencia
Métricas de Mantenibilidad	Métricas de Capacidad para ser Analizado
	Métricas de Capacidad para ser Cambiado
	Métricas de Estabilidad
	Métricas de Capacidad de ser Probado
Métricas de Portabilidad	Métricas de Adaptabilidad
	Métricas de Instalabilidad
	Métricas de Coexistencia
	Métricas de Capacidad para ser Reemplazado
	Métricas de Cumplimiento de Portabilidad

2.9.2.2.4. ISO/IEC 9126-4 Métricas de Calidad de Uso

Esta familia de la norma ISO/IEC 9126-4 permite describir las métricas de calidad de uso en relación a las experiencias por parte de los usuarios finales al producto software, efectividad en los procesos y requerimientos deseados, se basa en la seguridad

operacional, productividad en su ejecución y satisfacción por parte de los usuarios en las siguientes métricas de evaluación:

Tabla 5.
ISO/IEC 9126-4 Métricas de Calidad de Uso

ISO/IEC 9126-2 Métricas de Calidad de Uso

Categoría	Métricas
Efectividad	Eficacia en tarea
	Cumplimiento de tarea
	Frecuencia de error
Productividad	Tiempo de ejecución de tarea
	Eficiencia de tarea
	Productividad económica
	Proporción productiva
Seguridad	Respectiva eficiencia del usuario
	Seguridad del usuario
	Perjuicios económicos
	Daños del software
Satisfacción	Escala de satisfacción del usuario
	Cuestionario de satisfacción
	Uso discrecional

2.9.2.3. ISO/IEC 14598 Métodos de Valoración y Evaluación de la Calidad del Producto Software

Esta norma fue creada para crear un marco con procesos de evaluación para todo tipo de producto software finalizado o existente, al considerar la familia de la ISO 14598 se puede identificar seis etapas:

- **ISO/IEC 14598-1 Visión General**

Establece una relación entre el producto software, la calidad y el cumplimiento de todas las etapas de evaluación de la norma ISO 12598.

- **ISO/IEC 14598-2 Planificación y Gestión**

Contiene guías de soporte, definición de objetivos, políticas de la empresa, características de la tecnología, asignación de responsabilidades del software adquirido.

- **ISO/IEC 14598-3 Proceso de Desarrolladores**

Contiene indicadores que pueden predecir la calidad de un producto software final o ya desarrollado que va hacer adquirido al cumplimiento de requerimientos necesarios.

- **ISO/IEC 14598-4 Proceso de Comparadores**

Es utilizado por las organizaciones para comparar o rehusar los productos software que ya están desarrollados con el fin de ser aceptado por el comprador.

- **ISO/IEC 14598-5 Proceso de Evaluadores**

Contiene guías para evaluar el producto software considerando aspectos como si es imparcial y objetivo al adaptar en el cumplimiento de los requerimientos, un aspecto muy importante es considerar la necesidad de adquirir un producto

software ya desarrollado y no la necesidad de desarrollar un producto software propio e identifica la mejora continua en todos los procesos.

- **ISO/IEC 14598-6 Modulo de Evaluación**

Especifica el cumplimiento de la etapa del proceso de evaluadores, coordina un criterio que permite la toma de decisión considerando la calidad como calificación principal.



Figura 17. ISO/IEC 14598

Las herramientas de Ciberseguridad seleccionadas por el CSIRT deben cumplir con requisitos muy importantes que han sido calificados por estándares de calidad que nos pueden asegurar el cumplimiento en el desarrollo y resultado de su desarrollo, estos estándares nos permiten ver guías para comparaciones de productos software ya desarrollados, resaltando o considerando puntos más importantes en valor de acuerdo a los requerimientos necesarios por el CSIRT, la seguridad de información en su estandarización nos permite conocer el cumplimiento de las herramientas seleccionadas.

2.9.3. Normas de Anticorrupción y Ética

Son estándares que nos permiten garantizar las buenas prácticas profesionales enfocada en valores de honestidad y responsabilidad por tratar la corrupción como un riesgo que logra destruir la ética empresarial y las condiciones laborales de los recursos humanos.

2.9.3.1. ISO 37000: 37001

Es una norma internacional diseñada para ayudar a las organizaciones a implementar un sistema de gestión contra el soborno. Especifica una serie de medidas que su organización puede implementar para ayudar a prevenir, detectar y tratar el soborno.

El enfoque estructurado de ISO 37001 para identificar, evaluar, analizar y mitigar los riesgos de soborno con una comunicación, capacitación y procedimientos apropiados trae el modelo estandarizado utilizado por otros sistemas de gestión a este importante campo de riesgo empresarial.

Está desarrollada para ser integrada en los procesos de gestión y controles ya creados en la organización, se orienta a la estructura general de los sistemas de estandarización de la calidad y normas de sistemas de gestión, de esta manera se adapta de forma ágil con la norma ISO/IEC 900. Se divide en dos sectores por contratación:

- **Soborno por la organización**, su personal o socios comerciales para su propio beneficio.

- **Soborno de la organización**, su personal o socios comerciales en relación con sus actividades.

Esta norma es flexible y puede adaptarse para gestionar muchos tipos de sobornos lo que le permite adaptarse a una amplia gama de empresas, instituciones u organizaciones, incluyendo:

- Grandes empresas y organizaciones.
- Pequeñas y medianas empresas.
- Organizaciones públicas y sin ánimo de lucro.
- Organizaciones no gubernamentales (ONG) y organizaciones benéficas.

Los beneficios de un sistema de gestión anticorrupción certificado en ISO 37001 permite proteger y preservar la integridad de la organización mediante:

- La apertura de la organización al escrutinio externo de la eficacia de sus políticas y procesos contra el soborno.
- La demostración del cumplimiento de la legislación pertinente, como la Ley Antisoborno.
- La colaboración con las partes interesadas para supervisar y administrar el riesgo en toda la organización y la cadena de suministro.
- Asegurando que los proveedores, subcontratistas y agentes estén comprometidos con las mejores prácticas contra el soborno. (Institution, 2016).

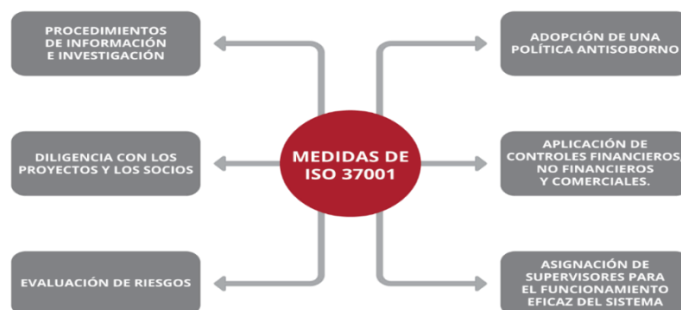


Figura 18. ISO 37000: 37001 Anticorrupción y Ética

Fuente: (Certification, 2018)

2.10. Priorización de Selección de Criterios de Evaluación

Utiliza métodos y herramientas para designar los criterios con mayor prioridad y puntuación en su análisis, considerando el área o categoría a la que pertenecen, generando un resultado cuantitativo, que permite conocer el grado de prioridad con respecto a todas las métricas a utilizar en el proyecto de consulta e investigación.

2.10.1. Matriz de Priorización de Holmes o Matriz de Impacto

Es una herramienta que permite la selección de opciones sobre la base de la ponderación y aplicación de criterios. Hace posible, determinar alternativas y los criterios a considerar para adoptar una decisión, clarificar problemas, oportunidades de mejora y proyectos. En general, establece prioridades entre un conjunto de elementos, para facilitar la toma de decisiones. La aplicación de la matriz de priorización conlleva un paso previo de determinación de las opciones sobre las que decidir, así como de identificación de criterios y de valoración del peso o ponderación que cada uno de ellos tendrá en la toma de decisiones. (Consultores, 2019)

Es una matriz compuesta por filas y columnas, en la parte superior se coloca el área o característica principal a la que pertenece todos los criterios a evaluar, se colocan todos los criterios en las celdas superiores y de lado izquierdo, de esta manera se forma una diagonal en la matriz que permite comparar todos los criterios entre ellos, en la parte derecha, se colocan los totales como resultado matemático de la sumatoria total y ponderación de los criterios a evaluar, como se muestra en la siguiente tabla.

Tabla 6.
Matriz de Priorización de Holmes o Matriz de Impacto

Característica	Criterio	Criterio	Criterio	Criterio	Total	Ponderación
	1	2	3	n		del Criterio
Criterio 1						%
Criterio 2						%
Criterio 3						%
Criterio n						%
TOTALES						1,00

3. CAPITULO III

Modelo de Selección de Herramientas de Ciberseguridad

3.1. Introducción

En este capítulo se plantea el desarrollo del modelo de análisis y selección, mediante la definición de etapas y actividades, relacionando criterios de ciberseguridad y métricas de evaluación y selección, además se identifica el análisis de la situación actual en la cual interviene la descripción de requerimientos del CSIRT, para el cumplimiento de las funciones definidas. Estos criterios de evaluación y selección están basados en estándares y buenas prácticas, como la norma ISO/IEC 9621 para establecer un modelo de calidad, y la norma ISO/IEC 14598 para la aplicación de la evaluación, este modelo se aplicará a un conjunto de herramientas obtenidas mediante un estudio preliminar de las ofertas en el mercado, con la finalidad de efectivizar los objetivos de seguridad y formación, establecidos en la creación el CSIRT académico, cumpliendo de manera correcta las actividades definidas.

El resultado esperado, es contar con una secuencia de actividades reguladas que permitan orientar en la labor de selección de las herramientas de Ciberseguridad, generando estrategias para la toma de decisiones en la selección, esto permite optimizar tiempo y recursos, en la implantación de las herramientas seleccionadas, ya que una mala elección puede producir pérdidas para la organización, puesto que esta invierte tiempo y recursos en este proceso.

3.2. Definición de los Procesos de Evaluación

El proceso de selección del software a utilizarse, requiere de tres aspectos importantes, los cuales permitirán obtener un resultado en función de las necesidades del CSIRT académico, estos aspectos son:

1. Justificación de la adquisición
2. Proceso de evaluación
3. Análisis y selección

En la justificación de la adquisición se plantean las actividades en base de la norma ISO 37000, con el objetivo de garantizar un proceso transparente, evitando la corrupción y soborno que permitirá obtener resultados óptimos en el proceso de selección.

Posteriormente en el proceso de evaluación, se tomará en cuenta a los modelos de calidad para establecer las características de calidad relacionadas con la efectividad y acoplamiento del producto software seleccionado en la realización de las actividades del CSIRT.

En la actualidad, se han propuesto varios modelos de evaluación de la calidad del software como el Modelo de McCall, Modelo de Boehm, Modelos ad-hoc y Normas ISO, para la evaluación de productos software, de las cuales se ha tratado en el capítulo anterior.

La propuesta del modelo para la selección de herramientas de ciberseguridad se basa en los principales parámetros de la Norma ISO/IEC 14598-5, ya que trata específicamente del proceso de evaluación de productos software, con la finalidad de

obtener resultados que aporten a la toma de decisiones en la elección del producto software a implantarse.

Adicionalmente, la Norma ISO 9126 proporciona un conjunto de métricas a evaluarse sobre el producto software, la norma ISO/IEC 14698-5 proporciona el procedimiento de evaluación, y la norma ISO 9162 proporciona los criterios de evaluación.

Finalmente, en el análisis de los resultados, los datos encontrados permiten comparar entre las herramientas, ¿Cuál es la más acertada?, y tomar una correcta decisión que garantiza que se va a cubrir de manera más eficiente las necesidades planteadas al adquirir el producto software o herramientas de ciberseguridad, en la siguiente imagen se presenta de forma organizada los procesos del modelo de análisis y selección propuesto.

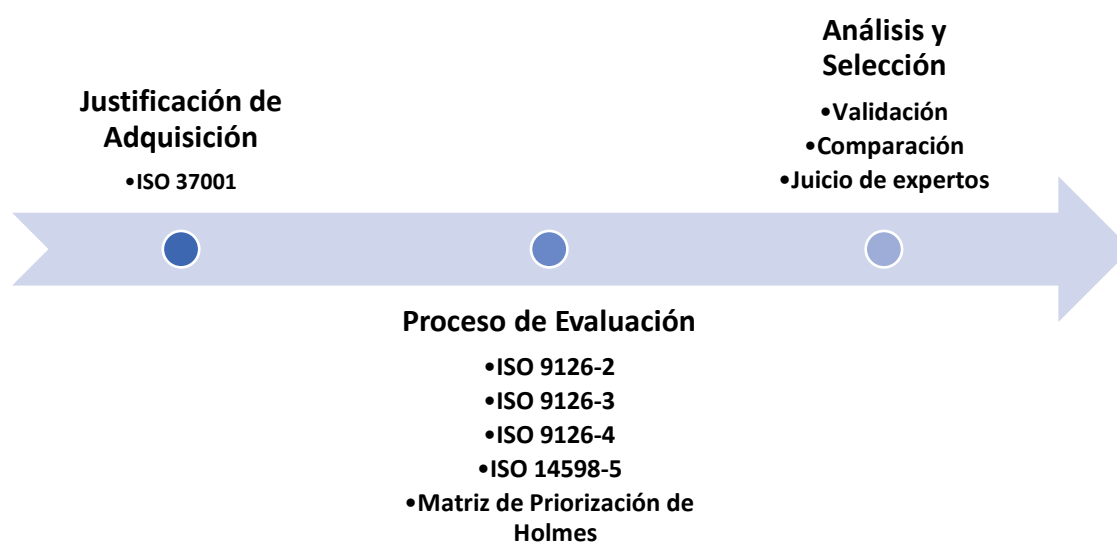


Figura 19. Proceso de Selección de Herramientas de Ciberseguridad para el CSIRT Académico ESPE

3.3. Justificación la Adquisición (ISO 37001)

Es muy importante de forma inicial, el justificar la solicitud de una herramienta por parte de CSIRT, ¿Por qué se debe adquirir una herramienta de software? En esta etapa se aclara de manera muy detallada, tomando en cuenta de manera interna las funciones y roles del CSIRT, es decir cada miembro del CSIRT debe limitarse a la solicitud de las herramientas en base a sus propias funciones y áreas de responsabilidad, así como tomar muy en cuenta de manera externa al CSIRT, y el valor económico limitado de inversión.

La necesidad de adquirir una herramienta de ciberseguridad debe ser rentable para el CSIRT, apoyando a procesos de seguridad y creando valor en conocimiento de adquisición, la implementación de una herramienta requiere contar con soluciones en un tiempo determinado.

Previamente identificados los requerimientos solicitados para la adquisición en base a una necesidad por cumplimiento de funciones y soluciones de seguridad del CSIRT, se requiere a validar los requisitos, de esta manera se verifica, que la solicitud de implementar la herramienta o herramientas tiene un respaldo justificado y necesario por solicitar.

