


**Universidad Nacional Mayor de San Marcos**

**Universidad del Perú. Decana de América**

Dirección General de Estudios de Posgrado

Facultad de Farmacia y Bioquímica

Unidad de Posgrado


# Propuesta de guía para la implementación de ciberseguridad en el ciclo de vida de sistemas computarizados y software de no producto en la industria farmacéutica

**TRABAJO ACADÉMICO**

Para optar el Título de Segunda Especialidad Profesional en Industria Farmacéutica


**AUTOR**

Rider Antonio CASTILLO SALIRROSAS

**ASESOR**

Mg. Mónica Guadalupe RETUERTO FIGUEROA



Lima - Perú

2025



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

https://creativecommons.org/licenses/by-nc-sa/4.0/

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

**Referencia bibliográfica**

Castillo R. Propuesta de guía para la implementación de ciberseguridad en el ciclo de vida de sistemas computarizados y software de no producto en la industria farmacéutica [Trabajo académico de segunda especialidad]. Lima: Universidad Nacional Mayor de San Marcos, Facultad de Farmacia y Bioquímica, Unidad de Posgrado; 2025.

## Metadatos complementarios

| | |
|---|---|
| **Datos de autor** | |
| Nombres y apellidos | Rider Antonio Castillo Salirrosas |
| Tipo de documento de identidad | DNI |
| Número de documento de identidad | 44685772 |
| URL de ORCID | https://orcid.org/0009-0004-0203-640X |
| **Datos de asesor** | |
| Nombres y apellidos | Mónica Guadalupe Retuerto Figueroa |
| Tipo de documento de identidad | DNI |
| Número de documento de identidad | 09481617 |
| URL de ORCID | https://orcid.org/0000-0001-8706-2789 |
| **Datos del jurado** | |
| **Presidente del jurado** | |
| Nombres y apellidos | Jorge Luis Arroyo Acevedo |
| Tipo de documento | DNI |
| Número de documento de identidad | 06785241 |
| **Miembro del jurado 1** | |
| Nombres y apellidos | Yovani Martín Condorhuamán Figueroa |
| Tipo de documento | DNI |
| Número de documento de identidad | 09597625 |
| **Miembro del jurado 2** | |
| Nombres y apellidos | Luis Alberto Inostroza Ruiz |
| Tipo de documento | DNI |

| | |
|---|---|
| Número de documento de identidad | 18089817 |
| **Miembro del jurado 3** | |
| Nombres y apellidos | Hugo Jesús Justil Guerrero |
| Tipo de documento | DNI |
| Número de documento de identidad | 40452674 |
| **Datos de investigación** | |
| Línea de investigación | No aplica. |
| Grupo de investigación | No aplica. |
| Agencia de financiamiento | Sin financiamiento. |
| Ubicación geográfica de la investigación | Universidad Nacional Mayor de San Marcos y sus coordenadas geográficas. |
| Año o rango de años en que se realizó la investigación | 2024 - 2025 |
| URL de disciplinas OCDE | Farmacología, Farmacia https://purl.org/pe-repo/ocde/ford#3.01.05 |

# ACTA DE SUSTENTACIÓN DE TRABAJO ACADÉMICO PARA OPTAR AL TÍTULO DE SEGUNDA ESPECIALIDAD PROFESIONAL EN INDUSTRIA FARMACÉUTICA

Siendo las **19:40 hrs. del 28 de febrero de 2025** se reunieron en la Unidad de Posgrado de la Facultad de Farmacia y Bioquímica de la Universidad Nacional Mayor de San Marcos, el Jurado de Trabajo Académico, presidido por el Dr. Jorge Luis Arroyo Acevedo e integrado por los siguientes miembros: Dr. Yovani Martín Condorhuamán Figueroa, Dr. Luis Alberto Inostroza Ruiz y el Dr. Hugo Jesús Justil Guerrero, para la sustentación oral y pública del trabajo Académico intitulada: **" Propuesta de guía para la implementación de ciberseguridad en el ciclo de vida de sistemas computarizados y software de no producto en la industria farmacéutica",** presentado por el **Q.F. Rider Antonio Castillo Salirrosas.**

Acto seguido se procedió a la exposición del trabajo Académico, con el fin de optar al Título de **Segunda Especialidad Profesional en Industria Farmacéutica**. Formuladas las preguntas, éstas fueron absueltas por el graduando.

A continuación, el Jurado de Trabajo Académico procedió a la calificación, la que dio como resultado el siguiente calificativo:

**17 DIECISIETE – MUY BUENO**

Luego, el Presidente del Jurado recomienda que la Facultad proponga que se le otorgue al **Q.F. Rider Antonio Castillo Salirrosas,** el Título de **Segunda Especialidad Profesional en Industria Farmacéutica.**

Siendo las 20:08 hrs. se levanta la sesión.

Se extiende el acta en Lima, a las 20:10 hrs. del 28 de febrero del 2025.

| | |
|---|---|
| Dr. Jorge Luis Arroyo Acevedo (P.P. T.C.)<br>Presidente | Dr. Yovani Martín Condorhuamán Figueroa (P. P. T.P.)<br>Miembro |
| Dr. Luis Alberto Inostroza Ruiz (P. P, T.P.)<br>Miembro | Dr. Hugo Jesús Justil Guerrero (P. Asoc, T.C.)<br>Miembro |

***Observaciones:***.....

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú, Decana de América

**CERTIFICADO DE SIMILITUD**

Yo, Mg. Mónica Guadalupe Retuerto Figueroa, en mi condición de asesora acreditado con el Dictamen N° 00026/FFB-UPG/2025 del trabajo académico, cuyo título es: **Propuesta de guía para la implementación de ciberseguridad en el ciclo de vida de sistemas computarizados y software de no producto en la industria farmacéutica**; presentado por el Q.F. **Rider Antonio Castillo Salirrosas,** para optar el Título de Segunda Especialidad Profesional en Industria Farmacéutica, CERTIFICO que se ha cumplido con lo establecido en la Directiva de Originalidad y de Similitud de Trabajos Académicos, de Investigación y Producción Intelectual. Según la revisión, análisis y evaluación mediante la plataforma PIDS, el documento evaluado cuenta con el **9**% de similitud, nivel PERMITIDO para continuar con los trámites correspondientes y para su publicación en el repositorio institucional.

Se emite el presente certificado en cumplimiento de lo establecido en las normas vigentes, como uno de los requisitos para la obtención del grado/ título/ especialidad correspondiente.

Lima, 27 de febrero de 2025

UNMSM
Firmado digitalmente por RETUERTO FIGUEROA Monica Guadalupe FAU 20148092282 soft
Motivo: Soy el autor del documento
Fecha: 27.02.2025 15:21:55 -05:00

Firma del Asesora _____

Nombres y Apellidos de la asesora, Mg. Mónica Guadalupe Retuerto Figueroa

DNI: 09481617

# ÍNDICE

**ABSTRACT** ..... **4**
**ÍNDICE DE TABLAS** ..... **5**
**ÍNDICE DE FIGURAS** ..... **6**
**ÍNDICE DE ACRÓNIMOS** ..... **7**
**CAPÍTULO I. INTRODUCCIÓN** ..... **8**
**1.2 Formulación del Problema** ..... 9
**1.3 Objetivos** ..... 10
**1.3.1 Objetivo general** ..... 10
**1.3.2 Objetivos específicos** ..... 10
**CAPÍTULO II. MARCO TEÓRICO** ..... **11**
**2.1 Antecedentes de la investigación** ..... 11
**2.2. Bases teóricas** ..... 13
**2.2.1 Ciclo de vida de sistema computarizado:** ..... 13
**2.2.2 La Ciberseguridad:** ..... 15
**CAPÍTULO III. METODOLOGÍA** ..... **17**
**3.1 Tipo de Investigación** ..... 17
**3 2. Consideraciones éticas (de ser el caso)** ..... 17
**3.3. Diseño metodológico** ..... 17
**3.4. Criterios de selección** ..... 18
**3.4.1. Criterios de inclusión** ..... 18
**3.4.2. Criterios de exclusión** ..... 18
**3.5. Técnicas o instrumentos de recolección de la información o de datos** ..... 18
**3.6. Procesamiento de la información o de datos** ..... 18
**CAPÍTULO IV. RESULTADOS** ..... **21**
**4.1 Propuesta** ..... 21
**4.2 Validación de la propuesta: Resultados de validez CVC** ..... 26
**4.3 Resultados de validez Coeficiente Alfa de Cronbach.** ..... 36
**CAPÍTULO V. DISCUSIÓN** ..... **39**
**CAPÍTULO VI. CONCLUSIONES** ..... **41**
**CAPÍTULO VII. REFERENCIAS BIBLOGRÁFICAS** ..... **42**
**CAPÍTULO VIII. ANEXOS** ..... **44**

## RESUMEN

El presente trabajo académico tiene por objetivo elaborar una guía para la implementación de ciberseguridad en el ciclo de vida de sistema computarizado y software de no producto en la industria farmacéutica, de tal manera que pueda servir de línea base para proteger los sistemas frente a posibles ataques y amenazas en el medio cibernético. La elaboración de la guía sigue un diseño descriptivo transversal, analizando las guías de referencia relacionadas a ciberseguridad con enfoque en el ciclo de vida de los sistemas computarizados y software de no producto como son la fase de concepto, proyecto, operación y retiro. Para el procesamiento de la información se utilizó el coeficiente de validez de contenido (CVC) y la fiabilidad o confiabilidad mediante el Alfa de Cronbach obteniendo resultados satisfactorios. Como conclusión del trabajo académico se espera que esta guía sirva como lineamiento para implementar controles de ciberseguridad en el ciclo de vida de los sistemas computarizados y software de no producto en la industria farmacéutica nacional e internacional garantizando así la protección de los datos, la integridad de los datos, y en líneas generales todos los activos de información.



Palabras clave: Ciberseguridad, sistema computarizado, software no producto, ciclo de vida, fiabilidad, datos

## ABSTRACT

The purpose of this academic work is to develop a guide for the implementation of cybersecurity in the life cycle of computerized systems and non-product software in the pharmaceutical industry, so that it can serve as a baseline to protect systems against possible attacks and threats in the cyber environment. The development of the guide follows a cross-sectional descriptive design, analyzing the reference guides related to cybersecurity with a focus on the life cycle of computerized systems and non-product software such as the concept, project, operation and retirement phases. For the processing of the information, the coefficient of content validity (CVC) and the reliability or trustworthiness through Cronbach's Alpha were used, obtaining satisfactory results. As a conclusion of the academic work, it is expected that this guide will serve as a guideline to implement cybersecurity controls in the life cycle of computerized systems and non-product software in the national and international pharmaceutical industry, thus guaranteeing the protection of data, data integrity, and in general all information assets.



Keywords: Cybersecurity, computer system, non-product software, life cycle, reliability, data.

## ÍNDICE DE TABLAS

**Tabla 1** Interpretación de Valores CVC…….19

**Tabla 2** Interpretación de valores de Alfa de Cronbach…….20

**Tabla 3** Puntos (52 ÍTEMS) propuestos en la guía…….21

**Tabla 4** Resultados de la evaluación del instrumento por criterio de expertos……..26

**Tabla 5** Resultado del CVC por ítem…….31

**Tabla 6** Resultado de la encuesta……37

**Tabla 7** Resultado del CVC por ítem Coeficiente Alfa de Cronbach…….37

## ÍNDICE DE FIGURAS

**Figura 1** Ciclo de vida del sistema computarizado…….13

**Figura 2** Fases del ciclo de vida…….15

**Figura 3** Relación entre seguridad de internet, seguridad web, seguridad de red y ciberseguridad……...……16

**Figura 4** Criterios de guía de ciberseguridad……..17

**Figura 5** Valor promedio (Mx) de los 5 expertos y su relación con cada ítem……..26

# ÍNDICE DE ACRÓNIMOS

**GAMP 5:** Buenas prácticas de fabricación automatizada

**ISO:** Organización internacional de estandarización

**CFR21:** Código de reglamento federal

**NIST**: Instituto Nacional de Estándares y Tecnología

**IOT**: Internet de las cosas

**DES:** Simulación de eventos directos

**OSI:** Interconexión de sistemas abiertos

**SD:** Dinámica de Sistemas

**URS:** Especificación de requerimientos de usuario

**FRS:** Especificación de requerimientos funcionales

**PLC:** Controlador lógico programable

**LIMS:** Sistema de gestión de información de Laboratorio

# CAPÍTULO I. INTRODUCCIÓN

Con la evolución de la tecnología, la inteligencia artificial y la industria 4.0; hace que puedan existir altos riesgos en materia de seguridad de la información, los mismos que deben ser analizados, evaluados y gestionados de una manera adecuada con el objetivo de garantizar los principios básicos de los datos: confidencialidad, integridad, disponibilidad y resiliencia de los datos e información. La ciberseguridad con alcance a la industria farmacéutica es una práctica mediante la cual se protege los dispositivos electrónicos, especialmente los que almacenan información con la finalidad de generar back up, restauración, guardado de datos y proteger de ataques cibernéticos y/o de accesos no autorizados (6).