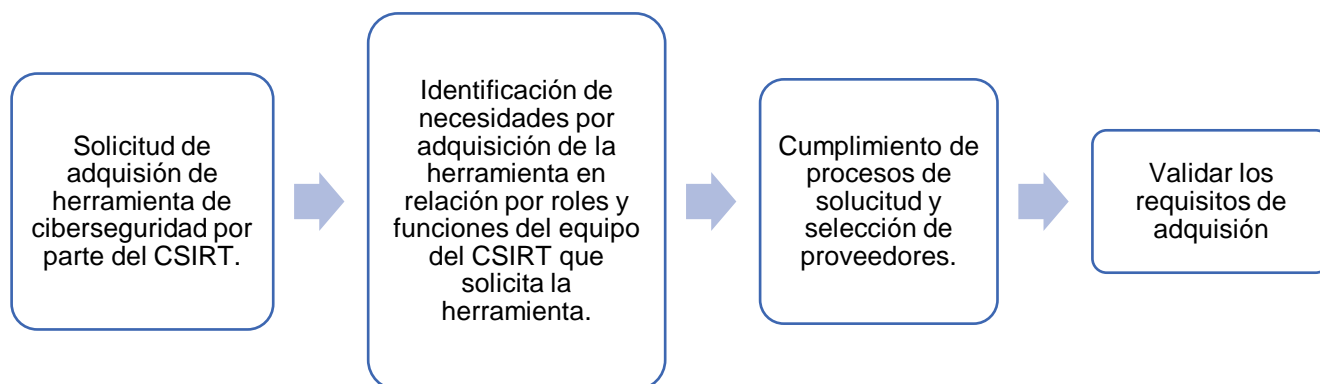


Figura 20. Procesos de Justificación ISO 37001 - CSIRT

3.4. Proceso de Evaluación

En base a la norma ISO/IEC 14698-5, se establece un proceso que cuenta con una serie de actividades que permiten llevar a cabo la evaluación del producto, este proceso se ilustra a continuación:

1. Establecimiento de los requerimientos
2. Especificación de la evaluación
3. Diseño de la evaluación
4. Ejecución de la evaluación
5. Conclusión de la evaluación

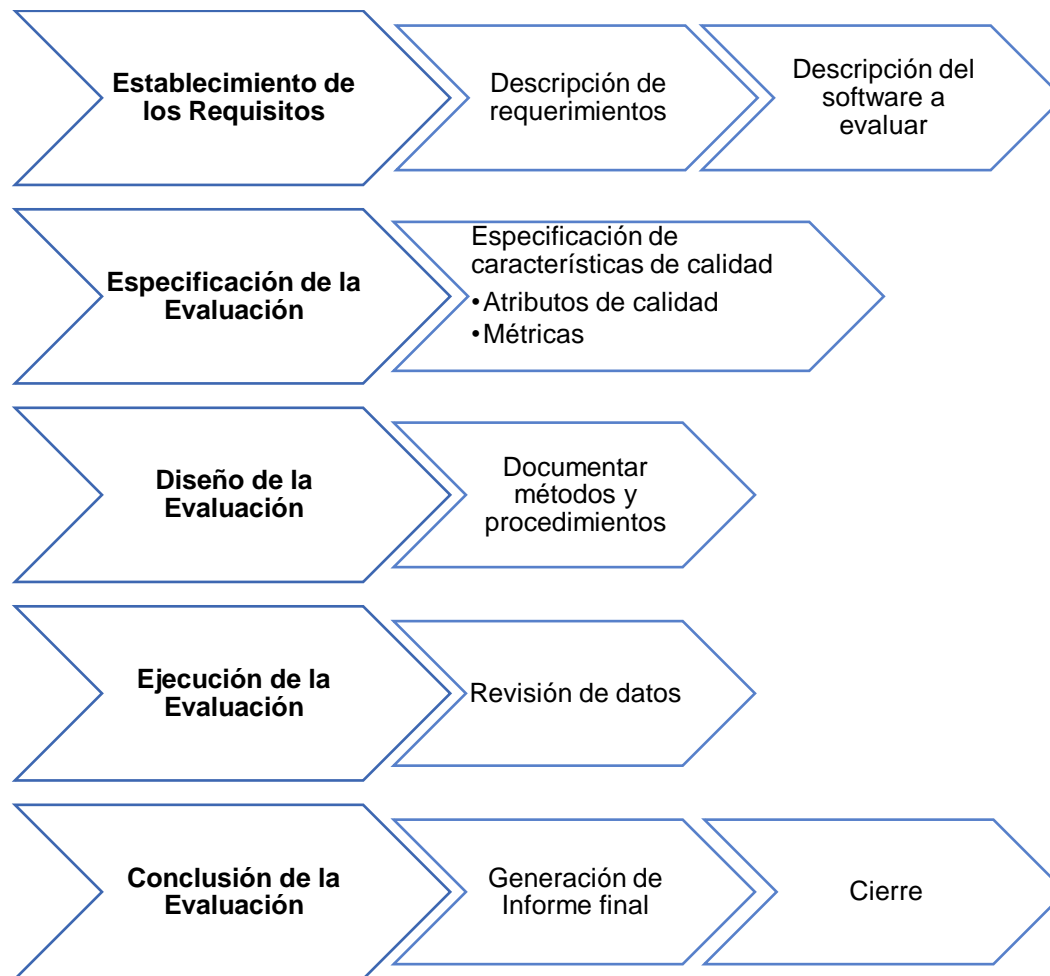


Figura 21. Actividades del Proceso de Evaluación

Fuente: ISO/IEC 14598-5

3.4.1 Establecimiento de los requerimientos

3.4.1.1 Describir los Requerimientos

Para el establecimiento de los requerimientos, se cuenta esencialmente con la definición de las actividades que va a realizar el CSIRT Académico, estas se encuentran categorizadas por función o servicio, cumplen con un rol determinado dependiendo de su naturaleza.

La descripción de los requerimientos está en base a las actividades definidas, se establecen las necesidades que deben solventar las herramientas seleccionadas, los servicios que requieren la utilización de herramientas son:



Figura 22. Clasificación de servicios de un CSIRT

La definición de las actividades a llevarse a cabo en el CSIRT, permiten detallar los requerimientos funcionales (explícitos) y no funcionales (implícitos).

Para obtener criterios de evaluación más objetivos, se los han clasificado en función de la naturaleza de los requerimientos a evaluarse, aplicada al contexto de un CSIRT académico y basándose en la norma ISO 9126, teniendo requerimientos funcionales y requerimientos no funcionales.

3.4.1.1.1. Requerimientos Funcionales

Se obtienen mediante la definición de tareas realizadas en el CSIRT, clasificándose en:

Funcionalidad

Se realiza un análisis de los servicios o funciones que proporciona el CSIRT, evaluando la adecuación funcional en base a su descripción:

Servicios Reactivos

Alertas y advertencias

Se requiere la funcionalidad que permita detectar una intrusión de seguridad de la información o vulnerabilidad, que además proporcione una recomendación de solución y mitigación.

Se debe proporcionar de un aviso o advertencia de manera oportuna por varios canales, que permita tomar acciones adecuadas, tomando en cuenta las recomendaciones otorgadas por la herramienta.

Manejo de incidentes

Se requiere una herramienta que proporcione la facilidad en el tratamiento de incidentes o casos, mediante la organización de estos por responsable, tipo de incidente y otros aspectos, como la visualización de pizarras, seguimiento de la evolución de la incidencia y su resolución, reportes de incidentes, entre otras características que permitan coordinar de manera óptima esta actividad.

Manejo de vulnerabilidades

Para esta actividad se plantea el requerimiento de herramientas, que mediante una auditoría técnica de la infraestructura de TI, permitan realizar:

- Análisis de vulnerabilidades
- Acción ante las vulnerabilidades

Con el propósito de coordinar el manejo de la información de vulnerabilidades halladas y la recomendación para su resolución

Manejo de artefacto (Artifacts)

En esta actividad se requieren herramientas que permitan realizar un tratamiento a los objetos implicados en un ataque o intrusión previamente ocurrida, para realizar un análisis que permita conocer su objetivo, y así prevenir futuros ataques con este mismo artefacto.

Servicios Proactivos

Anuncios

Se requieren herramientas que permitan la divulgación de información de nuevas intrusiones y vulnerabilidades halladas.

Monitoreo continuo

Es importante que la herramienta a seleccionarse cuente con la funcionalidad de monitoreo continuo, ya que es esencial detectar una intrusión o incidente de ciberseguridad en tiempo real, con el fin de tomar acciones inmediatas y oportunas para evitar que el impacto del riesgo tenga mayor afectación.

Auditoría de seguridad / Pentest.

Esta actividad se realiza con la finalidad de tener un conocimiento de las vulnerabilidades en la organización, permitiendo obtener acciones correctivas. Por esta razón es indispensable contar con una herramienta que permita realizar este análisis de manera eficiente, escaneando puertos, redes, aplicaciones e infraestructura de TI.

Además, se definen características muy importantes que se requieren en la implementación de herramientas de ciberseguridad en un CSIRT académico, tomando en cuenta las siguientes características:

Usabilidad

Es un aspecto fundamental, debido a que se plantean criterios que evalúan la facilidad de aprendizaje y facilidad de operación.

Portabilidad

Permite evaluar los aspectos que son importantes en la implementación de las herramientas, toma en cuenta la adaptabilidad, facilidad de instalación y coexistencia.

Posteriormente es importante en este punto establecer criterios que permitan evaluar, la cantidad de recursos disponibles, específicamente el presupuesto con el que cuenta la organización para la adquisición e implementación de las herramientas en el CSIRT.

3.4.1.1.2. Requerimientos No Funcionales

Los requerimientos no funcionales no están descritos de manera explícita, sin embargo, es importante tomar en cuenta, debido a que de ellos depende la calidad del producto que se va a elegir. Para el caso de las herramientas de ciberseguridad, se ha planteado tres características fundamentales que deben cumplir y estas son:

Fiabilidad

Esta característica provee criterios de madurez del producto software o herramienta, tomando en cuenta la densidad de fallos o falsos positivos.

Eficiencia

Permite evaluar el comportamiento y la capacidad del software, midiendo el tiempo de respuesta y tiempo medio de rendimiento, tomando en cuenta accesos simultáneos y solicitudes.

Seguridad

Toma en cuenta aspectos intrínsecos, como la otorgación de roles, autenticación y accesos.

Dada la descripción de los requerimientos y asociándolas con las características de la calidad del software a tomarse en cuenta en el proceso de evaluación, se obtiene las siguientes características:



Figura 23. Clasificación de Características de la Calidad del Software de Ciberseguridad

3.4.2 Describir el Producto Software a Evaluar

Los productos software a evaluarse son herramientas de ciberseguridad, cuyo propósito es la implementación, uso y aprendizaje en un CSIRT académico, tomando en cuenta la clasificación del producto software, se realiza el análisis correspondiente para

identificar su naturaleza. Según la norma ISO 14598, la clasificación del producto software está dada por: software base, software utilitario y software de aplicación.

Los productos software a evaluarse en este proceso, son herramientas cuyas funcionalidades se relacionan con la ciberseguridad y brindan facilidad a la administración de las actividades realizadas en un CSIRT académico.

Las plataformas o productos software deberán poseer las funcionalidades especificadas a continuación:



Software Utilitario	Software de Aplicación
	
<input type="checkbox"/> Escáneres de puerto	<input type="checkbox"/> Herramientas de monitoreo
<input type="checkbox"/> Escáneres de vulnerabilidad	<input type="checkbox"/> Sistema de inteligencia de amenazas cibernéticas
<input type="checkbox"/> Herramientas de alertas, advertencias y anuncios	<input type="checkbox"/> Advertencias y avisos
<input type="checkbox"/> Herramientas Forenses	
<input type="checkbox"/> Plataformas HoneyNet	

Figura 24. Clasificación de Funcionalidades por Tipo de Software

El producto software seleccionado, deberá cumplir con la cobertura de las funcionalidades requeridas, en el más alto porcentaje posible, ya que de esto dependerá el correcto desenvolvimiento de las actividades cotidianas del CSIRT académico.

Tomando en cuenta la clasificación de las herramientas o requerimientos establecidos por el CSIRT, se prevé un mejor análisis enfocado principalmente en las características de calidad, que garanticen que se cumplan con las expectativas para la realización de las actividades en el CSIRT.

Al relacionar las actividades con la que se han determinado los requerimientos funcionales, con las herramientas o software a ser evaluado, se obtiene la siguiente clasificación:

Servicios Reactivos



- Alertas y Advertencias**
 - Herramientas de alertas, advertencias y anuncios
- Manejo de incidentes
 - Herramientas de gestión de incidentes
- Manejo de la vulnerabilidad
 - Escáneres de puertos
 - Escáneres de vulnerabilidad
- Manejo de artefactos
 - Herramientas Forenses

Servicios Proactivos



- Anuncios**
 - Herramientas de alertas, advertencias y anuncios
- Monitoreo continuo
 - Herramientas de monitoreo
 - Plataformas HoneyNET
 - Sistema de inteligencia de amenazas cibernéticas
- Auditorias de Seguridad / Pentests
 - Herramientas Forenses

Figura 25. Clasificación de funcionalidades por servicio del CSIRT

Se debe tomar en cuenta que un producto software puede abarcar varias funcionalidades requeridas, las cuales deberá evaluarse independientemente.

3.4.3 Especificación de la evaluación

3.4.3.1 Definición de las características de calidad

Las aplicaciones a ser evaluadas se categorizan como producto final, en base al ciclo de vida de la norma ISO/IEC 14598-1, comprenden un conjunto de aplicaciones que realizan una determinada función relacionada con la ciberseguridad, como también aplicaciones especializadas en la gestión de CSIRT.

El objetivo de la evaluación, es verificar que estas aplicaciones cumplan con los requerimientos establecidos de manera óptima en función de las necesidades y recursos establecidos.


Dentro de estas funciones, se tiene aplicaciones de escritorio, aplicaciones web, aplicaciones de consola, entre otras, que pueden ser software libre o propietario.

Siguiendo el marco referencial proporcionado por la norma ISO/IEC 9126-2, 9126-3, en la cual se establece las características internas y externas de calidad de un producto software, y en base a la naturaleza del producto software a evaluar, se plantean los siguientes atributos de calidad que se han seleccionado:


Tabla 7.

Características de calidad para aplicaciones de Ciberseguridad


Características	Subcaracterísticas	Observación
Funcionalidad	<ul style="list-style-type: none"> • Cumplimiento funcional • Precisión 	Se analiza el cumplimiento de los requerimientos detallados a través de

CONTINÚA 

		las actividades realizadas en el CSIRT.
Usabilidad	<ul style="list-style-type: none"> • Facilidad de aprendizaje • Facilidad de uso u operación 	Se evalúa si la aplicación permite al usuario tener una curva de aprendizaje corta y asistida por documentación y por el proveedor
Fiabilidad	<ul style="list-style-type: none"> • Madurez 	Permite establecer si la herramienta de ciberseguridad proporciona resultados reales y permite medir la tasa de fallo que esta tiene. Los falsos positivos darán más trabajo al analizar los resultados obtenidos
Eficiencia	<ul style="list-style-type: none"> • Rendimiento • Utilización de recursos 	Se mide el tiempo y recursos que la

CONTINÚA 

		herramienta de ciberseguridad toma en realizar una determinada actividad.
Seguridad	<ul style="list-style-type: none"> • Cumplimiento con parámetros de seguridad en acceso. • Cumplimiento con administración de privilegios de usuarios de acuerdo a roles y funciones. 	Otorga una medición para verificar si la aplicación cumple con los parámetros de seguridad de acceso y visualización de información requeridos.
Portabilidad	<ul style="list-style-type: none"> • Adaptabilidad • Facilidad de implantación • Coexistencia 	La infraestructura de TI monitoreada por el CSIRT puede ser variante, en cuanto a la tecnología usada y otros aspectos, por esta razón es indispensable que las herramientas sean adaptables y

CONTINÚA 

además puedan
coexistir entre sí.