En los sectores donde se maneje información sensible o que simplemente esta información esté representada como un alto valor en el mercado y forme parte de sus operaciones, siempre estarán en el punto de ataque por ciber amenazas, para lo cual se deben implementar controles de prevención, detección y el sector debe tener una alta capacidad de respuesta para hacer frente a estas grandes amenazas.

Especialmente la información que se almacena en el sector farmacéutico es muy sensible, de alto valor en el mercado y muy vista por las ciber amenazas, ya que estas son muy valiosas y resultan ser mejor pagadas tanto por las patentes, fórmulas, guías de manufactura, registros sanitarios y otros. Los ataques industriales y las vulnerabilidades han alcanzado cifras alarmantes en los últimos años, por lo que resulta trascendental implementar lineamientos para proteger los activos de información (3).

Debido a lo antes indicado, la industria farmacéutica debe, en definitiva, investigar y desarrollar proyectos con un nivel técnico y practico que garantice la seguridad de la información. Se debe tener en cuenta que existen dos tipos de empresas: las que han sido atacadas y que no saben que ya han sido atacadas.

De acuerdo con la ISO IEC 27032:2023, segunda edición, “Ciberseguridad: Directrices para la seguridad de internet”, la ciberseguridad puede gestionar riesgos cuando los activos de información, sistemas computarizados y software de no producto se encuentran

conectados a red o están en un formato digital por computadora o en medios de almacenamiento y redes. Por otro lado, hay una serie de controles, técnicas y métodos de seguridad de la información aplicables a mantener una revisión periódica de los riesgos que existen. La seguridad de la red está basada en etapas como el diseño, implementación, operación y oportunidades de mejora en las redes, por lo que existirán controles para identificar, evaluar y mitigar los riesgos de seguridad relacionadas dentro de las empresas farmacéuticas, entre empresas y entre estas y los usuarios que la manejan (9).

De acuerdo con GAMP5 (Buenas prácticas de fabricación automatizada) para poder asegurar el cumplimiento del sistema computarizado de acuerdo con su uso previsto y a lo largo de su ciclo de vida, se debe seguir un enfoque integral, el mismo que debe estar dirigido a las siguientes fases: Concepto, proyecto, operación y retiro (7).

Es por ello, que se ha identificado que en las Plantas Farmacéuticas es posible implementar el proceso de Ciberseguridad en las diferentes áreas del negocio y de su sistema de gestión de la calidad. En estas áreas de la planta se encuentran ubicados, de acuerdo con la forma farmacéutica, equipos de dispensación, fabricación y envasado, equipos de Laboratorio (Materia prima, producto terminado, estabilidades, microbiología), aplicaciones y sistemas computarizados, sistemas globales; los cuales deben seguir un proceso de Validación de Sistemas computarizados asociado al cumplimiento de data integrity en los que se deben verificar la gestión de accesos, revisión del audit rail, gestión del backup correspondientes. Además, se debe verificar las vulnerabilidades, amenazas y ataques a la información (de los datos) que hoy en día se vuelven un activo importante y monetizable ya que la información tiene un poder incalculable para la industria farmacéutica donde esta información es sensible y confidencial.

## 1.2 Formulación del Problema

¿Cuáles son los lineamientos que se debe seguir en la implementación de ciberseguridad en el ciclo de vida de sistemas computarizados y software de no producto en la industria farmacéutica?

## 1.3 Objetivos

### 1.3.1 Objetivo general

Elaborar una propuesta de guía para la implementación de ciberseguridad en el ciclo de vida de sistemas computarizados y software de no producto en la industria farmacéutica.

### 1.3.2 Objetivos específicos

1.3.2.1 Establecer los lineamientos específicos para la implementación de ciberseguridad en la fase concepto del ciclo de vida en el sistema computarizado y software de no producto.

1.3.2.2 Establecer los lineamientos específicos para la implementación de ciberseguridad en la fase proyecto del ciclo de vida en el sistema computarizado y software de no producto.

1.3.2.3 Establecer los lineamientos específicos para la implementación de ciberseguridad en la fase operación del ciclo de vida del sistema computarizado y software de no producto.

1.3.2.4 Establecer los lineamientos específicos para la implementación de ciberseguridad en la fase retiro del ciclo de vida del sistema computarizado y software de no producto.

# CAPÍTULO II. MARCO TEÓRICO

## 2.1 Antecedentes de la investigación

Solfa et al. En el 2022, desarrolló una investigación respecto a la seguridad cibernética, el riesgo que representa en todo el eslabón de la cadena de suministro y su impacto relacionado en las operaciones digitales involucradas. Esta investigación siguió un enfoque analítico y descriptivo. Respecto a los resultados que se obtuvieron son trazables, positivos y significativos, llegando a recomendar algunas mejoras respecto a las tecnologías digitales en la industria farmacéutica para llegar a almacenar datos y la información de manera más segura y sobre todo confiable con los registros sanitarios, fórmulas y toda la información. Este modelo busca también optimizar los procesos y tener riesgos medidos previamente. De manera general, la industria farmacéutica debe desarrollar un plan para llegar a implementar la ciberseguridad (1).

Fuenzalida et al. En el 2022, realizó una investigación sobre la ejecución de una validación de sistema computarizado en software con alcance a un equipo de laboratorio de control de calidad (software chemStation) con el objetivo de garantizar el cumplimiento del CFR 21 en Chile – Laboratorio Synthon Ltda. Esta validación estuvo basada en la generación de protocolos y reportes de validación, los mismos que fueron aplicados tomando en cuenta la GAMP 5, mantenimiento un enfoque tipo prospectivo y su metodología se centró en el ciclo de vida del sistema computarizado. Este equipo de control de calidad y su software chemStation se trataba de un equipo legado (histórico), durante la investigación se encontraron observaciones y/o mejoras como: se debe incrementar los controles para generar copias de seguridad, revisión de Audit Trail, control de accesos y de los usuarios. Por otro lado, se pone énfasis en que la validación de sistemas computarizados es un proceso importante y no debe dejarse de lado, por lo que debe cumplirse con todos los estándares de calidad en base a las guías de referencia (2).

Pircalaboui et al. En el 2024, indica que en el sector farmacéutico al gestionar altas cantidades y volúmenes de información y generar una inversión elevada en el diseño y desarrollo de productos o medicamentos nuevos, la información que se gestiona es muy sensible y debe ser protegida, evaluada y gestionada para su éxito y sostenibilidad

mediante la implementación de controles de amenazas cibernéticas como malware, Pishing, ransomware, amenazas internas y ataques a la IOT (internet de las cosas) dentro de los sistemas de información. Indica también que se debe identificar las principales amenazas y vulnerabilidades, dado que un ataque o alteración de los datos puede traer consigo grandes pérdidas financieras, así como la perdida de la reputación, la marca y hasta amonestaciones legales. Con el avance tecnológico, la industria 4.0 y la transformación digital, las empresas farmacéuticas en todo el mundo están implementando controles en sus equipos, sistemas computarizados y software con el objetivo no solo de optimizar los procesos sino también como la proteger la información dado que esta es confidencial y sensible. De esta manera se mantendrá también, la confianza en los clientes (3).

En un estudio realizado en el Perú por Arenas en el 2023, basado en la ISO27032 y la NIST (Instituto Nacional de Estándares y Tecnología) indica que, en los últimos años, el número de los ciberataques han tenido una tendencia creciente. Se indica, además, que riesgos cibernéticos se presentan tanto en empresas grandes como pequeñas por lo que es necesario que las empresas cuenten con una herramienta que les ayude a prevenir las amenazas proponiendo seguir un modelo de madurez de ciberseguridad. El modelo propuesto fue construido tomando en cuenta la ISO 27032 y la NIST, es por ello que se definieron 4 etapas: Inicial, definido, establecido y mejorado, pudiendo ser que cualquier persona puede utilizar el modelo con bastante facilidad sin necesidad de alguna asistencia. De acuerdo con los resultados para la validación, 15 expertos fueron los que participaron en el proceso donde se evaluaron y en donde se les aplicó un cuestionario y sus respuestas fueron tomadas de manera positiva, demostrando así que el modelo cumple con su propósito de ser una herramienta útil para que las empresas evalúen de manera rápida y automatizada la seguridad de sus equipos, sistemas computarizados y aplicaciones (4)

En Estados Unidos, Kannan en el 2022, realizó un estudio con enfoque en industria farmacéutica con la finalidad de analizar ataques cibernéticos mediante un modelo de ciberseguridad en el que se incluyó detalles específicos de la infraestructura de la red, las configuraciones de seguridad y una lista de posibles amenazas y vulnerabilidades. La implementación de ciberseguridad permite a una empresa seguir acciones de los atacantes y evaluar el nivel de riesgo del sistema utilizando conocimiento sobre la infraestructura y los controles de seguridad de la información implementados. La DES (técnicas de

simulación de eventos discretos se usa normalmente en la simulación de redes o en la modelación de redes, esto significa que las defensas ante los ciberataques se pueden notar desde la capa 3 (que es una capa de red) del modelo OSI (Interconexión de sistemas abiertos), esto puede ocultar ataques fortuitos o ataques indirectos a capas superiores del modelo OSI. La SD (dinámica de sistemas) es un método que sirve para entender como es el comportamiento y/o evolución a lo largo del tiempo y como puede llegar a interactuar con los componentes y el rendimiento del sistema. Esta investigación logró modelar redes por computadora para investigar ciberataques indirectos y sus posibles efectos (5).

Devliyal et al en el 2024, se realizó un estudio con alcance a las técnicas de detección de los ataques cibernéticos en sistemas físicos en el servicio de atención farmacéutica, los mismos que lograron demostrar que son utilizados en la industria en salud con el objetivo de brindar una atención especial a los pacientes en las diversas situaciones clínicas que se presenten. En este sector existe una alta gama de equipos médicos, biomédicos, que requieren soluciones de seguridad avanzada. Este estudio se ejecutó con el objetivo de identificar distintos tipos de amenazas y vulnerabilidades. Por otro lado, en el sector farmacéutico se trabaja con una gran cantidad de información como la propiedad intelectual, datos de investigación, registros médicos, información y datos confidenciales. Se indica también que la industria farmacéutica tiene una gran responsabilidad de garantizar que los datos e información este debidamente protegida (6).

## 2.2. Bases teóricas

### 2.2.1 Ciclo de vida de sistema computarizado:

Para alcanzar el cumplimiento y la adecuación del sistema computarizado y software de no producto para su uso previsto en el ciclo de vida del software, se debe cumplir un enfoque general de acuerdo con las siguientes fases a continuación (7):

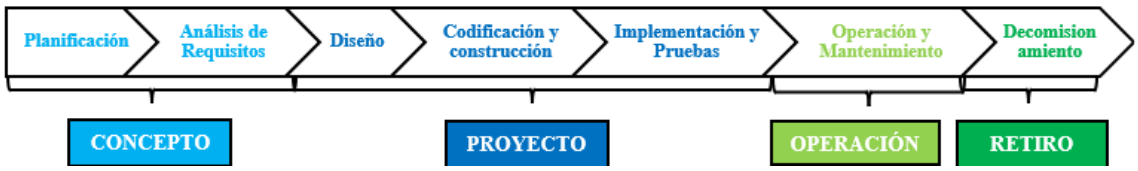



**Figura 1:** Ciclo de vida del sistema computarizado
**Fuente:** Autor, 2025

#### 2.2.1.1 Planificación

En esta etapa se determina el objetivo, tamaño, alcance y complejidad del sistema computarizado para establecer el flujo de actividades, responsabilidades, tiempos y documentación como entregables para desarrollar, instalar y mantener el sistema.