3.4.3.2 Selección de Métricas de Calidad para la Evaluación de una Herramienta de Ciberseguridad

Las métricas de evaluación, permiten obtener una medición cuantitativa de los atributos de calidad que se determinen. Estas métricas se seleccionan en función de las características o funcionalidades que requiere el CSIRT académico para cumplir con sus funciones, tomando en cuenta las características y atributos de calidad seleccionados para el contexto de herramientas de ciberseguridad.

Para la selección de las métricas es importante analizar los aspectos que se deben tomar en cuenta en la selección de una aplicación, que está destinada al cumplimiento de una actividad en el CSIRT académico, teniendo los siguientes propósitos de evaluación:

Funcionalidad:

- ¿La aplicación cumple con el mínimo requerido funcional descrito en las actividades que va a realizar?

Usabilidad:

- ¿El software es intuitivo y fácil de operar para usuarios nuevos?
- ¿El nivel de complejidad de las tareas toma un tiempo y esfuerzo elevado en función del dominio básico del usuario?

- ¿Se cuenta con información como manuales, tutoriales acerca del uso de la aplicación?
- ¿El proveedor facilita capacitación continua y soporte en el proceso de aprendizaje?

Fiabilidad

- ¿El número de falsos positivos es aceptable?
- ¿Existe coherencia en el número de falsos positivos obtenidos en diferentes pruebas?
- ¿El software identifica el mayor número de vulnerabilidades existentes?

Eficiencia

- ¿La herramienta de ciberseguridad responde en el tiempo esperado?
- ¿Los recursos requeridos por la herramienta de Ciberseguridad son proporcionales a la actividad realizada?

Seguridad

- ¿La herramienta de ciberseguridad cuenta con mecanismos de autenticación de acuerdo a la actividad a realizarse?
- ¿Se cuenta con roles definidos de acuerdo al perfil del miembro del CSIRT al realizar pruebas y gestión de incidentes?

Portabilidad

- ¿La aplicación es multiplataforma?

- ¿La aplicación brinda servicios que permiten la comunicación con otras aplicaciones?
- ¿El proceso de instalación cuenta con documentación o asistencia del proveedor?

3.4.3.3 Niveles de Calificación de Evaluación

En base a la norma ISO/IEC 14598-1 en evaluación de métricas, se considera en una escala de rango de cero (0) a diez (10), tomando en cuenta los siguientes aspectos:

- **Niveles de evaluación:**

Son los valores de análisis cualitativo que permite considerar si la métrica puede ser:

- Inaceptable. No cumple con ningún objetivo de análisis, su rango de evaluación es $0 \leq \text{valor} < 3$.
- Mínimamente aceptable. Cumple con algunos objetivos de análisis, considerando como aceptable o no aceptable, su rango de evaluación es $3 \leq \text{valor} < 5$.
- Aceptable. Logra cumplir el objetivo de análisis, su rango de evaluación es $5 \leq \text{valor} < 9$.
- Excede los objetivos. Sobrepasa el cumplimiento de objetivos de análisis, su rango de evaluación es $9 \leq \text{valor} \leq 10$.

- **Escala de medición:**

Es un rango milimetrado que permite considerar los segmentos de análisis.

- **Nivel de puntuación:**

Son parámetros de evaluación que permite concluir de forma cualitativa si satisface o no el cumplimiento de objetivos.

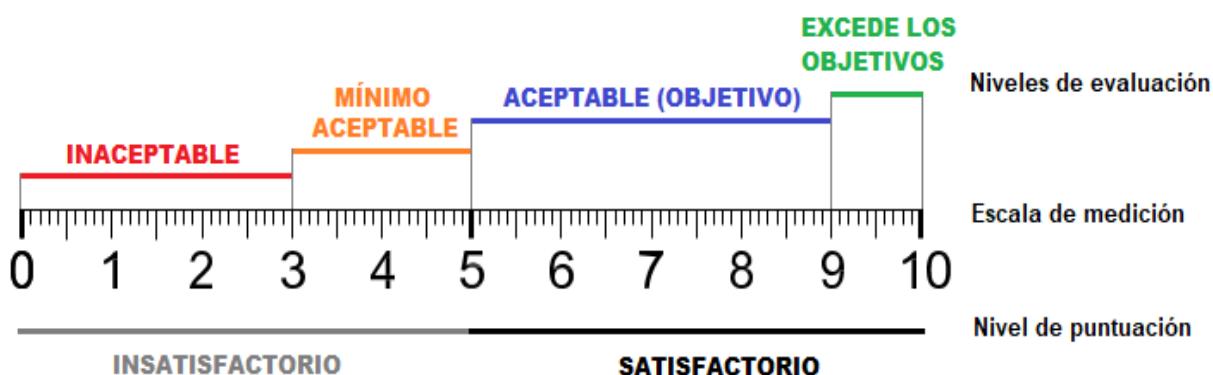


Figura 26. Niveles de Calificación de Evaluación

3.4.3.4 Desarrollo de la Matriz de Evaluación

Con la utilización de la matriz de priorización de Holmes, se puede obtener criterios de evaluación y el coeficiente de ponderación, considerando las características y subcaracterísticas de la calidad del software analizado y estudiado en este proyecto y mencionadas en los capítulos anteriores, con estos criterios se puede comparar todas las características entre todas, de esta manera no se olvida de tomar en cuenta a ninguna característica en su evaluación.

Obtención del Coeficiente de Ponderación

Es un valor numérico que forma parte de un ciento por ciento del total, este valor permite considerar el valor por medida porcentual de prioridad de una característica analizada con respecto a todas las características.

Desarrollo

Establecidos y analizados las características de evaluación de la calidad del software en relación con criterios de ciberseguridad, se obtiene las siguientes características:

- Funcionalidad
- Usabilidad
- Fiabilidad
- Eficiencia
- Seguridad
- Portabilidad

Se utiliza la matriz de Priorización de Holmes o de Impacto, para ingresar las características de calidad de software, los valores ingresados son analizados con un enfoque de orientación a productos software de herramientas de ciberseguridad, los criterios son analizados de manera organizada, relacionado todos contra todos, de esta manera se realiza la comparación por valor de priorización y característica a evaluar, como resultado se obtiene el coeficiente de ponderación por característica, representado en porcentaje (%), cómo se representa en la siguiente tabla:

Tabla 8.*Matriz de Priorización de Características de Herramientas de Ciberseguridad y Coeficiente de Ponderación*

Característica	Funcionalidad	Usabilidad	Fiabilidad	Eficiencia	Seguridad	Portabilidad	Total	Coeficiente de Ponderación
Funcionalidad	1	1	0	1	1	1	5	23,81%
Usabilidad	0	1	0	0	0	0	1	4,76%
Fiabilidad	1	1	1	1	1	1	6	28,57%
Eficiencia	0	1	0	1	0	1	3	14,29%
Seguridad	0	1	0	1	1	1	4	19,05%
Portabilidad	0	1	0	0	0	1	2	9,52%
TOTALES							21	100%

En el desarrollo de la matriz de priorización o impacto, se tomaron en cuenta aspectos que involucran necesariamente a herramientas de ciberseguridad, como productos softwares desarrollados, partiendo de este criterio y de las características seleccionadas en la evaluación se puede definir que:

La funcionalidad tiene mayor prioridad que la usabilidad, considerando que la funcionalidad debe cumplir en mayor porcentaje los requerimientos del CSIRT-ESPE, relacionado con las funciones que este posee, la usabilidad se lo puede tratar con capacitaciones al equipo responsable de CSIRT-ESPE, por parte del proveedor de la herramienta seleccionada, o puede contener información documentada de su uso en sus manuales.

La funcionalidad tiene menor grado de prioridad que la fiabilidad, considerando que la fiabilidad debe proporcionar resultados reales que permiten al CSIRT-ESPE tomar decisiones correctas con la utilización de las herramientas de ciberseguridad en los resultados obtenidos con las diferentes utilidades, en cumplimiento de sus funciones.

La funcionalidad tiene mayor grado de prioridad que la eficiencia, considerando que el cumplimiento de sus funciones y servicios, generan mayor satisfacción por parte del CSIRT-ESPE en la iteración con las herramientas, la eficiencia conlleva a obtener resultados correctos sin priorizar el tiempo y uso de recursos hardware propios de cada herramienta.

La funcionalidad tiene mayor grado de priorización que la seguridad ya que el cumplimiento de las funciones, genera mejores resultados, la seguridad se la puede reemplazar con utilización de políticas propias de seguridad por parte del CSIRT-ESPE.

La funcionalidad tiene mayor grado de prioridad que la portabilidad considerando el cumplimiento de funciones operativas muy importantes para el CSIRT-ESPE, la portabilidad se puede tratar con la utilización de diferentes herramientas que permitan la coexistencia en su entorno de infraestructura o área de tecnología.

La usabilidad tiene menor grado de priorización que la fiabilidad, ya que la fiabilidad genera resultados reales y correctos y esto conlleva que el CSIRT-ESPE pueda realizar sus funciones con datos e información real, la usabilidad se la puede tratar con capacitaciones y lectura de documentación por parte de la herramienta utilizada.

La usabilidad tiene menor grado de priorización que la eficiencia, ya que la eficiencia genera una mayor optimización de tiempo y recursos en la ejecución de funciones y esto permite al CSIRT-ESPE tratar sus funciones con mayor efectividad, la usabilidad se la puede tratar con capacitaciones propias o por parte del proveedor.

La usabilidad tiene menor grado de priorización que la seguridad, ya que la seguridad es muy importante al proteger la información de accesos y privilegios a diferentes roles o responsabilidades del personal o equipo del CSIRT-ESPE.

La usabilidad tiene menor grado de priorización que la portabilidad, ya que la portabilidad es muy esencial al adaptar a diferentes entornos de análisis por parte del

CSIRT-ESPE en la infraestructura tecnológica de la Universidad de las Fuerzas Armadas ESPE.

La fiabilidad es la característica con mayor prioridad que las restantes, ya que la credibilidad de la información obtenida, no puede ser reemplazada por ninguna otra característica, esto permite al CSIRT-ESPE obtener y gestionar resultados verídicos.

La seguridad tiene mayor prioridad que la eficiencia, ya que la seguridad considera accesos seguros por cada responsable del CSIRT-ESPE, la eficiencia obtiene resultados equitativos en tiempos diferentes y con el uso de recursos diferentes, que pueden ser tratados con medición.


La eficiencia tiene mayor grado de priorización que la portabilidad, ya que la eficiencia es más importante para el CSIRT-ESPE con la optimización de tiempo y recursos, la portabilidad puede ser tratada con el uso de diferentes herramientas y observando la validez de su coexistencia.

La seguridad tiene mayor grado de priorización que la portabilidad, ya que la seguridad comprende mayor confianza de accesos correctos a las diferentes funcionalidades de la herramienta por responsabilidades asignadas al CSIRT-ESPE, la portabilidad se la puede tratar con la implementación de diferentes herramientas con funciones similares.

Todos los criterios anteriormente mencionados son tomados en cuenta específicamente para herramientas de ciberseguridad en relación con el análisis de funciones del CSIRT-ESPE, obteniendo como resultado la siguiente tabla:

Tabla 9.*Propuesta de Métricas de Evaluación y Coeficiente de Ponderación***Métricas de Evaluación con Coeficiente de Ponderación**

Características	Subcaracterísticas	Métrica	Tipo de Métrica	Coeficiente de Ponderación (%)
Funcionalidad	<ul style="list-style-type: none"> Cumplimiento Funcional 	<ul style="list-style-type: none"> Cumplimiento de la funcionalidad 	Externa	23,81%
Usabilidad	<ul style="list-style-type: none"> Facilidad de Aprendizaje Facilidad de uso u operación 	<ul style="list-style-type: none"> Fácil función de aprendizaje Consistencia operacional de uso 	Externa	4,76%
Fiabilidad	<ul style="list-style-type: none"> Madurez 	<ul style="list-style-type: none"> Falsos positivos 	Externa	28,57%
Eficiencia	<ul style="list-style-type: none"> Comportamiento temporal 	<ul style="list-style-type: none"> Tiempo de respuesta Consumo de recursos (CPU, Memoria y almacenamiento) 	Externa	14,29%

CONTINÚA 

Seguridad	<ul style="list-style-type: none">• Utilización de recursos• Métodos de autenticación	<ul style="list-style-type: none">• Cumplimiento con seguridad de acceso	Externa	19,05%
Portabilidad	<ul style="list-style-type: none">• Adaptabilidad• Coexistencia	<ul style="list-style-type: none">• Facilidad de implantación• Grado de coexistencia	Externa	9,52%

En función de los propósitos identificados se puede detallar el conjunto de métricas, clasificadas por características y subcaracterísticas de calidad basadas en la norma ISO 9126-2 y 9126-3.

Las métricas detalladas se enfocan en la calidad externa de las herramientas de software utilizadas para la realización de las actividades planificadas en un CSIRT académico, estas métricas tendrán como resultado valoraciones que servirán para la toma de decisiones en la elección de herramientas a utilizarse.

3.4.3.5 Especificación de Las Métricas a Utilizarse

Se realiza una especificación de las métricas seleccionadas para el proceso de evaluación en base a la norma ISO/IEC 9126, identificando las categorías de las métricas externas, ya que las herramientas de ciberseguridad se encuentran como productos software finales o ya desarrollados y que serán solicitadas por el CSIRT- ESPE en cumplimiento de sus funciones con relación a los requerimientos necesarios por evaluar y seleccionar.


3.3.4. Diseño de la Evaluación

3.3.4.1. Diseño de la Evaluación de Métricas y Métodos

Tabla 10.

Diseño de la Evaluación de Métricas y Métodos

Características	Métrica	Método
Funcionalidad	<ul style="list-style-type: none"> • Cumplimiento de la funcionalidad 	<ul style="list-style-type: none"> • Análisis de Reportes.
	<ul style="list-style-type: none"> • Exactitud 	<ul style="list-style-type: none"> • Pruebas funcionales.
Usabilidad	<ul style="list-style-type: none"> • Facilidad de función de aprendizaje 	<ul style="list-style-type: none"> • Cantidad de documentación existente.
	<ul style="list-style-type: none"> • Consistencia operacional de uso 	<ul style="list-style-type: none"> • Pruebas de ejecución.
Fiabilidad	<ul style="list-style-type: none"> • Falsos positivos 	<ul style="list-style-type: none"> • Análisis de resultados de pruebas realizadas.
Eficiencia	<ul style="list-style-type: none"> • Tiempo de respuesta 	<ul style="list-style-type: none"> • Pruebas de carga.
	<ul style="list-style-type: none"> • Consumo de recursos (CPU, Memoria y almacenamiento) 	<ul style="list-style-type: none"> • Requerimiento del hardware especificado.

CONTINÚA 

Seguridad	<ul style="list-style-type: none"> • Cumplimiento con parámetros de seguridad en acceso. 	<ul style="list-style-type: none"> • Pruebas funcionales.
Portabilidad	<ul style="list-style-type: none"> • Facilidad de implantación • Grado de coexistencia 	<ul style="list-style-type: none"> • Instalación en escenario de prueba.

3.3.4.2. Descripción de Métricas

Característica: Funcionalidad

Subcaracterística: Cumplimiento Funcional

Tabla 11.

Detalle de Métrica: Cumplimiento de la Funcionalidad

Detalle de la Métrica	Resultado
Nombre	Cumplimiento de la funcionalidad
Propósito	¿Cuántas funciones satisface de acuerdo a los requerimientos del CSIRT-ESPE?
Método de aplicación	Contar el número de funciones que cumplen en la evaluación y comparar con las funciones o servicios de CSIRT-ESPE.
Medición y calculo	$X = \left(1 - \frac{A}{B}\right) \times 10$
Interpretación del valor medio	$0 \leq X \leq 10$

CONTINÚA 

Tipo de escala	Si x se aproxima a 10, entonces tiene un mayor cumplimiento funcional. A: Número de funciones faltantes B: Número de funciones requeridas
Tipo de media	Absoluta.
Entradas de medición	Especificación de requerimientos. Informe de revisión.
Referencia ISO/IEC 12207	6.6 Validación. 6.6 Revisión conjunta.
Usuarios designados	Evaluadores.


Característica: Usabilidad

Subcaracterística: Facilidad de Aprendizaje

Tabla 12.

Detalle de Métrica: Fácil función de aprendizaje

Detalle de la Métrica	Resultado
Nombre	Fácil función de aprendizaje
Propósito	¿Qué porcentaje de funciones están documentadas, en la descripción de la herramienta y en el manual de usuario?
Método de aplicación	Contar el número de funciones que se encuentran documentadas y comparar

CONTINÚA 


	con el número de funciones de la herramienta.
Medición y calculo	$X = \left(\frac{A}{B}\right) \times 10$
Interpretación del valor medio	$0 \leq X \leq 10$ Si x se aproxima a 10, entonces tiene una mayor facilidad de aprendizaje.
Tipo de escala	A: Número de funciones documentadas B: Número total de funciones requeridas
Tipo de media	Absoluta.
Entradas de medición	Documentación de la herramienta. Especificación de requerimientos. Informe de revisión.
Referencia ISO/IEC 12207	6.6 Validación. 6.6 Revisión conjunta.
Usuarios designados	Proveedores. Evaluadores.

Subcaracterística: Facilidad de Uso u Operación

Tabla 13.

Detalle de Métrica: Consistencia Operacional de Uso

Detalle de la Métrica	Resultado
Nombre	Consistencia operacional de uso
Propósito	¿Cuán consistentes son los componentes de la interfaz de usuario?
Método de aplicación	Contar las operaciones que se encontraron con inconsistencias y comparar con las operaciones realizadas por el usuario.
Medición y calculo	$X = \left(1 - \frac{A}{B}\right) \times 10$
Interpretación del valor medio	$0 \leq X \leq 10$ <p>Si x se aproxima a 10, entonces el usuario tiene mayor satisfacción en la consistencia operacional del uso de la herramienta.</p>
Tipo de escala	<p>A: Número de funciones que el usuario encontró inconsistentes.</p> <p>B: Número de funciones usadas por el usuario en el periodo de prueba.</p>
Tipo de media	Relativa.
Entradas de medición	Especificación de requerimientos.

CONTINÚA 

Referencia ISO/IEC 12207

Informe de revisión.

6.6 Validación.


6.6 Revisión conjunta.

Usuarios designados

Evaluadores.

Característica: Fiabilidad**Subcaracterística: Madurez****Tabla 14.***Detalle de Métrica: Falsos Positivos*

Detalle de la Métrica	Resultado
Nombre	Falsos positivos
Propósito	¿Cuántas funciones erradas fueron detectados durante la prueba?
Método de aplicación	Contar el número de funciones que se detectaron problemas en sus resultados, y comparar con el número de funciones evaluadas.
Medición y calculo	$X = \left(1 - \frac{A}{B}\right) \times 10$
Interpretación del valor medio	$0 \leq X \leq 10$ Si x se aproxima a 10, tiene menor número de falsos positivos.

CONTINÚA 

Tipo de escala	A: Número de funciones erradas B: Número de funciones probadas
Tipo de media	Relativa.
Entradas de medición	Especificación de requerimientos. Informe de revisión.
Referencia ISO/IEC 12207	6.6 Validación. 6.6 Revisión conjunta.
Usuarios designados	Evaluadores.


Característica: Eficiencia

Subcaracterística: Comportamiento Temporal

Tabla 15.

Detalle de Métrica: Tiempo de Respuesta

Detalle de la Métrica	Resultado
Nombre	Tiempo de respuesta
Propósito	¿Qué tiempo se estima para el cumplimiento de una función?
Método de aplicación	Estimar el tiempo de respuesta de la herramienta de un flujo o una especificación transaccional.
Medición y calculo	$X = \begin{cases} 10 & \forall B \leq A \\ \frac{A}{B} \times 10 & \forall B > A \end{cases}$

CONTINÚA 


Interpretación del valor medio	Si x se aproxima a 10, entonces tiene un tiempo de respuesta más óptimo.
Tipo de escala	A: Es el tiempo considerado óptimo en un proceso de evaluación. B: Es el tiempo obtenido en la evaluación.
Tipo de media	Relativa.
Entradas de medición	Ejecución de funciones de la herramienta a evaluar. Informe de revisión.
Referencia ISO/IEC 12207	6.6 Validación. 6.6 Revisión conjunta.
Usuarios designados	Evaluadores.

Subcaracterística: Utilización de Recursos

Tabla 16.

Detalle de Métrica: Consumo de Recursos

Detalle de la Métrica	Resultado
Nombre	Consumo de recursos (CPU, Memoria y Almacenamiento)
Propósito	¿Cuántos recursos de hardware se estiman para el correcto funcionamiento de la herramienta?

CONTINÚA 

Método de aplicación

Detallar el valor requerido de recursos de hardware a ser utilizados por la herramienta.

Medición y calculo

$$a = \begin{cases} 10 & \forall B \leq A \\ \frac{A}{B} \times 10 & \forall B > A \end{cases}$$

$$b = \begin{cases} 10 & \forall B \leq A \\ \frac{A}{B} \times 10 & \forall B > A \end{cases}$$

$$c = \begin{cases} 10 & \forall B \leq A \\ \frac{A}{B} \times 10 & \forall B > A \end{cases}$$

$$X = \frac{a + b + c}{3}$$

Interpretación del valor medio

Entre mayor se aproxime el valor de X a 10, es más aceptable la utilización de recursos de hardware para la implementación de la herramienta.


Tipo de escala

A: Es el valor del recurso hardware considerado óptimo en un proceso de evaluación.

B: Es el valor requerido por la herramienta para ejecutar el proceso de evaluación.

a: Calificación obtenida del recurso CPU.

b: Calificación obtenida del recurso Memoria RAM.

CONTINÚA 

	c: Calificación obtenida del recurso Disco Duro.
Tipo de media	Relativa.
Entradas de medición	Documentación de la herramienta. Informe de revisión.
Referencia ISO/IEC 12207	6.6 Validación. 6.6 Revisión conjunta.
Usuarios designados	Proveedores. Evaluadores.


Característica: Seguridad

Subcaracterística: Métodos de Autenticación

Tabla 17.

Detalle de Métrica: Cumplimiento con Seguridad de Acceso

Detalle de la Métrica	Resultado
Nombre	Cumplimiento con seguridad de acceso
Propósito	¿La herramienta cuenta con métodos de autenticación aceptables para la seguridad de acceso?
Método de aplicación	Evidenciar y analizar el cumplimiento de normas, políticas y estándares de medidas de seguridad de autenticación.

CONTINÚA 

Medición y calculo

$$X = \left(\frac{A}{B}\right) \times 10$$

Interpretación del valor medio

$$0 \leq X \leq 10$$

Si x se aproxima a 10, entonces tiene un mayor cumplimiento de normas de seguridad de acceso.

Tipo de escala

A: Número de normas que cumple

B: Número de normas estimadas

Tipo de media

Absoluta.

Entradas de medición

Especificación de requerimientos.

Informe de revisión.

Referencia ISO/IEC 12207

6.6 Validación.


6.6 Revisión conjunta.

Usuarios designados

Evaluadores.

Característica: Portabilidad**Subcaracterística: Adaptabilidad****Tabla 18.***Detalle de Métrica: Fácil de Implantación*

Detalle de la Métrica	Resultado
Nombre	Facilidad de implantación
Propósito	¿Qué proporción de funciones o características de la herramienta, tienen una guía de instalación y configuración?
Método de aplicación	Contar el número de funciones y características, cuya instalación y configuración se encuentre documentada y comparar con el número de funciones y características de la herramienta.
Medición y calculo	$X = \left(\frac{A}{B}\right) \times 10$
Interpretación del valor medio	$0 \leq X \leq 10$ <p>Si x se aproxima a 10, entonces tiene una mayor facilidad de instalación y configuración.</p>
Tipo de escala	A: Número de funciones y características con configuración e instalación documentadas

CONTINÚA 

Tipo de media	B: Número de funciones requeridas Absoluta.
Entradas de medición	Documentación de la herramienta. Especificación de requerimientos. Informe de revisión.
Referencia ISO/IEC 12207	6.6 Validación. 6.6 Revisión conjunta.
Usuarios designados	Proveedores. Evaluadores.

Subcaracterística: Coexistencia

Tabla 19.
Detalle de Métrica: Grado de Coexistencia

Detalle de la Métrica	Resultado
Nombre	Grado de coexistencia
Propósito	¿Cuáles componentes de software son incompatibles con otros existentes?
Método de aplicación	Contar las características que son compatibles con otros softwares.
Medición y calculo	$X = \left(\frac{A}{B}\right) \times 10$
Interpretación del valor medio	$0 \leq X \leq 10$

CONTINÚA 

	Si x se aproxima a 10, entonces tiene un mayor grado de coexistencia.
Tipo de escala	A: Número de características compatibles. B: Número de características probadas.
Tipo de media	Absoluta.
Entradas de medición	Documentación de la herramienta. Informe de revisión.
Referencia ISO/IEC 12207	6.6 Validación. 6.6 Revisión conjunta.
Usuarios designados	Evaluadores.

3.3.4.3. Matriz de Resultados y Comparación de Herramientas Evaluadas

Después de obtener los resultados de evaluación de cada característica detallada en el punto anteriormente mencionado, con la utilización de cada métrica e interpretado por el rango de resultados de uno (1) a diez (10), dependiendo cual sea el resultado obtenido, se establece una tabla, donde se coloca el nombre de las herramientas en la columna izquierda, seguido por colocar el resultado obtenido de las características respectivamente por herramienta en las divisiones establecidas

Después se multiplica por cada coeficiente de ponderación respectivamente por característica, se realiza una sumatoria total de cada producto obtenido, y se coloca como resultado final en la columna derecha, de esta manera se obtiene un resultado final, considerando el cien por ciento (100%) de la evaluación por característica evaluada.

Los resultados finales conjuntamente con la interpretación de rango en niveles de aceptación y considerando los decimales deseados para diferenciar en caso de tener resultados iguales, permiten tomar la decisión de seleccionar una herramienta de ciberseguridad que cumpla con los requerimientos necesarios de solicitud del CSIRT-ESPE, satisfaciendo las funciones.

Este procedimiento reúne una comparación de impacto y prioriza la selección en cumplimiento de las características a través de las métricas estudiadas en este proyecto de investigación, generando un modelo de apoyo al CSIRT-ESPE.

Este modelo está creado para cualquier número de herramientas de ciberseguridad a evaluar, como se muestra en la siguiente tabla.

Tabla 20.
Matriz de Resultados y Comparación de Herramientas Evaluadas

	Funcionalidad	Usabilidad	Fiabilidad	Eficiencia	Seguridad	Portabilidad	
Herramienta	Coeficiente: %	Coeficiente: %	Coeficiente: %	Coeficiente: %	Coeficiente: %	Coeficiente: %	100%
Herramienta 1							
Herramienta 2							
Herramienta 3							
Herramienta n							

3.3.5. Ejecución de la Evaluación

En esta etapa o fase previamente identificados las métricas correspondientes a las herramientas de ciberseguridad relacionado con las funciones y objetivos del CSIRT, además de priorizar y caracterizar los rangos de valores de medición de las métricas, se ejecuta la evaluación, análisis y estudio de las herramientas de ciberseguridad seleccionadas.

Utilizando el método Empírico – Experimental, permite a través de pruebas de implantación y ejecución (experimento), observar y estudiar todos los comportamientos en tiempo real mediante los resultados obtenidos.

3.3.6. Conclusión de la Evaluación

Generación del Informe Final

En esta etapa final del modelo, se genera un informe final, donde se detalla toda la información de manera documentada como un respaldo que permite tomar decisiones a los interesados en realizar la selección de herramientas de ciberseguridad, el informe final es una herramienta que permite analizar los resultados, métricas y métodos obtenidos, esto facilita la interpretación de los datos, permite visualizar conclusiones.

El Informe final comprende de un formato y componentes principales, detallados a continuación:

Tema: Título principal a tratar.

Introducción: Se detalla la importancia del problema y el motivo principal de la solicitud de las herramientas de ciberseguridad.

Objetivos: Se detalla que es lo que se pretende lograr con el análisis de selección, se considera, el objetivo general y específico, justificando su tiempo estimado de efectividad.

Alcance: Se detalla hasta donde lleva a cabo el estudio de selección de herramientas, el área a analizar, limitando los objetivos planteados.

Metodología: Se detalla cómo se lleva a cabo el estudio y que es lo que se realizó para lograr los resultados obtenidos.

Descripción de Resultados: Se detalla en forma de filas y columnas los resultados obtenidos, de esta manera se puede relacionar las características principales de las herramientas con los criterios seleccionados del modelo, se presenta los datos de manera objetiva y detallada.

Análisis de resultados: Se clasifica los resultados en base a criterios de selección propios del modelo y se interpreta los resultados, con principios establecidos en el modelo como:

- Concisión: Se compone de ideas claras y precisas.
- Legibilidad: Se compone de texto, tablas y gráficas entendibles e intuitivas que facilitan su interpretación.
- Equidad: Comparación e interpretación de los resultados de forma honrada e igual de condiciones a todas las herramientas seleccionadas en el estudio del modelo.