#### 2.2.1.2 Análisis de Requisitos

En esta etapa se documenta las especificaciones de requisitos de usuario y especificaciones de requisitos funcionales y también lo que están relacionados a nivel del sistema.

#### 2.2.1.3 Diseño

En la etapa de diseño, específicamente las especificaciones describen funciones de software, como se implementa a nivel de diseño y también la estrategia para mitigar los riesgos.

#### 2.2.1.4 Codificación y Construcción

En la etapa de codificación y construcción implementa el diseño del sistema en código fuente y/o ajustes de configuración para su uso previsto en la plataforma de hardware de destino.

#### 2.2.1.5 Implementación y Pruebas

En esta etapa se realiza una verificación de que el sistema funcione de acuerdo con los requerimientos aprobadas para dar paso a la ejecución de las pruebas.

#### 2.2.1.6 Operaciones y mantenimiento

Esta etapa se inicia después de instalar el hardware y/o software en el entorno productivo.

#### 2.2.1.7 Decomisionamiento o retiro

Esta es la última etapa es la de retiro, donde se elimina un sistema, software de no producto o una aplicación del ambiente productivo para darse de baja también en el sistema de calidad.

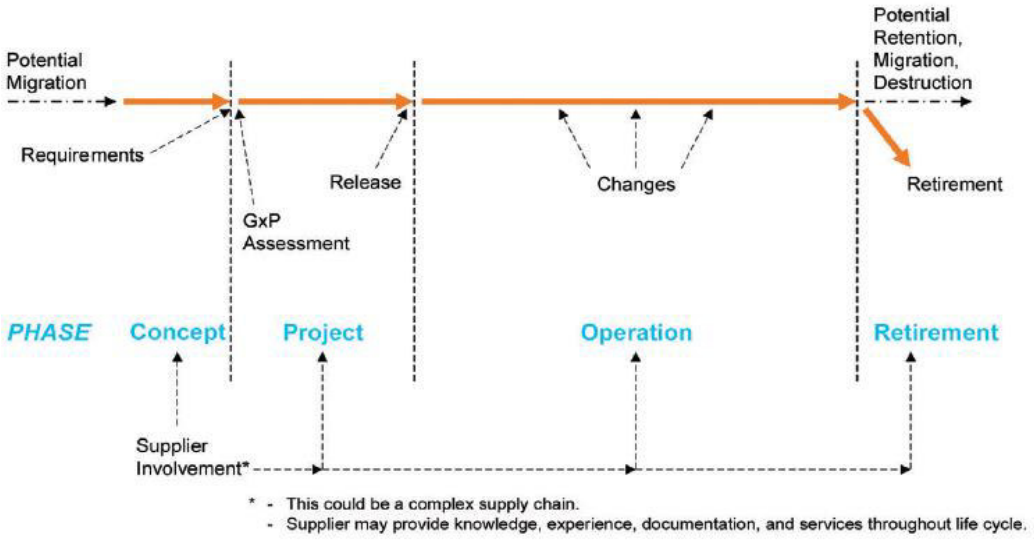



**Figura 2:** Fases del Ciclo de vida
**Fuente:** GAMP 5, versión 2.0, 3.1 Computerized System Life Cycle

### 2.2.2 La Ciberseguridad:

La seguridad de red se centra en el diseño, implementación, operación y mejora de las redes, así como en la identificación y mitigación de los riesgos de seguridad relacionados con las redes dentro de las empresas, entre empresas y entre estas y los usuarios quienes son finalmente quienes usan los activos de información (8) (9).

Por su parte, la ciberseguridad gestiona los riesgos asociados con la seguridad de la información en todos los niveles y esta se encuentra en formatos digitales por computadoras, dispositivos de almacenamiento para generar guardado de los datos o back up y redes. Diversos controles, métodos y técnicas de seguridad de la información son aplicables para gestionar los riesgos cibernéticos.

Asimismo, la ciberseguridad se enfoca en proteger los sistemas conectados a Internet, incluyendo hardware, software, programas y datos, frente a posibles ataques. Estos ataques suelen ser selectivos, sofisticados y persistentes. Las amenazas pueden originarse en Internet o derivarse de la conectividad con otras redes y sistemas dentro de la organización, así como con la red de clientes y proveedores de servicios con los que la organización interactúa en el curso de sus actividades comerciales.

La presente propuesta de guía deberá ser trazable con las fases del ciclo de vida del sistema computarizado, mediante sus etapas correspondientes.

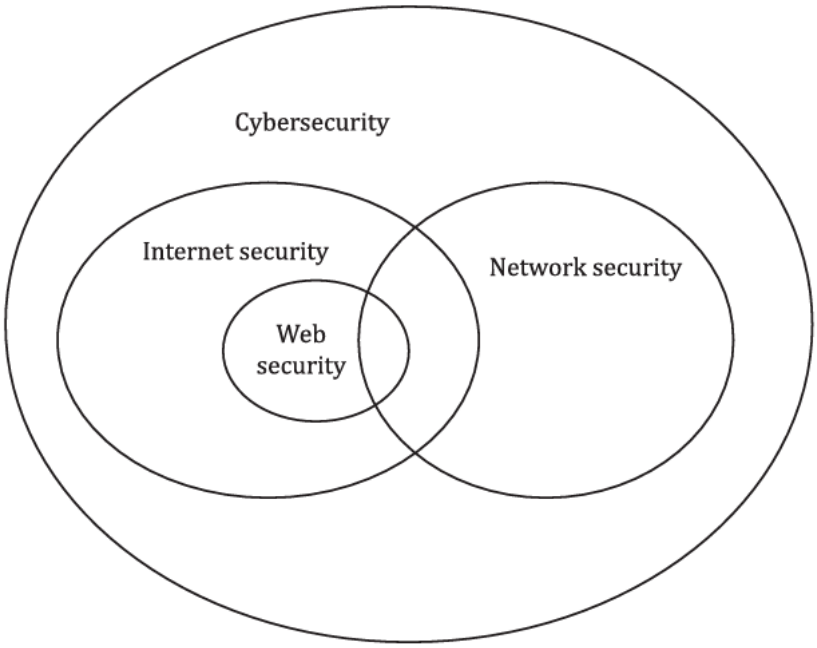



**Figura 3:** Relación entre seguridad de Internet, seguridad web, seguridad de red y Ciberseguridad
**Fuente:** ISO IEC 27032:2023, second edition. Cybersecurity — Guidelines for Internet security.

## CAPÍTULO III. METODOLOGÍA

### 3.1 Tipo de Investigación

El trabajo de investigación de acuerdo con el (11):

-Método de investigación: Inductivo
-Enfoque de investigación: Cualitativo
-Tipo de investigación: Básica
-Diseño de la investigación: Descriptivo transversal

### 3 2. Consideraciones éticas (de ser el caso)

No aplica

### 3.3. Diseño metodológico

Para el desarrollo del presente trabajo académico el cual sigue un diseño descriptivo transversal, de tal manera que se pueda recolectar y analizar la data de información para implementar la guía de ciberseguridad en el ciclo de vida del sistema computarizado y software de no producto en la industria farmacéutica y con una fecha de publicación no mayor a diez años, generadas en américa latina y en Europa (12).

Los criterios establecidos para el presente trabajo para analizar la guía son con un enfoque en el ciclo de vida del sistema computarizado: concepto, proyecto, operación y retiro.

Una vez obtenidos los resultados, se van a analizar e interpretar obteniendo inferencias cualitativas, las cuales son base para la elaboración de la guía:

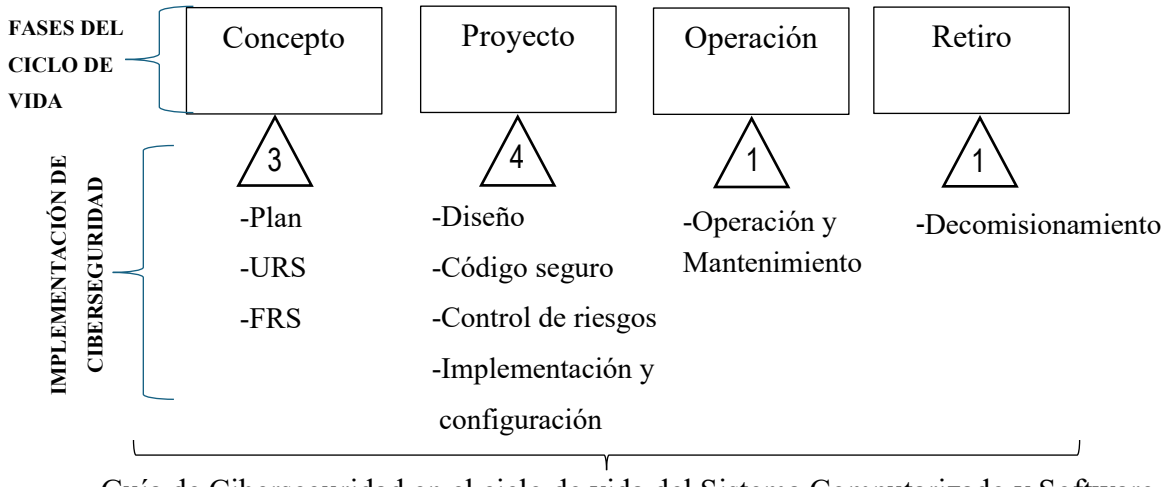



**Figura 4:** Criterios de guía Ciberseguridad
**Fuente:** GAMP 5, versión 2.0, Computerized System Life Cycle

Se valora el grado de acuerdo de los expertos (el autor recomienda la participación de cinco), los cuales deben tener una experiencia mínima de 5 años en validación de sistemas computarizados, soporte de tecnologías de información, calidad, calificaciones, validaciones) respecto a cada uno de los diferentes ítems (criterios de las guías) y al instrumento en general. Para ello, tras la aplicación de una escala tipo Likert de cinco alternativas (siendo 1 mínimo y 5 máximo puntaje), se calcula la media obtenida en cada uno de los ítems y, en base a esta, se calcula el CVC (coeficiente de validez de contenido) para cada elemento, evaluando el nivel de concordancia entre las guías (13).

### 3.4. Criterios de selección

#### 3.4.1. Criterios de inclusión

Sistemas computarizados y software de no producto, utilizados en la fabricación de productos como controladores lógicos programables (PLC) en equipos heredados o nuevos, sistemas de inspección visual automatizada, sistemas de gestión de calidad.

#### 3.4.2. Criterios de exclusión

Sistemas computarizados y software de producto, como productos médicos y no médicos que contienen software y firmware o lógica programable y que se consideran parte de un sistema interoperable y dispositivos heredados.

### 3.5. Técnicas o instrumentos de recolección de la información o de datos

Los datos que se recopilarán para dicho estudio se basan en la posibilidad de poder obtener información bibliográfica por medios físicos (documentos impresos) o digitales (documentos en formato pdf, word o en línea), acerca de las guías implementadas en la industria farmacéutica para sistemas computarizados y software de no producto (13).

### 3.6. Procesamiento de la información o de datos

Entre varios métodos de juicio para el panel de expertos, utilizaremos el método basado en Hernández-Nieto citado por Pedrosa, en el que el coeficiente de validez de contenido

(CVC) nos permite evaluar la confiabilidad de la validez de opinión entre los cinco expertos relacionados con los diferentes ítems y herramienta general. Por lo tanto, luego de usar una escala de tipo likert con cinco sugerencias, se evaluó el valor promedio obtenido en cada ítem y con base en ello se evaluó el CVC de cada componente (13).

Coeficiente de validez de contenido (CVC):

$$CVCi = Mx / Vmáx$$

Mx: Valor promedio de este elemento en las puntuaciones otorgadas por los expertos.
Vmáx: La puntuación más alta que cada ítem de clasificación puede obtener.
Para cada ítem se calculará el error (Pei), reduciendo así el sesgo que pueda introducir cualquier juez o experto, dado por Pei = (1/j)j, donde j es el número total de expertos.

Finalmente, el CVC se calculará aplicando CVC = CVCi – Pei y como criterio de aceptación se recomienda que estos elementos se mantengan como CVC es mayor que 0.80 (13), aunque algunos criterios menos estrictos establecen valores superiores a 0.70. Ver siguiente tabla:

Tabla 1 Interpretación de Valores CVC

| VALOR (CVC) | INTERPRETACIÓN |
|---|---|
| <0.60 | Validez y concordancia inaceptables |
| >0.60 y <0.70 | Validez y concordancia deficientes |
| >0.70 y <0.80 | Validez y concordancia aceptables |
| >0.80 y <0.90 | Validez y concordancia buenas |
| >0.90 | Validez y concordancia excelentes |

Nota: Fuente Avances Teóricos y Métodos para su estimación (13)

**Criterios de selección para construir el panel de expertos:**

1.- Poseer título de Químico Farmacéutico e Ingeniero de Sistemas.

2.- Contar con más de 5 años de experiencia en las áreas de Calidad, Validaciones, Calificaciones, Integridad de datos, Ciberseguridad, Tecnologías de la información y soporte TI, ANEXO I.

**Criterios para la evaluación del instrumento**

**1.- COHERENCIA.** El ítem mide el grado de correspondencia entre el enunciado y lo que se pretende medir.

**2.- CLARIDAD.** El ítem es claro (no genera confusión o contraindicaciones)

**3.- ESCALA.** El ítem puede ser respondido de acuerdo con la escala que presenta el documento.

**4.- RELEVANCIA.** El ítem es relevante para cumplir con las preguntas y objetivos de investigación.

**Indicadores de evaluación del instrumento**

Escala de valores o Likert, según: Valor 1: Inaceptable, Valor 2: Deficiente, Valor 3: Regular, Valor 4: Bueno, Valor 5: Excelente.

Con base en la evaluación del experto, éste adoptará el formato de evaluación de instrumentos que se muestra en el ANEXO II.

Para determinar la confiabilidad del instrumento se encuestó a (10) químicos farmacéuticos e ingenieros de sistemas con experiencia relacionada con el proceso de sistemas computarizados, data integrity, ciberseguridad, soporte TI que laboran en el sector farmacéutico, con la propuesta de "guía de implementación de ciberseguridad en el ciclo de vida del sistema computarizados y software de no producto", según la encuesta del ANEXO III (está encuesta tiene un enfoque basado en los indicadores de la operacionalización de las variables o documentos mínimos que se pueden formar parte de la implementación de ciberseguridad), en donde señalaron su calificación y sugerencias para la mejora del mismo, se evaluó la confiabilidad del instrumento a través del coeficiente afa de cronbach (14).

Tabla 2. Interpretación de valores de Alfa de Cronbach

| **VALOR (α de Cronbach)** | **INTERPRETACIÓN** |
|---|---|
| < 0.5 | Es inaceptable |
| > 0.5 y < 0.60 | Es pobre |
| > 0.60 y < 0.70 | Es cuestionable |

| | |
|---|---|
| > 0.70 y < 0.80 | Es aceptable |
| > 0.80 y < 0.90 | Es bueno |
| > 0.90 | Es excelente |

Nota. Fuente Avances Teóricos y Métodos para su Estimación

## CAPÍTULO IV. RESULTADOS

### 4.1 Propuesta

La propuesta de guía para la implementación de ciberseguridad en el ciclo de vida de sistemas computarizados y software de no producto en la industria farmacéutica proporciona un enfoque holístico de la ciberseguridad a través de la gestión del ciclo de vida seguro diseñado para garantizar que los productos, los sistemas de fabricación, sistemas de laboratorio y los sistemas de gestión de datos de calidad son resistentes a las amenazas y vulnerabilidades de ciberseguridad y puedan prevenir, detectar, responder y recuperarse adecuadamente, por lo que, a continuación se detalla los criterios mínimos establecidos en la presente guía:

**Tabla 3: Puntos (52 ÍTEMS) propuestos en la guía:**

De acuerdo con la guía propuesta se han establecido estos criterios para implementar los lineamientos de ciberseguridad en las fases del ciclo de vida (concepto, proyecto, operación y retiro) de sistema computarizado y software de no producto. La guía estandarizada se encuentra en el ANEXO IV.

Tabla 3 Puntos (52 ítems) propuestos en la guía:

| **FASE CONCEPTO** | | |
|---|---|---|
| **A** | **PLANIFICACIÓN** | |
| - | **Inventario** | |
| 1 | ¿Equipo está conectado a red? ¿red con salida a internet? (mencionar IP/link) | **Actividad/operación/variable**<br>Plan de implementación de ciberseguridad<br>**Objetivo:** |
| 2 | ¿Se encuentra instalado en PC? Mencionar RAM/Procesador / capacidad Disco Duro | |
| 3 | ¿Cuenta con monitor/PC/laptop o HMI? | |

| | | |
|---|---|---|
| 4 | ¿El software se encuentra en más de 01 PC? | Implementar un plan que permita establecer lineamientos específicos ante amenazas y vulnerabilidades en sistemas computarizados y software de no producto |
| 5 | ¿Cuenta con Sistema operativo? Indicar versión | |
| 6 | ¿Software cuenta con actualizaciones y parches de seguridad? ¿Se tiene algún plan/procedimiento? | |
| 7 | ¿Se cuenta con planes/procedimientos de recuperación ante desastres de software? Indicar | |
| 8 | ¿Se cuenta con un plan de implementación de ciberseguridad en la organización? Indicar | |
| **B** | **ANÁLISIS DE REQUISITOS** | |
| - | **Especificación de requisitos de usuario (URS) / funcionales (FRS)** | |
| 9 | Gestionar documentos técnicos para establecer requisitos del usuario con lineamientos de ciberseguridad (data integrity, vulnerabilidad, parches de seguridad, requisitos de recuperación, gestión de interfaces, entre otros | **Actividad/operación/variable**<br><br>Especificación de requerimientos de usuario (Especificación de requerimientos funcionales.<br><br>**Objetivo:**<br><br>Gestionar documento técnico que especifique los requisitos de usuario y funcionales (ítem 9). |
| 10 | Identificar necesidades y expectativas del sistema computarizado y software de no producto | |
| 11 | Requisitos de la seguridad física, cuando sea apropiado | |
| 12 | Consideraciones para los componentes de hardware y software | |
| 13 | Establecer requisitos bajo concepto básico de ciberseguridad: **Confidencialidad, integridad y disponibilidad.** | |
| **FASE PROYECTO** | | |
| **C** | **DISEÑO** | |
| - | **Seguridad por diseño** | |
| 14 | Gestionar la revisión de la seguridad por diseño para los sistemas computarizados y software de no producto, incluyendo la arquitectura del sistema personalizado cuando aplique. | |
| 15 | Datos del Proveedor:<br><br>Fabricante/Desarrollador, cuando aplique | |
| 16 | ¿Tiene puertos USB activos? ¿Cuántos? | |

| | | |
|---|---|---|
| 17 | ¿Se utilizan los puertos durante la operación rutinaria del equipo o durante su mantenimiento? | **Actividad/operación/variable**<br><br>Seguridad por diseño<br><br>**Objetivo:**<br><br>Gestionar documento técnico que especifique el diseño para los sistemas computarizados y software de no producto, incluyendo la arquitectura del sistema personalizado cuando aplique. |
| 18 | ¿Se pueden bloquear los puertos disponibles para dispositivos de almacenamiento masivo y eliminarlos del uso? | |
| 19 | ¿El Proveedor se encuentra calificado con criterios de ciberseguridad (data integrity, vulnerabilidad, parches de seguridad, requisitos de recuperación, gestión de interfaces, entre otros)? | |
| 20 | ¿Se accede remotamente? ¿El activo tiene una conexión remota como una conexión de escritorio remoto? | |
| 21 | **Parches y actualizaciones de software**<br><br>¿El activo tiene un método/plan controlado para la realización de parches y actualizaciones? | |
| 22 | **Protección de Malware**<br><br>¿El activo cuenta con herramientas de protección contra malware? | |
| 23 | **Interfaces seguras**<br><br>¿El activo tiene interfaces con otros sistemas/dispositivos? | |
| 24 | **Seguridad Física**<br><br>¿El activo está ubicado físicamente en un área con acceso controlado? (por ejemplo, una ubicación que requiere controles de acceso únicos)<br><br>**Nota:** La tarjeta de acceso a la instalación no es suficiente como acceso de control. | |
| 25 | **Control de Accesos**<br><br>¿Cuenta con control de accesos? | |
| 26 | ¿Usuarios son gestionados por un administrador de accesos? | |
| 27 | ¿El activo requiere autenticación de usuario individual para acceder? | |
| 28 | ¿Se pueden deshabilitar/inhabilitar cuentas? | |
| 29 | **Fortalecimiento del Sistema**<br><br>¿Cuenta la organización con herramientas para el fortalecimiento del sistema bajo un enfoque en ciberseguridad (Eliminar archivos y contraseñas predeterminadas, proteger archivos con información crítica | |

| | | |
|---|---|---|
| | para el negocio, violentar algoritmos confidenciales, eliminar aplicaciones y servicios innecesarios)? | |
| 30 | ¿Puede el activo eliminar el acceso de los usuarios que no lo utilizaron durante 90 días? | |
| 31 | ¿Existe algún documento estandarizado activo de gestión de accesos? | |
| 32 | ¿Se puede crear más de 01 usuario? ¿Permite realizar cuentas individualizadas? | |
| 33 | ¿Existen usuarios compartidos? | |
| 34 | ¿Existen roles diferenciados por nivel de acceso? ¿Cuáles? | |
| 35 | ¿Permite la creación de grupos o roles? | |
| 36 | ¿El software permite asignar/definir privilegios específicos? | |
| 37 | ¿Se puede establecer /definir una contraseña? | |
| 38 | ¿Las contraseñas se encuentran encriptadas? | |
| 39 | ¿Se puede modificar complejidad de la contraseña? | |
| 40 | ¿Existe bloqueo por inactividad / Logout? | |
| **D** | **CODIFICACIÓN Y CONSTRUCCIÓN** | |
| - | **Desarrollo de código seguro** | |
| 41 | ¿La organización desarrolla sistemas personalizados de software de no producto? ***Nota:*** *Aplica para sistemas computarizados y software de no producto para desarrollos in house.* | **Actividad/operación/variable**<br>Código seguro |
| 42 | Gestionar el diseño para los sistemas computarizados y software de no producto, considerando estándares de codificación de seguridad cibernética, comprobaciones de seguridad, exploraciones de vulnerabilidades de los componentes y herramientas de análisis de códigos estáticos. | **Objetivo:**<br>Gestionar un documento de desarrollo de código seguro. |
| - | **Verificación de controles de ciberseguridad** | |
| 43 | ¿Está codificado, construido, instalado y verificado en todas las pruebas para su uso previsto (de acuerdo con los requerimientos de usuario), incluir pruebas de penetración?<br>***Nota:*** *Las pruebas deben ser ejecutadas por probadores capacitados.* | **Actividad/operación/variable**<br>Controles de ciberseguridad<br>**Objetivo:** |

| | | |
|---|---|---|
| | | Gestionar la verificación de los controles de ciberseguridad |
| **E** | **IMPLEMENTACIÓN Y PRUEBAS** | |
| - | **Implementación y configuración** | |
| 44 | ¿Se tiene establecido un plan para ejecutar pruebas y controles de seguridad cibernética? | **Actividad/operación/variable**<br>Implementación y configuración<br>**Objetivo:**<br>Gestionar un plan para la implementación y configuración |
| **FASE OPERACIÓN** | | |
| **F** | **OPERACIÓN Y MANTENIMIENTO** | |
| - | **Operación** | |
| 45 | ¿Permite modificar zona horaria, fecha y hora sistema operativo y/o software? | **Actividad/operación/variable**<br>Operación y Mantenimiento<br>**Objetivo:**<br>Gestionar un plan de manejo, uso y operación y de mantenimiento de seguridad cibernética. |
| 46 | ¿Cuenta con un documento estandarizado para el manejo, uso y operación del equipo que relacione al software? | |
| 47 | ¿Cuenta con UPS? | |
| 48 | ¿Existe algún documento estandarizado para la gestión de recetas? Indicar código | |
| 49 | ¿El Sistema de alarmas monitorea y registra en el software? Indicar alarmas | |
| - | **Mantenimiento** | |
| 50 | Establecer un plan para identificar, monitorear, comunicar y elevar las señales de seguridad cibernética, incluidos los roles y responsabilidades definidos para cada uno. | |
| 51 | ¿Existe algún documento estandarizado de copias de seguridad y restauración de datos? | |
| **FASE RETIRO** | | |
| **G** | **DECOMISIONAMIENTO** | |
| - | **Baja de activos** | |

| | | |
|---|---|---|
| 52 | Establecer un plan de decomisionamiento con las actividades para el retiro: documentación, conversión y migración de datos. | **Actividad/operación/variable**<br><br>Decomisionamiento<br><br>**Objetivo:**<br><br>Gestionar un plan de decomisionamiento con las actividades para el retiro. |