4. CAPITULO IV

Caso de Estudio de Selección de Herramientas de Ciberseguridad para el CSIRT-ESPE

4.1. Introducción

En este capítulo se tratará el caso de estudio enfocado en el análisis de herramientas que se ajusten a las necesidades del CSIRT- ESPE, mediante el modelo de selección planteado en este caso de estudio.

Para definir el proceso de evaluación, se partirá de la obtención de requerimientos por medio del estudio de la situación actual y de la definición formal del CSIRT-ESPE.

4.2. Justificación de la Adquisición

Toda institución u organización publica dentro de la República del Ecuador, debe cumplir con leyes de procesos de solicitud y compras públicas, la organización o entidad que se encarga de este tipo de procesos se denomina, Servicio Nacional de Contratación Pública (SERCOP), esta institución pública es la responsable de contraer productos y servicios de proveedores a instrucciones públicas, mediante procesos de selección por calificación de merecimiento, la Universidad de las Fuerzas Armadas ESPE, al pertenecer a las universidades públicas del Ecuador, se rige a estos procesos, relacionando con la norma ISO 37001, se puede especificar que el cumplimiento correcto de estos procesos generan una solicitud y contratación de la herramienta de ciberseguridad adecuado por parte del CSIRT-ESPE, desde su inicio de solicitud hasta la contratación, compra o adquisición de dicha herramienta, se puede mencionar que el cumplimiento de los

procesos asignados por el SERCOP hacia la Universidad de las Fuerzas Armadas ESPE, cumplen con estándares de mitigación de corrupción e inclusive de considerar sin corrupción en todos los procesos de adquisición, estos procesos se los puedes mencionar en la siguiente grafica.

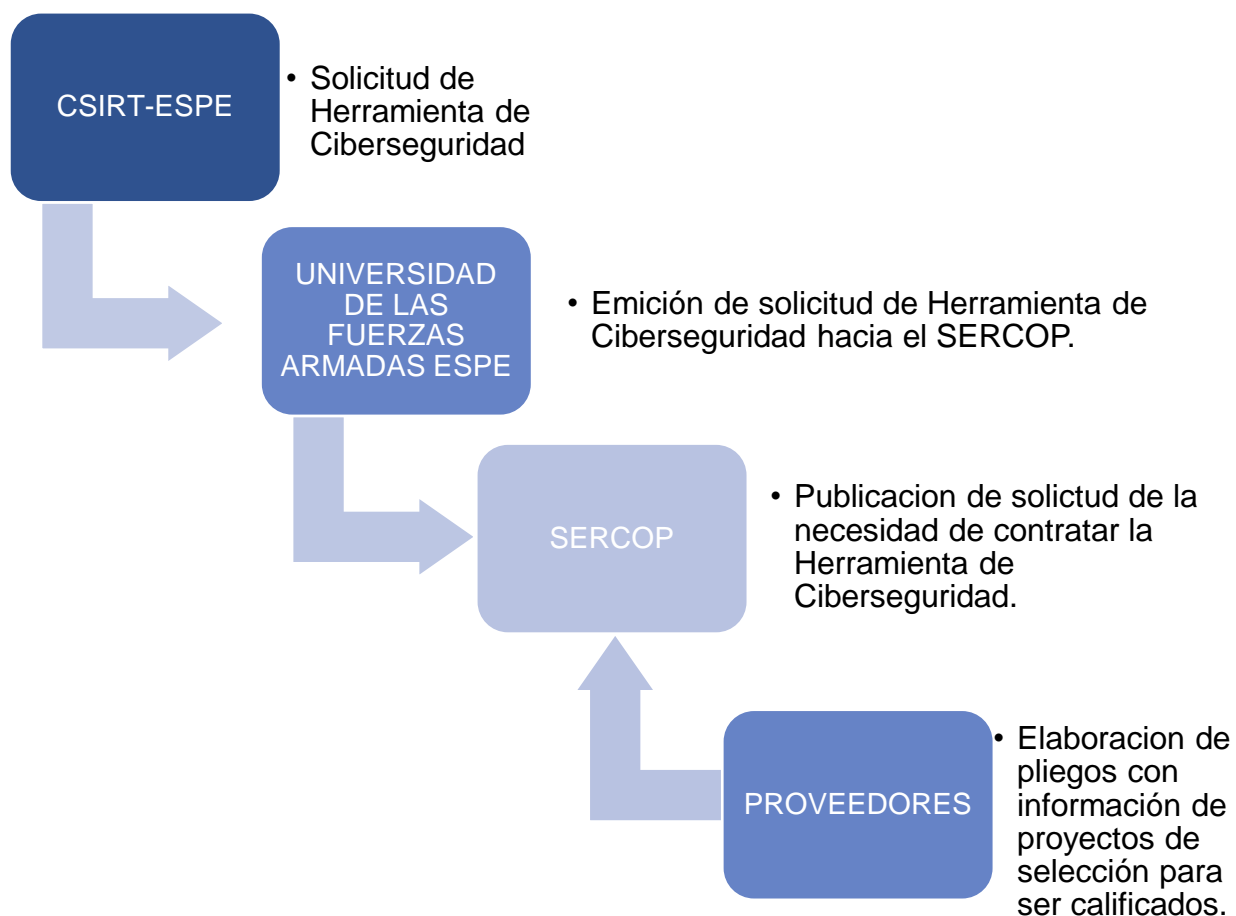


Figura 27. Procesos de selección ESPE - SERCOP

4.3. Proceso de Evaluación

4.3.1 Establecimiento de Requerimientos por CSIRT-ESPE

En el establecimiento formal del CSIRT-ESPE, se han tomado en cuenta un conjunto de servicios reactivos, proactivos y de gestión de la calidad y seguridad, con el fin de cumplir con una serie de actividades planificadas para la administración de incidentes de seguridad de la información.

Para obtener un portafolio de servicios que cumpla las necesidades de la institución según su situación actual, se realiza un análisis para priorizar los servicios que sean de mayor impacto, obteniendo como resultado la siguiente propuesta de portafolio inicial:

Tipo Servicio	Servicios
Servicios Reactivos	<ul style="list-style-type: none"> - Alertas y Advertencias. - Manejo de incidentes. - Manejo de vulnerabilidades.
Servicios Proactivos	<ul style="list-style-type: none"> - Comunicados, alertas. - Difusión de información relacionada con la seguridad.
Servicios de Gestión de Calidad de la Seguridad	<ul style="list-style-type: none"> - Sensibilización. - Educación y Capacitación.

Figura 28. Propuesta de servicios iniciales CSIRT-ESPE

Fuente: (De La Torre & Parra, 2018)

Para posteriores etapas, se plantea una proyección, en la cual el portafolito del CSIRT-ESPE aumentará, abarcando servicios adicionales como:

Tipo Servicio	Servicios
Servicios Reactivos	- Manejo de artifact
Servicios Proactivos	- Observatorio de tecnología - Evaluaciones o auditorías de seguridad. - Desarrollo de herramientas de seguridad. - Detección de intrusos.
Servicios de Gestión de Calidad de la Seguridad	- Análisis de riesgos. - Consultoría de seguridad. - Continuidad del negocio y recuperación tras un desastre.

Figura 29. Propuesta de servicios de desarrollo CSIRT-ESPE

Fuente: (De La Torre & Parra, 2018)

Para la realización de estas actividades se debe contar con herramientas de ciberseguridad, con la finalidad de realizar un trabajo automatizado y eficiente, para abarcar la gestión de un mayor número de servicios

4.3.2. Descripción del Producto Software

4.3.2.1 Nessus



Figura 30. Logo del Software Nessus

Fuente: (Tenable, 2019)

Es una herramienta de ciberseguridad de licencia privada desarrollada por Tenable, su principal característica o función es el escaneo de vulnerabilidades en diferentes plataformas o sistemas operativos, tiene un panel (dashboard) muy amigable con los usuarios basados en consola y gráficos que permite el informe y reportes de escaneos y de todas las funciones que posee.

Nessus cuenta con certificaciones propias y ayuda o soporte online, esto permite que sus clientes tengan acceso a diferentes soluciones o asesoramiento en sus diferentes funciones de ciberseguridad, además de contar con un soporte y acceso a la información de experiencias de usuarios, esta información se encuentra compartida por diferentes blogs de ayuda.

Nessus es una solución de evaluación de vulnerabilidades estándar de la industria para profesionales de la seguridad, ayuda a los profesionales de la seguridad de primera línea a identificar y reparar vulnerabilidades con rapidez y facilidad, incluso fallas de software, parches faltantes, malware y configuraciones erróneas, en una variedad de sistemas operativos, dispositivos y aplicaciones. (Tenable, 2019).

4.4.2. Cisco Stealthwatch



Figura 31. Logo de Cisco Stealthwatch

Fuente: (Cisco, 2019)

Stealthwatch es un producto software desarrollado por la empresa Estadounidense Cisco con la especialidad pionera a nivel mundial en las telecomunicaciones, desarrollando dispositivos de redes con su funcionamiento, mantenimiento y seguridad.

Stealthwatch Enterprise es la solución de análisis de seguridad y visibilidad líder en el sector que aprovecha la telemetría de la empresa a partir de la infraestructura de red existente. Proporciona una detección de amenazas avanzada, una respuesta acelerada a las mismas y una segmentación de red simplificada mediante el uso del machine learning de varias capas y un modelo de comportamiento avanzado, todo ello a través de la red extendida. (Cisco, 2019).

Dispone de licencias para su implementación, lo que permite garantizar soporte técnico y guías de instalación por parte de su empresa propietaria Cisco, posee infraestructura disponible para la nube con su versión Cloud Cisco Stealthwatch, dentro de su licenciamiento contiene inteligencia de amenazas, que permite una actualización constante de nuevas amenazas que se crean a nivel mundial, mencionando algunas de sus funciones son:

- Detección de amenazas en tiempo real
- Diagnóstico y respuesta a incidentes
- Segmentación de red
- Planificación de capacidad y rendimiento de la red
- Capacidad de satisfacción de los requisitos normativos

Contiene la tecnología de Telemetría que le permite analizar los datos de un gran periodo de tiempo, y lograr un seguimiento de auditoria informática, investigaciones y diagnóstico, se puede instalar en varios recopiladores de flujo considerando hardware y máquinas virtuales.

4.3.3. Ejecución de la Evaluación


Herramienta de Ciberseguridad Nessus

Evaluación de Métricas


Tabla 21.

Evaluación de Métrica Cumplimiento de la Funcionalidad para la Herramienta Nessus

	Característica:	Subcaracterística:	Métrica:
	Funcionalidad	Cumplimiento Funcional	Cumplimiento de la Funcionalidad
	Requisitos	Cumplimiento	Observaciones
Servicios Reactivos	Alertas y advertencias	Si	Nessus tiene un módulo de workflow en el cual se configura las alertas a correo electrónico, notificación de UI (User Interface), informes y alertas de Syslog.
	Manejo de Incidentes	Si	Nessus en el módulo de workflow permite crear de forma manual o automática tickets que permiten tratar las incidencias en base a una vulnerabilidad detectada.


CONTINÚA 

	Manejo de vulnerabilidades	Si	Nessus cuenta con los siguientes componentes: Resumen de vulnerabilidades, Exploración continua de vulnerabilidades, Seguimiento de proceso de mitigación, Entendimiento del riesgo por vulnerabilidad y comprensión del riesgo.
	Manejo de artifa	No	Nessus permite identificar los artefactos frágiles en el sistema, sin embargo, no permite una gestión total del mismo.
Servicios Proactivos	Comunicados y alerta	Si	Nessus permite generar informes de escaneos de seguridad, tratamiento de vulnerabilidad. Estos informes describen de manera gráfica y detallada los resultados obtenidos.
	Difusión de información relacionada con la seguridad	Si	Nessus a través de su comunidad provee información de las tendencias de ciberseguridad y de vulnerabilidades actuales, además de contar de contar capacitaciones online de las

CONTINÚA 

soluciones a los casos de vulnerabilidades detectadas.

Observatorio de tecnología	Si	Nessus tiene sitios web en los cuales permite realizar investigación de la tendencia de ciberseguridad mediante webinars y blogs continuos.
Evaluaciones o auditorias de seguridad	Si	El explorador de Nessus permite realizar auditorías de cumplimiento a múltiples plataformas mediante políticas de auditoria establecida por el CSIRT-ESPE. Permite realizar auditorías a: Bases de datos, Redes e infraestructura en la nube, Contenido Sensible. A demás provee políticas predefinidas como plantillas estándares.

CONTINÚA 

Detección de intrusos	Si	Nessus tiene un módulo de monitorio continuo en tiempo real que permite la detección a tiempo de intrusos en la infraestructura.
-----------------------	----	--

$$X = \left(1 - \frac{\text{Número de funciones faltantes}}{\text{Número de funciones requeridas}}\right) \times 10$$

$$X = \left(1 - \frac{1}{9}\right) \times 10 = 8,89$$


Tabla 22.

Resultado de la Característica Funcionalidad para la Herramienta Nessus

Característica	Subcaracterística	Métrica	Valor	Nivel de Evaluación	Nivel de Puntuación
Funcionalidad	Cumplimiento Funcional	Cumplimiento de la funcionalidad	8,89	Aceptable	Satisfactorio

Tabla 23.*Evaluación de Métrica Fácil función de aprendizaje para la Herramienta Nessus*

Característica:		Subcaracterística:		Métrica
Usabilidad		Facilidad de Aprendizaje		Fácil función de aprendizaje
Funciones CSIRT-ESPE		Funciones de Nessus	Cumplimiento	Documentación
Servicios Reactivos	Alertas y advertencias	SecurityCenter/ Workflow/Alerts	Si	https://docs.tenable.com/sccv/5_7/ Content/Alerts.htm
	Manejo de Incidentes	SecurityCenter/ Workflow/Tickets	Si	https://docs.tenable.com/sccv/5_7/ Content/Tickets.htm
	Manejo de vulnerabilidades	Analyze Data/Vulnerability Analysis	Si	https://docs.tenable.com/sccv/5_7/ Content/VulnerabilityAnalysis.htm
	Manejo de artífac	No cumple	No	

CONTINÚA 


Servicios Proactivos	Comunicados y alerta	Analyze Data/Reports/Manage Report Results	Si	https://docs.tenable.com/sccv/5_7/ Content/Reports/ManageReportRe sults.htm
	Difusión de información relacionada con la seguridad	Comunidad de Nessus	Si	https://community.tenable.com/s/
	Observatorio de tecnología	Comunidad de Nessus	Si	https://community.tenable.com/s/
	Evaluaciones o auditorías de seguridad	Active Scan Objects/Configure Scans/Active Scan Objects	Si	https://docs.tenable.com/sccv/5_7/ Content/AuditFiles.htm
Detección de intrusos	Configure Scans/ Resources /Passive Vulnerability Scanner	Si	https://docs.tenable.com/sccv/5_7/ Content/PassiveVulnerabilityScan ners.htm	

$$X = \left(\frac{\text{Número de funciones documentadas}}{\text{Número total de funciones requeridas}} \right) \times 10 = \left(\frac{8}{9} \right) \times 10 = 8,89$$

Tabla 24.