## 4.2 Validación de la propuesta: Resultados de validez CVC

A partir de los resultados que se han recopilado de la evaluación del instrumento de investigación mediante el juicio de expertos (5), cada ítem (52) tiene un valor en la escala de Likert del 1 al 5 basado en indicadores (4). A continuación, en la siguiente figura se muestra la distribución de los resultados:

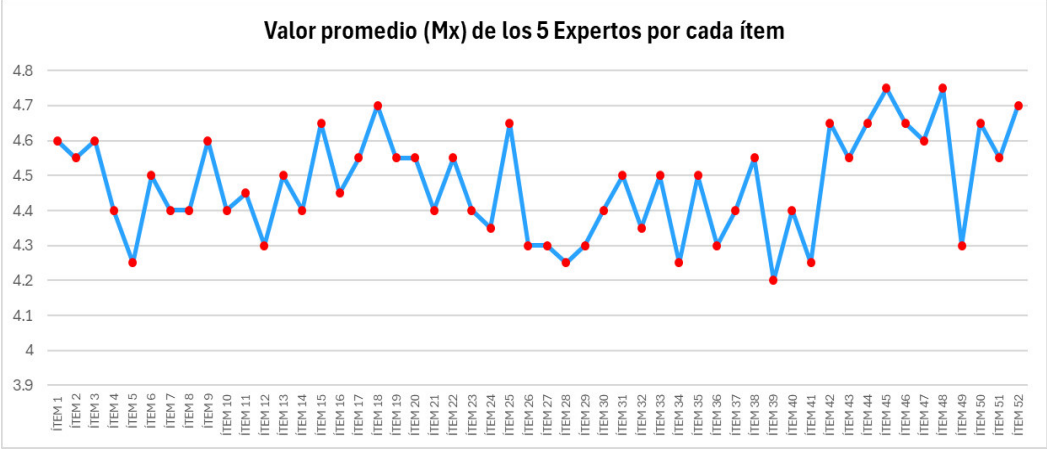



Figura 5: Valor promedio (Mx) de los 5 expertos y su relación con cada ítem.

Fórmula CVC: CVCi = Mx / Vmáx

A partir de estos valores se ponderan los valores para el cálculo del CVC

Número de expertos (j): 5

CVCi: Valor máximo entre el número de expertos

Mx (Media de ítem por cada juez): Se encuentra detallado en la figura 5 anterior. Se hizo el cálculo tomando en consideración el promedio máximo de los 5 expertos por cada ítem (52) y con alcance a los 4 indicadores.

Pei (Probabilidad de error por ítem): (1/j)^j

Tabla 4. Resultados de la evaluación del instrumento por criterio de expertos

| | CONTENIDO | | EXPERTOS | | | | |
|---|---|---|---|---|---|---|---|
| | **COD.** | **INDICADORES** | **1** | **2** | **3** | **4** | **5** |
| ÍTEM 1 | A.1 | COHERENCIA | 4 | 5 | 5 | 5 | 4 |
| | | CLARIDAD | 5 | 5 | 5 | 5 | 5 |
| | | ESCALA | 5 | 4 | 5 | 4 | 5 |
| | | RELEVANCIA | 3 | 4 | 5 | 5 | 4 |
| ÍTEM 2 | A.2 | COHERENCIA | 5 | 4 | 4 | 5 | 5 |
| | | CLARIDAD | 4 | 5 | 4 | 4 | 5 |
| | | ESCALA | 5 | 5 | 4 | 4 | 5 |
| | | RELEVANCIA | 5 | 5 | 5 | 4 | 4 |
| ÍTEM 3 | A.3 | COHERENCIA | 5 | 5 | 5 | 5 | 5 |
| | | CLARIDAD | 5 | 5 | 4 | 5 | 5 |
| | | ESCALA | 4 | 5 | 5 | 4 | 4 |
| | | RELEVANCIA | 3 | 4 | 5 | 5 | 4 |
| ÍTEM 4 | A.4 | COHERENCIA | 3 | 3 | 5 | 5 | 5 |
| | | CLARIDAD | 3 | 5 | 4 | 4 | 5 |
| | | ESCALA | 5 | 4 | 4 | 5 | 4 |
| | | RELEVANCIA | 5 | 5 | 5 | 5 | 4 |
| ÍTEM 5 | A.5 | COHERENCIA | 4 | 3 | 5 | 5 | 5 |
| | | CLARIDAD | 3 | 4 | 4 | 4 | 4 |
| | | ESCALA | 4 | 4 | 5 | 4 | 5 |
| | | RELEVANCIA | 5 | 4 | 5 | 3 | 5 |
| ÍTEM 6 | A.6 | COHERENCIA | 5 | 4 | 5 | 4 | 5 |
| | | CLARIDAD | 5 | 5 | 4 | 4 | 4 |
| | | ESCALA | 5 | 5 | 4 | 4 | 5 |
| | | RELEVANCIA | 5 | 4 | 4 | 4 | 5 |
| ÍTEM 7 | A.7 | COHERENCIA | 4 | 5 | 3 | 4 | 5 |
| | | CLARIDAD | 4 | 3 | 4 | 5 | 5 |
| | | ESCALA | 4 | 5 | 4 | 5 | 5 |
| | | RELEVANCIA | 5 | 4 | 5 | 4 | 5 |
| ÍTEM 8 | A.8 | COHERENCIA | 5 | 4 | 4 | 5 | 4 |
| | | CLARIDAD | 5 | 5 | 3 | 5 | 4 |
| | | ESCALA | 3 | 4 | 4 | 5 | 5 |
| | | RELEVANCIA | 5 | 4 | 5 | 4 | 5 |
| ÍTEM 9 | B.1 | COHERENCIA | 4 | 5 | 4 | 5 | 5 |
| | | CLARIDAD | 3 | 5 | 5 | 5 | 5 |
| | | ESCALA | 4 | 5 | 5 | 4 | 5 |
| | | RELEVANCIA | 5 | 5 | 4 | 4 | 5 |
| ÍTEM 10 | B.2 | COHERENCIA | 3 | 5 | 4 | 5 | 4 |
| | | CLARIDAD | 4 | 4 | 4 | 4 | 5 |
| | | ESCALA | 5 | 5 | 5 | 5 | 5 |
| | | RELEVANCIA | 4 | 4 | 4 | 4 | 5 |
| | B.3 | COHERENCIA | 4 | 4 | 4 | 5 | 4 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ÍTEM 11 | | CLARIDAD | 5 | 3 | 5 | 4 | 5 |
| | | ESCALA | 4 | 4 | 5 | 4 | 5 |
| | | RELEVANCIA | 5 | 4 | 5 | 5 | 5 |
| ÍTEM 12 | B.4 | COHERENCIA | 5 | 4 | 5 | 4 | 4 |
| | | CLARIDAD | 4 | 4 | 5 | 4 | 4 |
| | | ESCALA | 4 | 4 | 4 | 5 | 4 |
| | | RELEVANCIA | 5 | 4 | 4 | 5 | 4 |
| ÍTEM 13 | B.5 | COHERENCIA | 5 | 3 | 5 | 5 | 4 |
| | | CLARIDAD | 3 | 5 | 4 | 4 | 5 |
| | | ESCALA | 5 | 5 | 5 | 5 | 4 |
| | | RELEVANCIA | 3 | 5 | 5 | 5 | 5 |
| ÍTEM 14 | C.1 | COHERENCIA | 3 | 5 | 5 | 4 | 5 |
| | | CLARIDAD | 4 | 4 | 4 | 5 | 4 |
| | | ESCALA | 4 | 4 | 5 | 5 | 5 |
| | | RELEVANCIA | 5 | 4 | 5 | 4 | 4 |
| ÍTEM 15 | C.2 | COHERENCIA | 4 | 4 | 4 | 5 | 5 |
| | | CLARIDAD | 5 | 5 | 5 | 5 | 4 |
| | | ESCALA | 4 | 4 | 5 | 5 | 5 |
| | | RELEVANCIA | 4 | 5 | 5 | 5 | 5 |
| ÍTEM 16 | C.3 | COHERENCIA | 4 | 5 | 4 | 5 | 5 |
| | | CLARIDAD | 5 | 3 | 5 | 5 | 5 |
| | | ESCALA | 5 | 4 | 5 | 4 | 4 |
| | | RELEVANCIA | 3 | 4 | 5 | 5 | 4 |
| ÍTEM 17 | C.4 | COHERENCIA | 4 | 5 | 3 | 5 | 4 |
| | | CLARIDAD | 4 | 5 | 5 | 4 | 5 |
| | | ESCALA | 4 | 5 | 5 | 4 | 5 |
| | | RELEVANCIA | 5 | 5 | 5 | 5 | 4 |
| ÍTEM 18 | C.5 | COHERENCIA | 5 | 5 | 5 | 5 | 5 |
| | | CLARIDAD | 4 | 5 | 5 | 5 | 5 |
| | | ESCALA | 4 | 5 | 5 | 5 | 4 |
| | | RELEVANCIA | 5 | 3 | 5 | 5 | 4 |
| ÍTEM 19 | C.6 | COHERENCIA | 4 | 5 | 5 | 5 | 5 |
| | | CLARIDAD | 3 | 5 | 5 | 5 | 4 |
| | | ESCALA | 4 | 4 | 5 | 5 | 5 |
| | | RELEVANCIA | 4 | 4 | 5 | 5 | 4 |
| ÍTEM 20 | C.7 | COHERENCIA | 4 | 5 | 5 | 5 | 4 |
| | | CLARIDAD | 5 | 5 | 5 | 4 | 4 |
| | | ESCALA | 5 | 4 | 4 | 5 | 5 |
| | | RELEVANCIA | 4 | 5 | 5 | 5 | 3 |
| ÍTEM 21 | C.8 | COHERENCIA | 3 | 4 | 5 | 5 | 4 |
| | | CLARIDAD | 4 | 5 | 5 | 5 | 5 |
| | | ESCALA | 3 | 4 | 5 | 5 | 4 |
| | | RELEVANCIA | 3 | 5 | 4 | 5 | 5 |
| | C.9 | COHERENCIA | 3 | 4 | 5 | 5 | 5 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ÍTEM 22 | | CLARIDAD | 5 | 4 | 4 | 5 | 5 |
| | | ESCALA | 5 | 5 | 5 | 5 | 5 |
| | | RELEVANCIA | 3 | 3 | 5 | 5 | 5 |
| ÍTEM 23 | C.10 | COHERENCIA | 5 | 5 | 5 | 4 | 4 |
| | | CLARIDAD | 5 | 4 | 5 | 5 | 4 |