Evaluación de Métrica Consistencia operacional de uso para la Herramienta Nessus


Característica:	Subcaracterística	Métrica	
Usabilidad	Facilidad de Uso u Operación	Consistencia operacional de uso	
Funciones de Nessus	Casos inconsistentes	Casos evaluados	Cumplimiento $x = \left(1 - \frac{\text{Número de casos inconsistentes}}{\text{Número de casos evaluados}} \right) \times 10$
SecurityCenter/ Workflow/Alerts	1	5	8,00
SecurityCenter/ Workflow/Tickets	0	2	10,00
Analyze Data/Vulnerability Analysis	1	3	6,67
Analyze Data/Reports/Manage Report Results	0	1	10,00

CONTINÚA 

Active Scan Objects/Configure Scans/Active Scan Objects	2	6	6,67
Configure Scans/ Resources /Passive Vulnerability Scanner	2	4	5,00
		PROMEDIO	7,72

Tabla 25.
Resultado de la Característica Usabilidad para la Herramienta Nessus


Característica	Subcaracterística	Métrica	Valor	Nivel de Evaluación	Nivel de Puntuación
Usabilidad	Facilidad de Aprendizaje	Fácil función de aprendizaje	8,89	Aceptable	Satisfactorio

CONTINÚA 

Facilidad de Uso u	Consistencia	7,72	Aceptable	Satisfactorio
Operación	operacional			
	de uso			
Promedio		8,30	Aceptable	Satisfactorio

Tabla 26.
Evaluación de Métrica Falsos positivos para la Herramienta Nessus

Característica:	Subcaracterística		Métrica
Fiabilidad	Madurez	Falsos positivos	
Funciones de Nessus	Funciones erradas	Funciones probadas	Cumplimiento
			$x = \left(1 - \frac{\text{Funciones erradas}}{\text{Funciones probadas}}\right) \times 10$
SecurityCenter/ Workflow/Alerts	0	3	10,00
SecurityCenter/ Workflow/Tickets	0	2	10,00
Analyze Data/Vulnerability Analysis	0	1	10,00
Analyze Data/Reports/Manage Report Results	1	4	7,50

CONTINÚA 

Active Scan Objects/Configure Scans/Active Scan Objects	2	4	5,00
Configure Scans/ Resources /Passive Vulnerability Scanner	0	4	10,00
Promedio:			8,75

Tabla 27.

Resultado de la Característica Fiabilidad para Nessus

Característica	Subcaracterística	Métrica	Valor	N. Evaluación	N. Puntuación
Fiabilidad	Madurez	Falsos positivos	8,75	Aceptable	Satisfactorio

Tabla 28.
Evaluación de Métrica Tiempo de respuesta para la Herramienta Nessus

Característica	Subcaracterística	Métrica
Eficiencia	Comportamiento Temporal	Tiempo de respuesta
Función de Ejecución	Tiempo óptimo	Tiempo obtenido en la evaluación
Escáner de vulnerabilidades de red de prueba (50.000 Host)	60 minutos	74 minutos


$$X = \begin{cases} 10 & \forall \text{ Tiempo obtenido} \leq A \\ \frac{\text{Tiempo Optimo}}{\text{Tiempo obtenido}} \times 10 & \forall \text{ Tiempo obtenido} > A \end{cases}$$

$$X = \frac{\text{Tiempo Optimo}}{\text{Tiempo obtenido}} \times 10$$

$$X = \frac{60}{74} \times 10 = 8,10$$

Tabla 29.
Evaluación de Métrica Consumo de recursos para la Herramienta Nessus

Característica		Subcaracterística	Métrica
Eficiencia		Utilización de Recursos	Consumo de recursos (CPU, Memoria y Almacenamiento)
Recurso de hardware	Función de ejecución	Valor mínimo de la herramienta	Valor óptimo
CPU (Procesador)	Escáner de vulnerabilidades de red de prueba (50.000 Host)	2GHZ	2.4GHZ
Memoria RAM	Escáner de vulnerabilidades de red de prueba (50.000 Host)	8GB	16GB

CONTINÚA 

Disco Duro	Escáner de vulnerabilidades de red de prueba (50.000 Host)	30GB	20GB
------------	--	------	------

$$CPU: a = \begin{cases} 10 & \forall \text{ Valor requerido por la herramienta} \leq \text{Valor óptimo} \\ \frac{\text{Valor óptimo}}{\text{Valor requerido por la herramienta}} \times 10 & \forall \text{ Valor requerido por la herramienta} > \text{Valor óptimo} \end{cases}$$

$$a = 10$$

$$RAM: b = \begin{cases} 10 & \forall \text{ Valor requerido por la herramienta} \leq \text{Valor óptimo} \\ \frac{\text{Valor óptimo}}{\text{Valor requerido por la herramienta}} \times 10 & \forall \text{ Valor requerido por la herramienta} > \text{Valor óptimo} \end{cases}$$

$$b = 10$$

$$DISCO DURO: c = \begin{cases} 10 & \forall \text{ Valor requerido por la herramienta} \leq \text{Valor óptimo} \\ \frac{\text{Valor óptimo}}{\text{Valor requerido por la herramienta}} \times 10 & \forall \text{ Valor requerido por la herramienta} > \text{Valor óptimo} \end{cases}$$

$$c = \frac{20}{30} \times 10 = 6,66$$

$$X = \frac{a + b + c}{3} = \frac{10 + 10 + 6,66}{3} = 8,88$$

Tabla 30.
Resultado de la Característica Eficiencia para Nessus

Característica	Subcaracterística	Métrica	Valor	N. Evaluación	N. Puntuación
Eficiencia	Comportamiento Temporal	Tiempo de respuesta	8,10	Aceptable	Satisfactorio
	Utilización de Recursos	Consumo de recursos (CPU, Memoria y Almacenamiento)	8,88	Aceptable	Satisfactorio
	Promedio:		8,49	Aceptable	Satisfactorio

Tabla 31.

Evaluación de Métrica Cumplimiento con seguridad de acceso para la Herramienta Nessus

Característica:	Subcaracterística:	Métrica:
Seguridad	Métodos de Autenticación	Cumplimiento con seguridad de acceso
Políticas y Estándares	Cumplimiento	Observación
Definición de roles	Si	Nessus permite la definición de roles de acuerdo al perfil del usuario, existen los siguientes roles: Administrador, Gerente de seguridad, Auditor, Administrador de credenciales, Ejecutivo, Analista de seguridad y Analista de vulnerabilidad.
Privilegios	Si	La asignación de las funciones en Nessus se las realiza mediante los roles otorgados a un usuario.
Factor múltiple de autenticación	Si	Nessus permite la autenticación por medio de: Tarjetas inteligentes, Tarjetas de verificación de identidad personal y Tarjetas de acceso común, adicionales al usuario clave establecidos.

$$X = \left(1 - \frac{\text{Número de normas que cumple}}{\text{Número de normas estimadas}} \right) \times 10$$

$$X = \left(\frac{3}{3} \right) \times 10 = 10$$


Tabla 32.

Resultado de la Característica Seguridad para Nessus

Característica	Subcaracterística	Métrica	Valor	N. Evaluación	N. Puntuación
Seguridad	Métodos de Autenticación	Cumplimiento con seguridad de acceso	10	Excede de los objetivos	Satisfactorio

Tabla 33.
Evaluación de Métrica Facilidad de implantación para Nessus

Característica:		Subcaracterística:		Métrica
Portabilidad		Adaptabilidad		Facilidad de implantación
Funciones CSIRT-ESPE		Funciones de Nessus	Cumplimiento	Documentación
Servicios Reactivos	Alertas y advertencias	SecurityCenter/ Workflow/Alerts	Si	Cisco Stealthwatch Documents: https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/management_console/smc_users_guide/SW_6_9_0_SMC_Users_Guide_DV_1_2.pdf
	Manejo de Incidentes	SecurityCenter/ Workflow/Tickets	Si	
	Manejo de vulnerabilidades	Analyze Data/Vulnerability Analysis	Si	
	Manejo de artifa	No cumple	No	
	Comunicados y alerta	Analyze Data/Reports/Manage Report Results	Si	
Servicios Proactivos				

CONTINÚA 

Difusión de información relacionada con la seguridad	Comunidad de Nessus	Si
Observatorio de tecnología	Comunidad de Nessus	Si
Evaluaciones o auditorias de seguridad	Active Scan Objects/Configure Scans/Active Scan Objects	Si
Detección de intrusos	Configure Scans/ Resources /Passive Vulnerability Scanner	Si


$$X = \left(\frac{\text{Número de funciones y características con configuración e instalación documentadas}}{\text{Número de funciones requeridas}} \right) \times 10$$

$$X = \left(\frac{8}{9} \right) \times 10 = 8,89$$

Tabla 34.

Evaluación de Métrica Grado de coexistencia para la Herramienta Nessus

Característica:	Subcaracterística:	Métrica:
Portabilidad	Coexistencia	Grado de coexistencia
Funciones de Nessus	Coexiste con otros softwares	Observaciones
SecurityCenter/ Workflow/Alerts	No	Esta función solo se la puede realizar desde la herramienta Nessus.
SecurityCenter/ Workflow/Tickets	Si	
Analyze Data/Vulnerability Analysis	Si	

CONTINÚA 

Analyze Data/Reports/Manage Report Results	Si	Nessus provee un Apirest para la comunicación con otras aplicaciones. Este Api se denomina PyNessus y está elaborada en Python.sd
Active Scan Objects/Configure Scans/Active Scan Objects	Si	
Configure Scans/ Resources /Passive Vulnerability Scanner	Si	

$$X = \left(\frac{\text{Número de características compatibles}}{\text{Número de características probadas}} \right) \times 10$$

$$X = \left(\frac{5}{6} \right) \times 10 = 8,33$$

Tabla 35.
Resultado de la Característica Portabilidad para la Herramienta Nessus

Característica	Subcaracterística	Métrica	Valor	Nivel de Evaluación	Nivel de Puntuación
Portabilidad	Adaptabilidad	Facilidad de implantación	8,89	Aceptable	Satisfactorio

CONTINÚA 

Coexistencia	Grado de coexistencia	8,33	Aceptable	Satisfactorio
	Promedio	8,61	Aceptable	Satisfactorio

Valores Obtenidos de la Herramienta Nessus

Tabla 36.

Resultado General de la Herramienta Nessus

Característica	Valor
Funcionalidad	8,89
Usabilidad	8,30
Fiabilidad	8,75
Eficiencia	8,49
Seguridad	10,00
Portabilidad	8,61


Herramienta de Ciberseguridad Cisco Stealthwatch

Evaluación de Métricas

Tabla 37.

Evaluación de Métrica Cumplimiento de la funcionalidad para la Herramienta Cisco Stealthwatch

	Característica:	Subcaracterística:	Métrica:
	Funcionalidad	Cumplimiento Funcional	Cumplimiento de la funcionalidad
	Requisitos	Cumplimiento	Observaciones
Servicios	Alertas y advertencias	Si	Cisco Stealthwatch cuenta con métodos de telemetría como NetFlow, que permite una visibilidad en tiempo real de la red, detectando vulnerabilidades, proveyendo información mediante alertas y advertencias, para el correcto manejo de los incidentes. A demás permite identificar artifacs que son objeto de ataques para su correcto manejo.
Reactivos	Manejo de incidentes	Si	
	Manejo de vulnerabilidades	Si	
	Manejo de artifac	Si	
	Comunicados y alerta	Si	

CONTINÚA 

Servicios Proactivos	Difusión de información relacionada con la seguridad	Si	Cisco Stealthwatch provee mecanismos de investigación de incidencias y cumplimiento, utilizando NetFlow para crear un registro de auditoria históricos, para que los investigadores puedan analizar el comportamiento anormal, además las pistas de auditoria se basan en leyes y regulaciones que ayudan a proteger la información sensible que monitoreará el CSIRT-ESPE.
	Observatorio de tecnología	Si	
	Evaluaciones o auditorias de seguridad	Si	
	Detección de intrusos	Si	

$$X = \left(1 - \frac{\text{Número de funciones faltantes}}{\text{Número de funciones requeridas}}\right) \times 10$$

$$X = \left(1 - \frac{9}{9}\right) \times 10 = 10,00$$

Tabla 38.

Resultado de la Característica Funcionalidad para la Herramienta Cisco Stealthwatch


Característica	Subcaracterística	Métrica	Valor	Nivel de Evaluación	Nivel de Puntuación
Funcionalidad	Cumplimiento Funcional	Cumplimiento de la funcionalidad	10,00	Excede los objetivos	Satisfactorio

Tabla 39.


Evaluación de Métrica Fácil función de aprendizaje para la Herramienta Cisco Stealthwatch

Característica:	Subcaracterística:	Métrica
Usabilidad	Facilidad de Aprendizaje	Fácil función de aprendizaje
Funciones CSIRT-ESPE	Funciones de Cisco Stealthwatch	Cumplimiento Documentación
		Link: https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/management_console/smc_users_guide/SW_6_9_0_SMC_Users_Guide_DV_1_2.pdf

.pdf

CONTINÚA 

Servicios Reactivos	Alertas y advertencias	Cisco Manager Console-Alarms	Si	Cisco User Guide for Stealthwatch System. Páginas 36 a 37.
	Manejo de Incidentes	Cisco Manager Console-Responding to Alarms	Si	Cisco User Guide for Stealthwatch System. Páginas 231 a 249
	Manejo de vulnerabilidades	Cisco Manager Console-Host Groups	Si	Cisco User Guide for Stealthwatch System. Páginas 96 a 101.
	Manejo de artifa	No tiene	No	No existe documentación en el manual de usuario.
	Comunicados y alertas	Cisco Manager Console-Views and Dashboard	Si	Cisco User Guide for Stealthwatch System. Páginas 109 a 117.
Servicios Proactivos	Difusión de información relacionada con la seguridad	Cisco Stealthwatch Comunity	Si	Cisco Stealthwatch a través de su comunidad provee información de las tendencias de ciberseguridad y de vulnerabilidades actuales,

CONTINÚA 

además de contar de contar capacitaciones online de las soluciones a los casos de vulnerabilidades detectadas.


Observatorio de tecnología	Cisco Stealthwatch Community	Si	Cisco Stealthwatch tiene sitios web en los cuales permite realizar investigación de la tendencia de ciberseguridad mediante webinars y blogs continuos.
Evaluaciones o auditorias de seguridad	Cisco Manager Console-Working with Documents	Si	Cisco User Guide for Stealthwatch System. Páginas 303 a 321.
Detección de intrusos	Cisco Manager Console-Monitoring Traffic and Network Performance	Si	Cisco User Guide for Stealthwatch System. Páginas 133 a 151.

$$X = \left(\frac{\text{Número de funciones documentadas}}{\text{Número total de funciones requeridas}} \right) \times 10 = \left(\frac{8}{9} \right) \times 10 = 8,89$$

Tabla 40.