| | | ESCALA | 3 | 4 | 5 | 4 | 5 |
| | | RELEVANCIA | 4 | 4 | 5 | 3 | 5 |
| ÍTEM 24 | C.11 | COHERENCIA | 4 | 3 | 5 | 5 | 4 |
| | | CLARIDAD | 3 | 5 | 4 | 5 | 4 |
| | | ESCALA | 5 | 4 | 5 | 5 | 5 |
| | | RELEVANCIA | 5 | 3 | 4 | 5 | 4 |
| ÍTEM 25 | C.12 | COHERENCIA | 4 | 4 | 5 | 5 | 4 |
| | | CLARIDAD | 5 | 5 | 4 | 5 | 4 |
| | | ESCALA | 5 | 5 | 5 | 5 | 5 |
| | | RELEVANCIA | 4 | 5 | 5 | 5 | 4 |
| ÍTEM 26 | C.13 | COHERENCIA | 4 | 5 | 5 | 5 | 4 |
| | | CLARIDAD | 5 | 4 | 4 | 5 | 5 |
| | | ESCALA | 3 | 4 | 4 | 4 | 4 |
| | | RELEVANCIA | 3 | 4 | 5 | 4 | 5 |
| ÍTEM 27 | C.14 | COHERENCIA | 5 | 4 | 5 | 5 | 3 |
| | | CLARIDAD | 5 | 4 | 4 | 4 | 5 |
| | | ESCALA | 4 | 5 | 5 | 5 | 5 |
| | | RELEVANCIA | 3 | 4 | 4 | 5 | 5 |
| ÍTEM 28 | C.15 | COHERENCIA | 4 | 5 | 4 | 5 | 3 |
| | | CLARIDAD | 4 | 5 | 5 | 5 | 5 |
| | | ESCALA | 4 | 5 | 5 | 4 | 5 |
| | | RELEVANCIA | 4 | 4 | 4 | 5 | 5 |
| ÍTEM 29 | C.16 | COHERENCIA | 3 | 4 | 4 | 4 | 4 |
| | | CLARIDAD | 5 | 5 | 5 | 5 | 4 |
| | | ESCALA | 4 | 4 | 4 | 5 | 5 |
| | | RELEVANCIA | 4 | 5 | 5 | 5 | 5 |
| ÍTEM 30 | C.17 | COHERENCIA | 5 | 5 | 5 | 4 | 5 |
| | | CLARIDAD | 5 | 5 | 5 | 4 | 4 |
| | | ESCALA | 3 | 5 | 4 | 5 | 4 |
| | | RELEVANCIA | 5 | 5 | 5 | 5 | 5 |
| ÍTEM 31 | C.18 | COHERENCIA | 5 | 5 | 4 | 5 | 5 |
| | | CLARIDAD | 5 | 4 | 5 | 4 | 5 |
| | | ESCALA | 4 | 4 | 5 | 5 | 5 |
| | | RELEVANCIA | 5 | 5 | 5 | 4 | 3 |
| ÍTEM 32 | C.19 | COHERENCIA | 5 | 5 | 5 | 4 | 5 |
| | | CLARIDAD | 4 | 4 | 4 | 4 | 4 |
| | | ESCALA | 3 | 5 | 5 | 5 | 5 |
| | | RELEVANCIA | 3 | 4 | 4 | 4 | 5 |
| | C.20 | COHERENCIA | 5 | 4 | 5 | 4 | 4 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ÍTEM 33 | | CLARIDAD | 4 | 4 | 4 | 5 | 4 |
| | | ESCALA | 5 | 5 | 5 | 4 | 5 |
| | | RELEVANCIA | 4 | 5 | 5 | 4 | 5 |
| ÍTEM 34 | C.21 | COHERENCIA | 4 | 4 | 5 | 3 | 4 |
| | | CLARIDAD | 4 | 4 | 4 | 4 | 3 |
| | | ESCALA | 5 | 4 | 5 | 4 | 5 |
| | | RELEVANCIA | 4 | 5 | 5 | 4 | 5 |
| ÍTEM 35 | C.22 | COHERENCIA | 4 | 3 | 5 | 4 | 5 |
| | | CLARIDAD | 3 | 5 | 5 | 4 | 4 |
| | | ESCALA | 5 | 5 | 5 | 5 | 5 |
| | | RELEVANCIA | 3 | 5 | 5 | 5 | 5 |
| ÍTEM 36 | C.23 | COHERENCIA | 3 | 4 | 5 | 5 | 5 |
| | | CLARIDAD | 4 | 4 | 5 | 4 | 4 |
| | | ESCALA | 5 | 4 | 4 | 5 | 4 |
| | | RELEVANCIA | 4 | 4 | 4 | 4 | 5 |
| ÍTEM 37 | C.24 | COHERENCIA | 4 | 4 | 5 | 5 | 5 |
| | | CLARIDAD | 4 | 5 | 5 | 4 | 5 |
| | | ESCALA | 4 | 4 | 3 | 5 | 5 |
| | | RELEVANCIA | 3 | 4 | 5 | 5 | 4 |
| ÍTEM 38 | C.25 | COHERENCIA | 4 | 4 | 3 | 5 | 4 |
| | | CLARIDAD | 3 | 5 | 5 | 5 | 5 |
| | | ESCALA | 5 | 5 | 4 | 5 | 5 |
| | | RELEVANCIA | 5 | 5 | 4 | 5 | 5 |
| ÍTEM 39 | C.26 | COHERENCIA | 5 | 4 | 4 | 4 | 4 |
| | | CLARIDAD | 5 | 3 | 4 | 4 | 5 |
| | | ESCALA | 4 | 3 | 4 | 3 | 5 |
| | | RELEVANCIA | 5 | 4 | 5 | 4 | 5 |
| ÍTEM 40 | C.27 | COHERENCIA | 5 | 5 | 4 | 4 | 5 |
| | | CLARIDAD | 4 | 5 | 4 | 4 | 4 |
| | | ESCALA | 3 | 5 | 4 | 5 | 4 |
| | | RELEVANCIA | 5 | 5 | 5 | 5 | 3 |
| ÍTEM 41 | D.1 | COHERENCIA | 5 | 4 | 3 | 4 | 4 |
| | | CLARIDAD | 5 | 4 | 4 | 4 | 5 |
| | | ESCALA | 5 | 4 | 4 | 4 | 5 |
| | | RELEVANCIA | 3 | 4 | 5 | 4 | 5 |
| ÍTEM 42 | D.2 | COHERENCIA | 4 | 5 | 4 | 5 | 5 |
| | | CLARIDAD | 4 | 4 | 5 | 5 | 5 |
| | | ESCALA | 5 | 5 | 5 | 5 | 5 |
| | | RELEVANCIA | 5 | 5 | 5 | 5 | 5 |
| ÍTEM 43 | D.3 | COHERENCIA | 4 | 5 | 5 | 5 | 4 |
| | | CLARIDAD | 4 | 4 | 5 | 4 | 4 |
| | | ESCALA | 5 | 5 | 5 | 5 | 5 |
| | | RELEVANCIA | 4 | 4 | 5 | 5 | 5 |
| | E.1 | COHERENCIA | 4 | 5 | 4 | 3 | 5 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ÍTEM 44 | | CLARIDAD | 5 | 5 | 5 | 5 | 5 |
| | | ESCALA | 4 | 5 | 5 | 5 | 5 |
| | | RELEVANCIA | 5 | 4 | 5 | 5 | 5 |
| ÍTEM 45 | F.1 | COHERENCIA | 5 | 5 | 5 | 5 | 5 |
| | | CLARIDAD | 5 | 4 | 5 | 5 | 4 |
| | | ESCALA | 4 | 5 | 5 | 4 | 5 |
| | | RELEVANCIA | 5 | 5 | 5 | 5 | 4 |
| ÍTEM 46 | F.2 | COHERENCIA | 5 | 5 | 5 | 4 | 3 |
| | | CLARIDAD | 4 | 5 | 5 | 5 | 5 |
| | | ESCALA | 4 | 4 | 5 | 5 | 5 |
| | | RELEVANCIA | 5 | 4 | 5 | 5 | 5 |
| ÍTEM 47 | F.3 | COHERENCIA | 4 | 5 | 5 | 5 | 4 |
| | | CLARIDAD | 5 | 5 | 5 | 5 | 5 |
| | | ESCALA | 5 | 3 | 4 | 5 | 4 |
| | | RELEVANCIA | 4 | 5 | 5 | 4 | 5 |
| ÍTEM 48 | F.4 | COHERENCIA | 5 | 4 | 4 | 5 | 5 |
| | | CLARIDAD | 5 | 5 | 4 | 5 | 5 |
| | | ESCALA | 4 | 5 | 5 | 5 | 5 |
| | | RELEVANCIA | 5 | 5 | 4 | 5 | 5 |
| ÍTEM 49 | F.5 | COHERENCIA | 4 | 4 | 5 | 5 | 3 |
| | | CLARIDAD | 4 | 4 | 4 | 4 | 4 |
| | | ESCALA | 4 | 4 | 5 | 5 | 5 |
| | | RELEVANCIA | 4 | 4 | 5 | 4 | 5 |
| ÍTEM 50 | F.6 | COHERENCIA | 5 | 5 | 4 | 5 | 5 |
| | | CLARIDAD | 4 | 5 | 5 | 5 | 4 |
| | | ESCALA | 5 | 5 | 5 | 5 | 5 |
| | | RELEVANCIA | 4 | 4 | 5 | 4 | 5 |
| ÍTEM 51 | F.7 | COHERENCIA | 5 | 5 | 4 | 5 | 5 |
| | | CLARIDAD | 5 | 5 | 5 | 5 | 5 |
| | | ESCALA | 5 | 5 | 5 | 5 | 5 |
| | | RELEVANCIA | 5 | 5 | 5 | 5 | 4 |
| ÍTEM 52 | G.1 | COHERENCIA | 4 | 5 | 5 | 5 | 4 |
| | | CLARIDAD | 5 | 5 | 5 | 5 | 5 |
| | | ESCALA | 5 | 5 | 5 | 5 | 5 |
| | | RELEVANCIA | 5 | 5 | 5 | 5 | 5 |

Tabla 5. Resultado del CVC por ítem

| | **CONTENIDO** | | **Mx** | **VALOR MÁXIMO (Vmáx.)** | **CVCi** | **Pei** | **CVC** |
|---|---|---|---|---|---|---|---|
| | **COD.** | **INDICADORES** | | | | | |
| ÍTEM 1 | A.1 | COHERENCIA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | CLARIDAD | 5 | 5 | 1 | 0.00032 | 1.00 |
| | | ESCALA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | RELEVANCIA | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| ÍTEM 2 | A.2 | COHERENCIA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | CLARIDAD | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| | | ESCALA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | RELEVANCIA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| ÍTEM 3 | A.3 | COHERENCIA | 5 | 5 | 1 | 0.00032 | 1.00 |
| | | CLARIDAD | 4.8 | 5 | 0.96 | 0.00032 | 0.96 |
| | | ESCALA | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| | | RELEVANCIA | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| ÍTEM 4 | A.4 | COHERENCIA | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| | | CLARIDAD | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| | | ESCALA | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| | | RELEVANCIA | 4.8 | 5 | 0.96 | 0.00032 | 0.96 |
| ÍTEM 5 | A.5 | COHERENCIA | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| | | CLARIDAD | 3.8 | 4 | 0.95 | 0.00032 | 0.95 |
| | | ESCALA | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| | | RELEVANCIA | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| ÍTEM 6 | A.6 | COHERENCIA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | CLARIDAD | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| | | ESCALA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | RELEVANCIA | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| ÍTEM 7 | A.7 | COHERENCIA | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| | | CLARIDAD | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| | | ESCALA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | RELEVANCIA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| ÍTEM 8 | A.8 | COHERENCIA | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| | | CLARIDAD | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| | | ESCALA | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| | | RELEVANCIA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| ÍTEM 9 | B.1 | COHERENCIA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | CLARIDAD | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | ESCALA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | RELEVANCIA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| ÍTEM 10 | B.2 | COHERENCIA | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| | | CLARIDAD | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| | | ESCALA | 5 | 5 | 1 | 0.00032 | 1.00 |
| | | RELEVANCIA | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| ÍTEM 11 | B.3 | COHERENCIA | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| | | CLARIDAD | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| | | ESCALA | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| | | RELEVANCIA | 4.8 | 5 | 0.96 | 0.00032 | 0.96 |
| ÍTEM 12 | B.4 | COHERENCIA | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| | | CLARIDAD | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| | | ESCALA | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | RELEVANCIA | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| ÍTEM 13 | B.5 | COHERENCIA | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| | | CLARIDAD | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| | | ESCALA | 4.8 | 5 | 0.96 | 0.00032 | 0.96 |
| | | RELEVANCIA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| ÍTEM 14 | C.1 | COHERENCIA | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| | | CLARIDAD | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| | | ESCALA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | RELEVANCIA | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| ÍTEM 15 | C.2 | COHERENCIA | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| | | CLARIDAD | 4.8 | 5 | 0.96 | 0.00032 | 0.96 |
| | | ESCALA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | RELEVANCIA | 4.8 | 5 | 0.96 | 0.00032 | 0.96 |
| ÍTEM 16 | C.3 | COHERENCIA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | CLARIDAD | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | ESCALA | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| | | RELEVANCIA | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| ÍTEM 17 | C.4 | COHERENCIA | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| | | CLARIDAD | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | ESCALA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | RELEVANCIA | 4.8 | 5 | 0.96 | 0.00032 | 0.96 |
| ÍTEM 18 | C.5 | COHERENCIA | 5 | 5 | 1 | 0.00032 | 1.00 |
| | | CLARIDAD | 4.8 | 5 | 0.96 | 0.00032 | 0.96 |
| | | ESCALA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | RELEVANCIA | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| ÍTEM 19 | C.6 | COHERENCIA | 4.8 | 5 | 0.96 | 0.00032 | 0.96 |
| | | CLARIDAD | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| | | ESCALA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | RELEVANCIA | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| ÍTEM 20 | C.7 | COHERENCIA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | CLARIDAD | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | ESCALA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | RELEVANCIA | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| ÍTEM 21 | C.8 | COHERENCIA | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| | | CLARIDAD | 4.8 | 5 | 0.96 | 0.00032 | 0.96 |
| | | ESCALA | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| | | RELEVANCIA | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| ÍTEM 22 | C.9 | COHERENCIA | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| | | CLARIDAD | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | ESCALA | 5 | 5 | 1 | 0.00032 | 1.00 |
| | | RELEVANCIA | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| ÍTEM 23 | C.10 | COHERENCIA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | CLARIDAD | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | ESCALA | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | RELEVANCIA | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| ÍTEM 24 | C.11 | COHERENCIA | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| | | CLARIDAD | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| | | ESCALA | 4.8 | 5 | 0.96 | 0.00032 | 0.96 |
| | | RELEVANCIA | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| ÍTEM 25 | C.12 | COHERENCIA | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| | | CLARIDAD | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | ESCALA | 5 | 5 | 1 | 0.00032 | 1.00 |
| | | RELEVANCIA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| ÍTEM 26 | C.13 | COHERENCIA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | CLARIDAD | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | ESCALA | 3.8 | 4 | 0.95 | 0.00032 | 0.95 |
| | | RELEVANCIA | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| ÍTEM 27 | C.14 | COHERENCIA | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| | | CLARIDAD | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| | | ESCALA | 4.8 | 5 | 0.96 | 0.00032 | 0.96 |
| | | RELEVANCIA | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| ÍTEM 28 | C.15 | COHERENCIA | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| | | CLARIDAD | 4.8 | 5 | 0.96 | 0.00032 | 0.96 |
| | | ESCALA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | RELEVANCIA | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| ÍTEM 29 | C.16 | COHERENCIA | 3.8 | 4 | 0.95 | 0.00032 | 0.95 |
| | | CLARIDAD | 4.8 | 5 | 0.96 | 0.00032 | 0.96 |
| | | ESCALA | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| | | RELEVANCIA | 4.8 | 5 | 0.96 | 0.00032 | 0.96 |
| ÍTEM 30 | C.17 | COHERENCIA | 4.8 | 5 | 0.96 | 0.00032 | 0.96 |
| | | CLARIDAD | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | ESCALA | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| | | RELEVANCIA | 5 | 5 | 1 | 0.00032 | 1.00 |
| ÍTEM 31 | C.18 | COHERENCIA | 4.8 | 5 | 0.96 | 0.00032 | 0.96 |
| | | CLARIDAD | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | ESCALA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | RELEVANCIA | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| ÍTEM 32 | C.19 | COHERENCIA | 4.8 | 5 | 0.96 | 0.00032 | 0.96 |
| | | CLARIDAD | 4 | 4 | 1 | 0.00032 | 1.00 |
| | | ESCALA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | RELEVANCIA | 4 | 5 | 0.8 | 0.00032 | 0.80 |
| ÍTEM 33 | C.20 | COHERENCIA | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| | | CLARIDAD | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| | | ESCALA | 4.8 | 5 | 0.96 | 0.00032 | 0.96 |
| | | RELEVANCIA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| ÍTEM 34 | C.21 | COHERENCIA | 4 | 5 | 0.8 | 0.00032 | 0.80 |
| | | CLARIDAD | 3.8 | 4 | 0.95 | 0.00032 | 0.95 |
| | | ESCALA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | RELEVANCIA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| ÍTEM 35 | C.22 | COHERENCIA | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| | | CLARIDAD | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| | | ESCALA | 5 | 5 | 1 | 0.00032 | 1.00 |
| | | RELEVANCIA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| ÍTEM 36 | C.23 | COHERENCIA | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| | | CLARIDAD | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| | | ESCALA | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| | | RELEVANCIA | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| ÍTEM 37 | C.24 | COHERENCIA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | CLARIDAD | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | ESCALA | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| | | RELEVANCIA | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| ÍTEM 38 | C.25 | COHERENCIA | 4 | 5 | 0.8 | 0.00032 | 0.80 |
| | | CLARIDAD | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | ESCALA | 4.8 | 5 | 0.96 | 0.00032 | 0.96 |
| | | RELEVANCIA | 4.8 | 5 | 0.96 | 0.00032 | 0.96 |
| ÍTEM 39 | C.26 | COHERENCIA | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| | | CLARIDAD | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| | | ESCALA | 3.8 | 5 | 0.76 | 0.00032 | 0.76 |
| | | RELEVANCIA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| ÍTEM 40 | C.27 | COHERENCIA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | CLARIDAD | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| | | ESCALA | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| | | RELEVANCIA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| ÍTEM 41 | D.1 | COHERENCIA | 4 | 5 | 0.8 | 0.00032 | 0.80 |
| | | CLARIDAD | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| | | ESCALA | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| | | RELEVANCIA | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| ÍTEM 42 | D.2 | COHERENCIA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | CLARIDAD | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | ESCALA | 5 | 5 | 1 | 0.00032 | 1.00 |
| | | RELEVANCIA | 5 | 5 | 1 | 0.00032 | 1.00 |
| ÍTEM 43 | D.3 | COHERENCIA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | CLARIDAD | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| | | ESCALA | 5 | 5 | 1 | 0.00032 | 1.00 |
| | | RELEVANCIA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| ÍTEM 44 | E.1 | COHERENCIA | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| | | CLARIDAD | 5 | 5 | 1 | 0.00032 | 1.00 |
| | | ESCALA | 4.8 | 5 | 0.96 | 0.00032 | 0.96 |
| | | RELEVANCIA | 4.8 | 5 | 0.96 | 0.00032 | 0.96 |
| ÍTEM 45 | F.1 | COHERENCIA | 5 | 5 | 1 | 0.00032 | 1.00 |
| | | CLARIDAD | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | ESCALA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | RELEVANCIA | 4.8 | 5 | 0.96 | 0.00032 | 0.96 |
| ÍTEM 46 | F.2 | COHERENCIA | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| | | CLARIDAD | 4.8 | 5 | 0.96 | 0.00032 | 0.96 |
| | | ESCALA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | RELEVANCIA | 4.8 | 5 | 0.96 | 0.00032 | 0.96 |
| ÍTEM 47 | F.3 | COHERENCIA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | CLARIDAD | 5 | 5 | 1 | 0.00032 | 1.00 |
| | | ESCALA | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| | | RELEVANCIA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| ÍTEM 48 | F.4 | COHERENCIA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | CLARIDAD | 4.8 | 5 | 0.96 | 0.00032 | 0.96 |
| | | ESCALA | 4.8 | 5 | 0.96 | 0.00032 | 0.96 |
| | | RELEVANCIA | 4.8 | 5 | 0.96 | 0.00032 | 0.96 |
| ÍTEM 49 | F.5 | COHERENCIA | 4.2 | 5 | 0.84 | 0.00032 | 0.84 |
| | | CLARIDAD | 4 | 4 | 1 | 0.00032 | 1.00 |
| | | ESCALA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | RELEVANCIA | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| ÍTEM 50 | F.6 | COHERENCIA | 4.8 | 5 | 0.96 | 0.00032 | 0.96 |
| | | CLARIDAD | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | ESCALA | 5 | 5 | 1 | 0.00032 | 1.00 |
| | | RELEVANCIA | 4.4 | 5 | 0.88 | 0.00032 | 0.88 |
| ÍTEM 51 | F.7 | COHERENCIA | 4.8 | 5 | 0.96 | 0.00032 | 0.96 |
| | | CLARIDAD | 5 | 5 | 1 | 0.00032 | 1.00 |
| | | ESCALA | 5 | 5 | 1 | 0.00032 | 1.00 |
| | | RELEVANCIA | 4.8 | 5 | 0.96 | 0.00032 | 0.96 |
| ÍTEM 52 | G.1 | COHERENCIA | 4.6 | 5 | 0.92 | 0.00032 | 0.92 |
| | | CLARIDAD | 5 | 5 | 1 | 0.00032 | 1.00 |
| | | ESCALA | 5 | 5 | 1 | 0.00032 | 1.00 |
| | | RELEVANCIA | 5 | 5 | 1 | 0.00032 | 1.00 |
| **PROMEDIO TOTAL** | | | | | | | **0.91** |

Como se puede observar en la tabla, al realizar el cálculo de la diferencia entre el CVCi menos la probabilidad de error (Pei) de cada ítem del valor obtenido para CVC por ítem, finalmente se realiza el promedio, lo que nos como resultado un valor de 0,91 (validez y concordancia excelente).

### 4.3 Resultados de validez Coeficiente Alfa de Cronbach.

Para evaluar la confiabilidad en el presente trabajo académico utilizamos una encuesta

según el ANEXO III, en la que se recogen las valoraciones de los (10) Químicos Farmacéuticos y/o Ingenieros de Sistemas.

Tabla 6. Resultado de la encuesta

| | Ítem 1 | Ítem 2 | Ítem 3 | Ítem 4 | Ítem 5 | Ítem 6 | Ítem 7 | Ítem 8 | Suma |
|---|---|---|---|---|---|---|---|---|---|
| Persona 1 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 4 | 38 |
| Persona 2 | 4 | 5 | 4 | 4 | 4 | 4 | 4 | 2 | 31 |
| Persona 3 | 3 | 3 | 3 | 2 | 2 | 4 | 3 | 2 | 22 |
| Persona 4 | 4 | 4 | 4 | 5 | 5 | 5 | 4 | 4 | 35 |
| Persona 5 | 5 | 2 | 3 | 4 | 4 | 3 | 5 | 3 | 29 |
| Persona 6 | 4 | 4 | 3 | 3 | 2 | 4 | 5 | 3 | 28 |
| Persona 7 | 3 | 4 | 5 | 4 | 4 | 4 | 4 | 4 | 32 |
| Persona 8 | 3 | 5 | 3 | 4 | 2 | 3 | 4 | 2 | 26 |
| Persona 9 | 4 | 4 | 5 | 5 | 4 | 3 | 3 | 3 | 31 |
| Persona 10 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 39 |
| **Varianza** | **0.60** | **0.89** | **0.80** | **0.69** | **1.41** | **0.60** | **0.56** | **0.96** | |
| **Suma. Var.** | **6.51** | | | | | | | | |
| **Varianza suma ítems** | **24.89** | | | | | | | | |

Como se puede observar en la tabla 6 se ha determinado: la suma de cada persona, la varianza de cada ítem, la sumatoria de la varianza y la varianza de la suma de todos los ítems, obteniendo así un alfa de cronbach el cual nos da un valor de 0.84.

$$\alpha = \frac{K}{K-1}\left[1 - \frac{\sum S_i^2}{S_T^2}\right]$$

Tabla 7. Resultado del CVC por ítem Coeficiente Alfa de Cronbach

| **Σ (Símbolo sumatoria)** | **Resultado** |
|---|---|
| α (Coeficiente de confiabilidad de contenido) | **0.84** |
| $\Sigma S_i^2$ K (Número de ítems del instrumento) = | 8 |
| $S_T^2$ (Sumatoria de Varianza de los ítems) = | 6.51 |
| Vt (Varianza total del instrumento) = | 24.89 |

Para la interpretación del resultado del coeficiente alfa de cronbach, se utilizó lo indicado por Gliem Gliem, citado por Torres (14) que mientas el valor sea más cercano a 1 existe más consistencia interna de los ítems. Por otro lado, Carbajal et al, citado por Torres (14) indica que el margen aceptable para los coeficientes de fiabilidad comprende un rango de 0.7 y 0.9 respectivamente. De acuerdo con lo anteriormente explicado el valor obtenido de 0.84 es considerado bueno y aceptable.

## CAPÍTULO V. DISCUSIÓN

De acuerdo con los resultados encontrados en el presente trabajo académico para elaborar una guía para la implementación de ciberseguridad en el ciclo de vida de sistemas computarizados y software de no producto en la industria farmacéutica y con la finalidad de evitar el acceso no autorizado, la modificación, uso indebido o la denegación de uso o el uso no autorizado de información almacenada accedida o transferida a un usuario externo, se determinaron los lineamientos de ciberseguridad aplicable a cada fase (concepto, proyecto, operación y retiro), así como también sus indicadores por cada etapa y esto está de acuerdo con Solfa et al. En el 2022, donde indica que las empresas farmacéuticas deben desarrollar un plan para implementar la ciberseguridad (1).