Evaluación de Métrica Consistencia operacional de uso para la Herramienta Cisco Stealthwatch

Característica:	Subcaracterística:	Métrica:		
Usabilidad	Facilidad de Uso u Operación	Consistencia operacional de uso		
Funciones de Cisco Stealthwatch	Casos inconsistentes	Casos evaluados	Cumplimiento $x = \left(1 - \frac{\text{Número de casos inconsistentes}}{\text{Número de casos evaluados}} \right) \times 10$	
	Cisco Manager Console-Alarms	1	3	6,67
	Cisco Manager Console- Responding to Alarms	0	3	10,00
	Cisco Manager Console-Host Groups	0	2	10,00


CONTINÚA 

Cisco Manager Console-Views and Dashboard	0	1	10,00
Cisco Manager Console-Working with Documents	1	2	5,00
Cisco Manager Console-Monitoring Traffic and Network Performance	0	3	10,00
		PROMEDIO	8,61

Tabla 41.

Resultado de la Característica Usabilidad para la Herramienta Cisco Stealthwatch


Característica	Subcaracterística	Métrica	Valor	Nivel de Evaluación	Nivel de Puntuación
Usabilidad	Facilidad de Aprendizaje	Fácil función de aprendizaje	8,89	Aceptable	Satisfactorio

CONTINÚA 

Facilidad de Uso u	Consistencia	8,61	Aceptable	Satisfactorio
Operación	operacional			
	de uso			
Promedio		8,75	Aceptable	Satisfactorio

Tabla 42.
Evaluación de Métrica Falsos positivos para la Herramienta Cisco Stealthwatch

Característica:	Subcaracterística:	Métrica:
Fiabilidad	Madurez	Falsos positivos
Funciones de Cisco Stealthwatch	Funciones erradas	Funciones probadas
		Cumplimiento
		$x = \left(1 - \frac{\text{Funciones erradas}}{\text{Funciones probadas}}\right) \times 10$
Cisco Manager Console-Alarms	0	3
Cisco Manager Console- Responding to Alarms	0	2
		10,00
		10,00

CONTINÚA 

Cisco Manager Console-Host Groups	1	2	5,00
Cisco Manager Console-Views and Dashboard	0	2	10,00
Cisco Manager Console-Working with Documents	0	3	10,00
Cisco Manager Console-Monitoring Traffic and Network Performance	0	3	10,00
		Promedio	9,17

Tabla 43.

Resultado de la Característica Fiabilidad para la Herramienta Cisco Stealthwatch

Característica	Subcaracterística	Métrica	Valor	N. Evaluación	N. Puntuación
Fiabilidad	Madurez	Falsos positivos	9,17	Excede los objetivos	Satisfactorio

Tabla 44.

Evaluación de Métrica Tiempo de respuesta para la Herramienta Cisco Stealthwatch


Característica:	Subcaracterística:	Métrica:
Eficiencia	Comportamiento Temporal	Tiempo de respuesta
Función de Ejecución	Tiempo óptimo	Tiempo obtenido en la evaluación
Escáner de vulnerabilidades de red de prueba (50.000 Host)	60 minutos	43 minutos

$$X = \begin{cases} 10 & \forall \text{ Tiempo obtenido} \leq A \\ \frac{\text{Tiempo Óptimo}}{\text{Tiempo obtenido}} \times 10 & \forall \text{ Tiempo obtenido} > A \end{cases}$$

$$X = 10$$

Tabla 45.
Evaluación de Métrica Consumo de recursos para la Herramienta Cisco Stealthwatch

Característica:		Subcaracterística:	Métrica:
Eficiencia		Utilización de Recursos	Consumo de recursos (CPU, Memoria y Almacenamiento)
Recurso de hardware	Función de ejecución	Valor mínimo de la herramienta	Valor óptimo
CPU (Procesador)	Escáner de vulnerabilidades de red de prueba (50.000 Host)	2.2GHZ	2.4GHZ
Memoria RAM	Escáner de vulnerabilidades de red de prueba (50.000 Host)	16GB	16GB

CONTINÚA 

Disco Duro	Escáner de vulnerabilidades de red de prueba (50.000 Host)	125GB	20GB
------------	--	-------	------

$$CPU: a = \begin{cases} 10 & \forall \text{ Valor requerido por la herramienta} \leq \text{Valor óptimo} \\ \frac{\text{Valor óptimo}}{\text{Valor requerido por la herramienta}} \times 10 & \forall \text{ Valor requerido por la herramienta} > \text{Valor óptimo} \end{cases}$$

$$a = 10$$

$$RAM: b = \begin{cases} 10 & \forall \text{ Valor requerido por la herramienta} \leq \text{Valor óptimo} \\ \frac{\text{Valor óptimo}}{\text{Valor requerido por la herramienta}} \times 10 & \forall \text{ Valor requerido por la herramienta} > \text{Valor óptimo} \end{cases}$$

$$b = 10$$

$$DISCO DURO: c = \begin{cases} 10 & \forall \text{ Valor requerido por la herramienta} \leq \text{Valor óptimo} \\ \frac{\text{Valor óptimo}}{\text{Valor requerido por la herramienta}} \times 10 & \forall \text{ Valor requerido por la herramienta} > \text{Valor óptimo} \end{cases}$$

$$c = \frac{20}{125} \times 10 = 1,6$$

$$X = \frac{a + b + c}{3} = \frac{10 + 10 + 1,6}{3} = 7,20$$

Tabla 46.

Resultado de la Característica Eficiencia para la Herramienta Cisco Stealthwatch

Característica	Subcaracterística	Métrica	Valor	N. Evaluación	N. Puntuación
Eficiencia	Comportamiento	Tiempo de	10	Excede de los	Satisfactorio
	Temporal	respuesta		objetivos	
	Utilización de	Consumo de	7,2	Aceptable	Satisfactorio
	Recursos	recursos (CPU, Memoria y Almacenamiento)			
		Promedio:	8,60	Aceptable	Satisfactorio

Tabla 47.

Evaluación de Métrica Cumplimiento con seguridad de acceso para la Herramienta Cisco Stealthwatch

Característica:	Subcaracterística:	Métrica:
Seguridad	Métodos de Autenticación	Cumplimiento con seguridad de acceso
Políticas y Estándares	Cumplimiento	Observación
Definición de roles	Si	<p>Cisco Stealthwatch permite asignar roles a los usuarios, como:</p> <ul style="list-style-type: none"> • All • Configuration Manager • Network Engineer • Security Analyst • Stealthwatch Power User
Privilegios	Si	Cisco Stealthwatch permite definir acciones de escritura lectura a los diferentes módulos asignados al usuario.
Factor múltiple de autenticación	Si	Cisco Systems provee varios métodos de autenticación como tokens de seguridad y accesos biométricos.

$$X = \left(1 - \frac{\text{Número de normas que cumple}}{\text{Número de normas estimadas}} \right) \times 10$$

$$X = \left(\frac{3}{3} \right) \times 10 = 10$$

Tabla 48.

Resultado de la Característica Seguridad para la Herramienta Cisco Stealthwatch

Característica	Subcaracterística	Métrica	Valor	N. Evaluación	N. Puntuación
Seguridad	Métodos de Autenticación	Cumplimiento con seguridad de acceso	10	Excede de los objetivos	Satisfactorio

Tabla 49.

Evaluación de Métrica Facilidad de implantación para la Herramienta Cisco Stealthwatch

Característica:		Subcaracterística:		Métrica:
Portabilidad		Adaptabilidad		Facilidad de implantación
Funciones CSIRT-ESPE		Funciones de Cisco Stealthwatch	Cumplimiento	Documentación
Servicios Reactivos	Alertas y advertencias	Cisco Manager Console- Alarms	Si	https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html
	Manejo de Incidentes	Cisco Manager Console- Responding to Alarms	Si	https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html
	Manejo de vulnerabilidades	Cisco Manager Console- Host Groups	Si	https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html
	Manejo de artifa		No	

CONTINÚA 

Servicios Proactivos	Comunicados y alertas	Cisco Manager Console-Views and Dashboard	Si	https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html
	Difusión de información relacionada con la seguridad	Cisco Stealthwatch Community	Si	https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html
	Observatorio de tecnología	Cisco Stealthwatch Community	Si	https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html
	Evaluaciones o auditorias de seguridad	Cisco Manager Console-Working with Documents	Si	https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html
	Detección de intrusos	Cisco Manager Console-Monitoring Traffic and Network Performance	Si	https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html


$$X = \left(\frac{\text{Número de funciones y características con configuración e instalación documentadas}}{\text{Número de funciones requeridas}} \right) \times 10$$

$$X = \left(\frac{8}{9} \right) \times 10 = 8,89$$

Tabla 50.

Evaluación de Métrica Grado de coexistencia para la Herramienta Cisco Stealthwatch

Característica:	Subcaracterística:	Métrica:
Portabilidad	Coexistencia	Grado de coexistencia.
Funciones de Cisco Stealthwatch	Coexiste con otros softwares	Observaciones
Cisco Manager Console-Alarms	Si	Cisco Stealthwatch proporciona un conjunto de
Cisco Manager Console- Responding to Alarms	Si	API REST, que permite utilizar las funciones de Cisco Stealthwatch en cualquier lenguaje de

CONTINÚA 

Cisco Manager Console-Host Groups	Si	programación y coexistir con aplicaciones externas.
Cisco Manager Console-Views and Dashboard	Si	
Cisco Manager Console-Working with Documents	No	
Cisco Manager Console-Monitoring Traffic and Network Performance	Si	

$$X = \left(\frac{\text{Número de características compatibles}}{\text{Número de características probadas}} \right) \times 10$$

$$X = \left(\frac{5}{6} \right) \times 10 = 8,33$$

Tabla 51.

Resultado de la Característica Portabilidad para la Herramienta Cisco Stealthwatch

Característica	Subcaracterística	Métrica	Valor	Nivel de Evaluación	Nivel de Puntuación
Portabilidad	Adaptabilidad	Facilidad de implantación	8,89	Aceptable	Satisfactorio
	Coexistencia	Grado de coexistencia	8,33	Aceptable	Satisfactorio
		Promedio	8,61	Aceptable	Satisfactorio

Valores Obtenidos de la Herramienta Cisco Stealthwatch

Tabla 52.

Resultado General de la Herramienta Cisco Stealthwatch

Característica	Valor
Funcionalidad	10,00
Usabilidad	8,75
Fiabilidad	9,17
Eficiencia	8,60
Seguridad	10,00
Portabilidad	8,61

4.4 Análisis de Resultados e Informe Final

Informe Final del Modelo de Análisis y Selección de Herramientas de Ciberseguridad para el CSIRT Académico de la Universidad de las Fuerzas Armadas ESPE, Herramientas Analizadas: Nessus y Cisco Stealthwatch.

Mediante el modelo de evaluación establecido, se han obtenido resultados de dos herramientas analizadas: Nessus y Cisco Stealthwatch, tomando en cuenta los aspectos de calidad descritos en la norma ISO 9621 y mediante una ponderación de los resultados de estas características utilizando la matriz de priorización para enfatizarlas en el contexto de ciberseguridad, se realiza el análisis comparativo de ambas herramientas con la finalidad de proporcionar una guía para la toma de decisión en la adquisición de la herramienta para el caso CSIRT-ESPE.

Los resultados obtenidos en esta evaluación son los siguientes:

Tabla 53.

Cuadro comparativo del resultado de evaluación

Característica	Nessus	Cisco Stealthwatch
Funcionalidad	8,89	10
Usabilidad	8,3	8,75
Fiabilidad	8,75	9,17
Eficiencia	8,49	8,6
Seguridad	10	10
Portabilidad	8,61	8,61

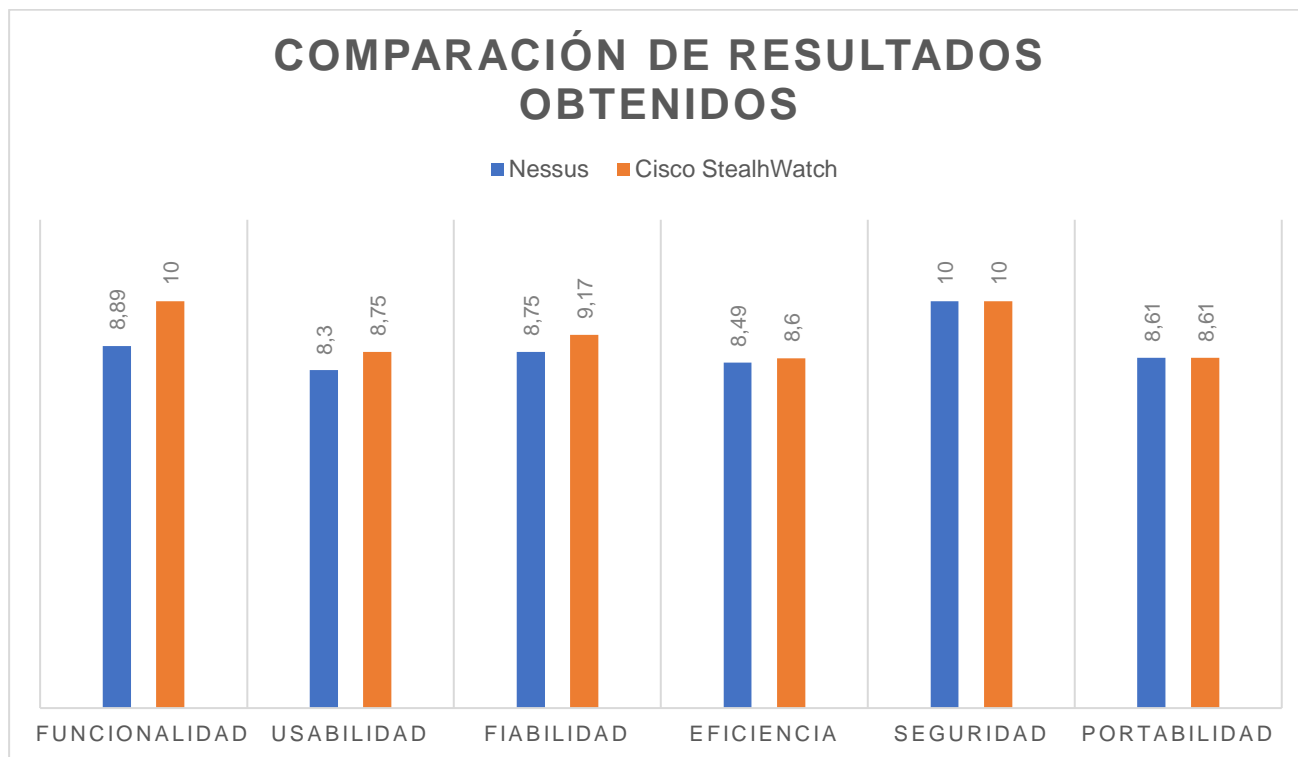


Figura 32. Comparación de resultados obtenidos

Como se puede apreciar, en el gráfico, ambas herramientas se encuentran dentro de los parámetros de calidad establecidos, según los niveles de evaluación se tiene resultados dentro de los siguientes rangos:

Tabla 54.

Niveles de resultados obtenidos en la evaluación

Nivel de Evaluación	Nessus	Cisco Stealthwatch
Aceptable	5	3
Sobrepasa los objetivos	1	3

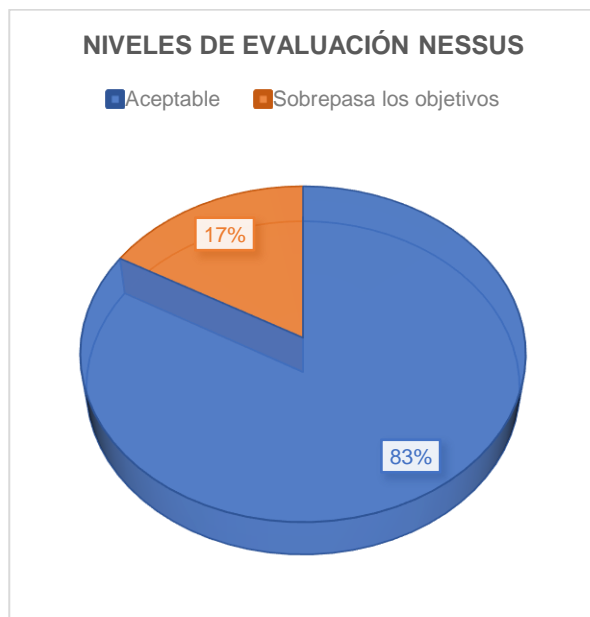


Figura 33. Niveles de evaluación de la Herramienta Nessus

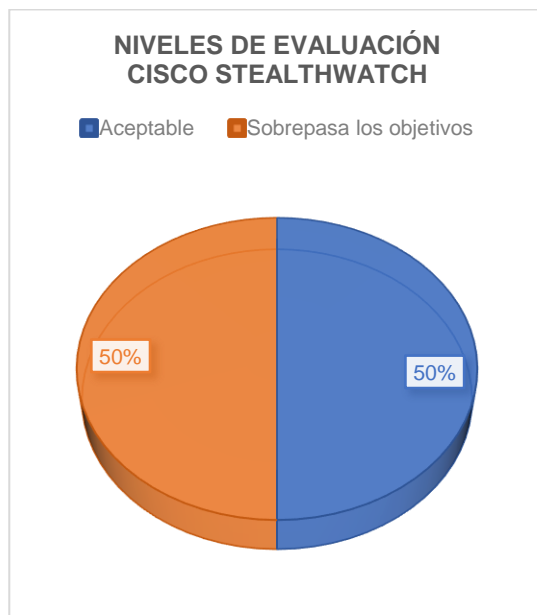


Figura 34. Niveles de evaluación de la Herramienta Cisco Stealthwatch

Para obtener la calificación final de la evaluación se utiliza la matriz de priorización de resultados obtenidos, la cual radica en dar ponderación a cada una de las características de calidad evaluada a través de las métricas, teniendo priorizado la calificación total como:

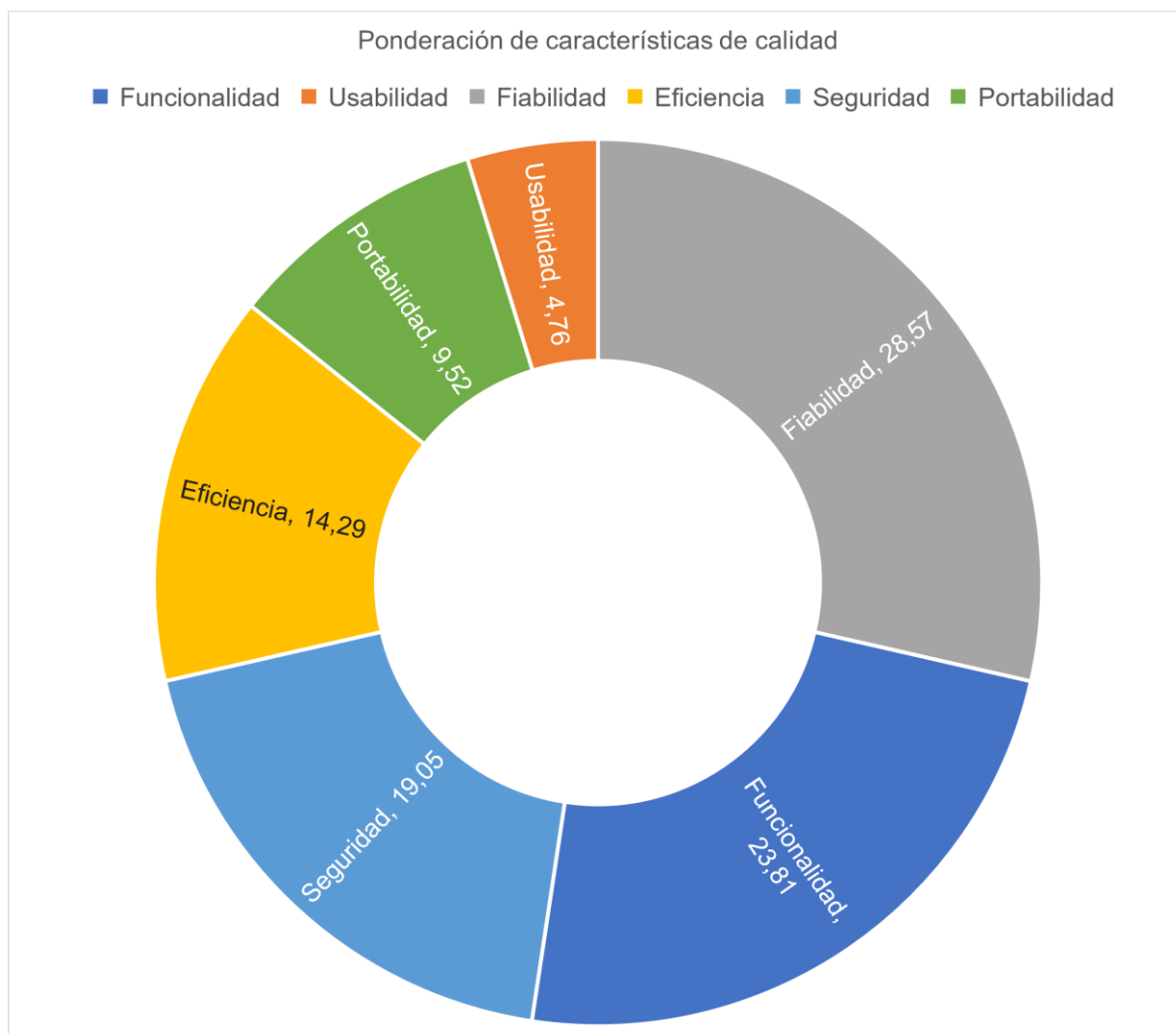


Figura 35. Ponderación de características de calidad

Tabla 55.
Resultados de Matriz de Comparación

	Funcionalidad	Usabilidad	Fiabilidad	Eficiencia	Seguridad	Portabilidad	
Coeficiente de Evaluación	23,81%	4,76%	28,57%	14,29%	19,05%	9,52%	100%
Nessus	8,89	8,30	8,75	8,49	10,00	8,61	8,95
Cisco Stealthwatch	10,00	8,75	9,17	8,60	10,00	8,61	9,37

4.5 Validación de Resultados

Selección de Herramientas de Ciberseguridad

La generación de informes documentados como salida de resultados del análisis de las herramientas de ciberseguridad estudiadas: Nessus y Cisco Stealthwatch, además del cuadro de comparación generado en el análisis de resultados, permiten al CSIRT-ESPE tomar una decisión acertada apoyándose de criterios de evaluación definidos en cumplimiento de sus funciones establecidas. En este caso de estudio se puede definir o concluir que la Herramienta de Ciberseguridad Cisco Stealthwatch se adapta mucho más a las solicitudes por cumplimiento de funciones por parte del CSIRT-ESPE, valores definidos por cálculos matemáticos como resultado de métricas de evaluación de software y normas ISO de Calidad de Software.

5. CAPITULO V

Conclusiones y Recomendaciones

5.1 Conclusiones

- Al terminar el proyecto de investigación, se establece que las herramientas que se usa en un CSIRT, deben facilitar la consecución de las actividades definidas por las funciones o servicios proactivos y reactivos del CSIRT, tales como: tratamiento de incidentes, gestión de vulnerabilidades, alertas, monitoreo y otros.
- La norma ISO-14598 definió marcos de trabajo de evaluación del producto software y la norma ISO-9126 identificó un modelo de calidad de software basado en métricas internas y externas, entre ambas proporcionan criterios de evaluación y aceptación de herramientas.
- El CSIRT-ESPE, prioriza la formación y entrenamiento de docentes y estudiantes en el área de seguridad, por esta razón sus servicios se enfocan en llevar a cabo este objetivo, para esto se requiere de herramientas de entrenamiento y gestión de incidentes de seguridad.
- Al finalizar el modelo e identificar cada actividad y proceso, se definió las etapas o fases, y estas son: justificación de la adquisición, proceso de evaluación y validación de los resultados, en cada uno de estas etapas se define la utilización de normas que permitieron elaborar un método genérico para la selección de herramientas de ciberseguridad.

5.2 Recomendaciones

- Establecer reuniones programadas por parte del CSIRT-ESPE, para tratar temas acerca de las funciones o servicios proactivos y reactivos, con cumplimiento de las herramientas de ciberseguridad seleccionadas, permiten recibir criterios de mejora en base a la experiencia en los resultados obtenidos, de esta manera el modelo de selección optimizará los procesos de análisis.
- Integrar más normas ISO referentes a la calidad del software, permitirán que el modelo de selección se involucre en resultados más detallados y minuciosos en su evaluación, se debe relacionar necesariamente con criterios de productos software de ciberseguridad.
- Se recomienda documentar todo proceso por experiencia de usuario por parte del CSIRT-ESPE en el uso de este modelo, ya que esto permitirá una retroalimentación y educación a futuros estudiantes que pertenecerán al CSIRT-ESPE.
- Se puede considerar el criterio de expertos de otros CSIRT académicos al momento de evaluar los procesos de las etapas definidas de evaluación y selección de este modelo, esto permitirá conocer puntos de vista diferentes y actualizar conocimientos de ciberseguridad.

5.3 Bibliografía

Andrade R, F. W. (2013). Diseño y dimensionamiento de un equipo de un equipo de respuesta ante incidentes de seguridad informática. *Congreso de ciencia y Tecnología ESPE*.

Astigarrá, E. (1999). *Universidad de Deusto*. Obtenido de El Método Delphi:
http://prospectiva.eu/zaharra/Metodo_delphi.pdf

Certification, G. S. (2018). *Certificación ISO 37001 - Sistema de gestión antisoborno - GlobalSTD*. Obtenido de Certificación ISO 37001 - Sistema de gestión antisoborno - GlobalSTD: <https://www.globalstd.com/certificacion/iso-37001>

Cisco. (21 de Febrero de 2019). *Cisco Stealthwatch*. Obtenido de Cisco Stealthwatch Enterprise:
https://www.cisco.com/c/es_es/products/collateral/security/stealthwatch/datasheet-es.html

Cisco Systems. (2017). *Cisco 2017 Annual Cybersecurity Report*. Obtenido de https://www.cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html

Código Orgánico de la Economía Social de los Conocimientos. (2006). *Artículo 144'*. Quito.

Código Orgánico Integral Penal. (2014). *COIP Artículo 234*. Quito.

- Consultores, A. (2019). *Aiteco Consultores - Matriz de Priorización*. Obtenido de Aiteco Consultores - Matriz de Priorización: <https://www.aiteco.com/matriz-de-priorizacion/>
- Cordero, Z. R. (01 de 06 de 2009). *La Investigación Aplicada*. San Jose, Costa Rica.
- Dalkey, N. C. (1972). *Experimental assessment of Delphi procedures with group value judgments*. Lexington: Lexington Books.
- Dalkey, N. C. (1972). *The Delphi method: An experimental study of group opinion*.
- De La Torre, H., & Parra, M. (2018). *Estrategia y diseño de un Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) académico para la Universidad de las Fuerzas Armadas ESPE. Perfil de Tesis de Grado*. Quito, Pichincha, Ecuador.
- Decreto Ejecutivo 1014. (2008). *Utilización de Software Libre en la Administración Pública*. Quito.
- Incidentes, E. d. (2018). *CSIRT*. Obtenido de CSIRT: <https://www.csirt.es/index.php/es/>
- Institution, T. B. (2016). *Anticorrupción y ética empresarial ISO 37001:2016*. Obtenido de Anticorrupción y ética empresarial ISO 37001:2016: <https://www.bsigroup.com/es-ES/ISO-37001-Anticorrupcion-y-etica-empresarial/>
- ISACA. (2017). *Glosario*. Obtenido de <https://www.isaca.org/Pages/Glossary.aspx>
- Krutz, R. L., & Vines, R. D. (2002). *The CISSP Prep Guide: Gold Edition*. En Krutz, Vines (págs. 8-11). New York, NY, USA: John Wiley & Sons, Inc.

- Lipson. (2002). *Tracking and Tracing Cyber-Attacks*. Pittsburgh: Carnegie Mellon Software Engineering Institute.
- Mahmood, T., & Afzal, U. (2013). Security Analytics: Big Data Analytics for Cybersecurity A Review of Trends, Techniques and Tools. *2013 2nd National Conference on Information Assurance (NCIA)* .
- Manadhata, P. K. (11 de 2018). *An Attack Surface Metric*. Pittsburgh: School of Computer Science Carnegie Mellon University. Obtenido de <http://reports-archive.adm.cs.cmu.edu/anon/2008/CMU-CS-08-152.pdf>
- Microsoft. (10 de Octubre de 2017). *Herramienta de Evaluación de Seguridad de Microsoft*. Obtenido de Herramienta de Evaluación de Seguridad de Microsoft: <https://docs.microsoft.com/es-es/security-updates/security/technetsecurityherramientadeevaluacindeseguridaddemicrosoftmsat>
- Moreno, J. Z. (2015). *Ciberdiccionario*.
- Nacional, A. (2010). *Ley del Sistema Nacional de Registro de Datos Públicos*.
- Nuix. (04 de 04 de 2019). *Nuix Plataforma Software*. Obtenido de <https://www.nuix.com/>
- Públicos, S. N. (2010). *Ley del Sistema Nacional de Registro de Datos Públicos*.
- Ron Egas, M., Velazques, C., Lafranco, Macias, & Diaz. (2017). *Practical Guide To Implement An Academic Computing Security Incident Response Team (Academic CSIRT)*.

Tenable. (2019). *Nessus*. Obtenido de Nessus: <https://es->

[la.tenable.com/products/nessus/nessus-professional](https://es-la.tenable.com/products/nessus/nessus-professional)

Vaclav Prenosil, M. H. (2016). *A Survey on Network Security Monitoring*

Implementations. Conference: 2016 IEEE 4th International Conference on Future

Internet of Things and Cloud Workshops (FiCloudW).

Van Der Heide, M. (2017). *Establishing a CSIRT*. Tahi CERT.

Wyk, K. v. (18 de 07 de 2007). *Penetration Testing Tools*. Obtenido de Build Security In:

<https://www.us-cert.gov/bsi/>