El ciclo de vida de un sistema computarizado y software de no producto, de acuerdo con Fuenzalida en el 2022 (2), es que la validación puede basarse en la generación de protocolos y reportes, los mimos que fueron tomando en consideración lo indicado en la GAMP5, el cual puede mantener un enfoque prospectivo. Además, indica que se debe tener en cuenta sobre la ejecución de la validación de sistemas computarizados dado que es un proceso importante y con el cual se garantizará que la información está protegida y salvaguardada. La presente guía de ciberseguridad incluye también lo relacionado a la validación de sistemas computarizados de tal manera que se cumplan los estándares de calidad y cumplimiento.

Respecto al informe de opinión de expertos o jueces del instrumento de investigación, los 5 expertos revisaron detenidamente los datos incluidos en este documento, los mismos que devolvieron debidamente firmado, dando fe de la información que se decantó en el mismo – ver ANEXO VI.

La simulación de ciberseguridad de acuerdo con Kannan 2022 (5) tiene un enfoque en la industria farmacéutica centrándose en modelos de infraestructura para identificar posibles amenazas y vulnerabilidades de tal manera que se sigan acciones como la evaluación de riesgos sobre la infraestructura de ataques fortuitos o ataques indirectos. Teniendo como base la guía planteada en el presente trabajo académico, estos controles ya se incluyen dentro de la misma, así que es una buena referencia para poder implementarla.

Para los resultados de validez de coeficiente alfa cronbach, se aplicó una encuesta a 10 personas (tal como se indica en los indicadores de evaluación del instrumento).
Como se puede observar en la tabla 6 se determinó: la suma de cada persona, la varianza de cada ítem, la sumatoria de la varianza y la varianza de la suma de todos los ítems, obteniendo así un alfa de cronbach el cual nos da un valor de 0.84, el cual es considerado bueno y aceptable.

Al tener la industria farmacéutica una gran responsabilidad para garantizar que los datos e información y que esté debidamente protegida según Devliyal 2024 (6) indica en su estudio que existen técnicas de detección de ataques cibernéticos en sistemas físicos, así como los distintos tipos de amenazas y vulnerabilidades. La presente guía tiene lineamientos también para garantizar la protección de la información de los sistemas computarizados y software de no producto.

## CAPÍTULO VI. CONCLUSIONES

1. Se implementó la guía de ciberseguridad en el ciclo de vida de sistemas computarizados y software de no producto en la industria farmacéutica, la cual consta de 52 ítems que pueden ser tomados como referencia para implementar en la industria farmacéutica nacional e internacional.

2. Se han establecido los lineamientos específicos para la implementación de la ciberseguridad **en la Fase de Concepto** respecto a implementar un plan de ciberseguridad y de especificación de requisitos de usuarios (URS) y funcionales (FRS).

3. Se ha llegado a establecer los lineamientos específicos para la implementación de la ciberseguridad **en la Fase de Proyecto** respecto a implementar un documento de diseño, código seguro, control de riesgos y de implementación y configuración.

4. Se ha llegado a establecer los lineamientos específicos para la implementación de la ciberseguridad **en la Fase de Operación** respecto a implementar un plan de operación y mantenimiento.

5. Se ha llegado a establecer los lineamientos específicos para la implementación de la ciberseguridad **en la Fase de Retiro** respecto a implementar un plan de decomisionamiento.

## CAPÍTULO VII. REFERENCIAS BIBLOGRÁFICAS


1. Solfa FD. Impactos de la ciberseguridad y el riesgo de la cadena de suministro en las operaciones digitales: evidencia de la industria farmacéutica. Revista Internacional de Tecnología, Innovación y Gestión (IJTIM). 27 de octubre de 2022; 2(2):18-32.
2. Fuenzalida Leal PA. Implementación de validación de sistema computarizado en software de control de espectrofotómetro UV para cumplimiento con normativa CFR21 en laboratorio de desarrollo analítico para Synthon Chile Ltda.
3. Alexandra P, Camelia C, Elena CC, Bogdan P, Razvan DC. evaluación de riesgos cibernéticos en la industria farmacéutica: vulnerabilidades, amenazas y estrategias de respuesta global. Universidad de estudios Económicos de Bucarest. 1(5) de octubre de 2024.
4. Arenas E, Palomino J, Mansilla JP. Cybersecurity Maturity Model to Prevent Cyberattacks on Web Applications Based on ISO 27032 and NIST. In2023 IEEE XXX International Conference on Electronics, Electrical Engineering and Computing (INTERCON) 2023 Nov 2 (pp. 1-8). IEEE.
5. Kannan U, Swamidurai R. Ataque cibernético indirecto a las empresas farmacéuticas. Revista de Resultados Negativos Farmacéuticos. 1 de enero de 2023: 1766-82.
6. Devliyal S, Goyal HR, Sharma S. Técnicas de detección de ataques cibernéticos en sistemas ciberfísicos para servicios de atención farmacéutica. En 2023, Tercera Conferencia Internacional sobre Computación y Comunicación Cibernéticas Seguras (ICSCCC), 2023, 26 de mayo (pp. 281-286). IEEE.
7. Guía de Buenas Prácticas de Fabricación Automatizada versión 5, A Risk-Based Approach to Compliant GxP Computerized Systems. Validation of Laboratory Computerized Systems, version 2 (2022). GAMP Good Practice Guides, international Society for Pharmaceutical Engineering (ISPE), (Citado 03 de enero del 2023). Disponible en internet: www.ispe.org.
8. ISO/IEC 27000 Information technology – Security techniques – Information security management systems – Overview and vocabulary. Second edition; 2018. Disponible en: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en

9. ISO/IEC 27032:2023 Cybsersecurity – Guidelines for internet security. Second edition; 2023. Disponible en: https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27032:ed-2:v1:en
10. Manual de Buenas prácticas de Manufactura DS 021-2018 Definiciones operativas. 2018. Disponible en: https://www.digemid.minsa.gob.pe/webDigemid/normas-legales/2018/decreto-supremo-n-021-2018-sa/
11. Arispe, C. Yangali, J. Guerrero, M. Lozada, O. Acuña, L. Arellano, C. (2020). La investigación científica. Una aproximación para los estudios de posgrado. (Ecuador). (Citado 16 de mayo del 2023). Disponible en internet: https://repositorio.uide.edu.ec/bitstream/37000/4310/1/LA%20INVESTIGACI%c3%93N%20CIENT%c3%8dFICA.pdf?authuser=2.
12. Lopez, C. Velasquez, V. (2016). Diseño de una guía metodológica para la implementación del sistema integral de gestión y control de la Gobernación de Cundinamarca. (Colombia). SIGNOS / ISSN: 2145-1389 / Vol. 8 / N.º 1 / 2016 / pp. 45-58.
13. Pedrosa, I., Suárez-Álvarez y García-Cueto, E. (2013). Evidencias sobre la Validez de Contenido: Avances Teóricos y Métodos para su Estimación [Content Validity Evidences: Theoretical Advances and Estimation Methods]. (Citado 27 de mayo del 2023). Disponible en internet: http://dx.doi.org/10.5944/ap.10.2.11820
14. Torres, J., (2021). Fiabilidad de escalas: interpretación y limitaciones del Alfa de Cronbach. Disponible en: https://www.researchgate.net/publication/350590351_Fiabilidad_de_las_escalas_interpretacion_y_limitaciones_del_Alfa_de_Cronbach.

# CAPÍTULO VIII. ANEXOS

## ANEXO I

## INFORME DE OPINIÓN DE EXPERTOS O JUECES DEL INSTRUMENTO DE INVESTIGACIÓN

### I. DATOS GENERALES:

1.1 **Nombres y Apellidos del SME[1]:**
1.2 **Grado Académico o tiempo de experiencia en el área** (como experto en Sistemas de Información, Sistemas de Calidad, Sistemas Computarizados, Data Integrity y Ciberseguridad)
1.3 **Profesión:**
1.4 **Institución donde Labora:**
1.5 **Cargo que desempeña:**
1.6 **Nombre del instrumento:** Ciberseguridad en el ciclo de vida de Sistema Computarizado y software de no producto en la industria farmacéutica
1.7 **Autor del instrumento:** Rider Antonio Castillo Salirrosas

Estimado(a), se le invita a participar en el proceso de evaluación de un instrumento.
Para ello se adjunta el instrumento a evaluar y el formato que servirá para que usted pueda hacernos llegar sus apreciaciones.

Agradezco su opinión y feedback que permitirá validar el instrumento y así obtener información válida, el cual es un requerimiento para cualquier investigación.

Se solicita que lea el instrumento y luego identifique el ítem o pregunta y conteste marcando con un aspa en la casilla que usted considere conveniente.

_____

**Firma SME**

[1] SME: Subject Matter Expert

## INFORME DE OPINIÓN DE EXPERTOS O JUECES DEL INSTRUMENTO DE INVESTIGACIÓN

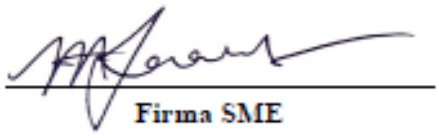
### I. DATOS GENERALES:

1.1 **Apellidos y nombres del SME[1]:** Willian Felinto Suarez
1.2 **Grado Académico o tiempo de experiencia en el área** (como experto en Sistemas de Información, Sistemas de Calidad, Sistemas Computarizados, Data Integrity y Ciberseguridad) MBA, 21 años Project Management, Quality Systems IT, Cybersecurity, Computerized System Validation.
1.3 **Profesión:** Ingeniero de Sistemas
1.4 **Institución donde Labora:** Abbott Laboratorios – Site Brasil
1.5 **Cargo que desempeña:** IT Quality Systems Coordinator – LATAM
1.6 **Nombre del instrumento:** Ciberseguridad en el ciclo de vida de Sistema Computarizado y software de no producto en la industria farmacéutica
1.7 **Autor del instrumento:** Rider Antonio Castillo Salirrosas

Estimado(a), se le invita a participar en el proceso de evaluación de un instrumento.
Para ello se adjunta el instrumento a evaluar y el formato que servirá para que usted pueda hacernos llegar sus apreciaciones.

Agradezco su opinión y feedback que permitirá validar el instrumento y así obtener información válida, el cual es un requerimiento para cualquier investigación.

Se solicita que lea el instrumento y luego identifique el ítem o pregunta y conteste marcando con un aspa en la casilla que usted considere conveniente.



Firma SME

National ID: 120446414 IFP

[1] SME: Subject Matter Expert

## INFORME DE OPINIÓN DE EXPERTOS O JUECES DEL INSTRUMENTO DE INVESTIGACIÓN

### I. DATOS GENERALES:

1.1 **Apellidos y nombres del SME[1]:** Sandra Patricia Fernandez
1.2 **Grado Académico o tiempo de experiencia en el área** (como experto en Sistemas de Información, Sistemas de Calidad, Sistemas Computarizados, Data Integrity y Ciberseguridad) 20 años Project Management, Quality Systems IT, Cybersecurity, Computerized System.
1.3 **Profesión:** Ingeniero de Sistemas
1.4 **Institución donde Labora:** Abbott Laboratorios – Site Colombia
1.5 **Cargo que desempeña:** LATAM GxP Applications Manager
1.6 **Nombre del instrumento:** Ciberseguridad en el ciclo de vida de Sistema Computarizado y software de no producto en la industria farmacéutica
1.7 **Autor del instrumento:** Rider Antonio Castillo Salirrosas

Estimado(a), se le invita a participar en el proceso de evaluación de un instrumento. Para ello se adjunta el instrumento a evaluar y el formato que servirá para que usted pueda hacernos llegar sus apreciaciones.

Agradezco su opinión y feedback que permitirá validar el instrumento y así obtener información válida, el cual es un requerimiento para cualquier investigación.

Se solicita que lea el instrumento y luego identifique el ítem o pregunta y conteste marcando con un aspa en la casilla que usted considere conveniente.



**Firma SME**
**DNI (C.C) . 29.873.326 Colombia**
**Ingeniero de Sistemas**
**Matricula Profesional N°: 76235-125373 COPNIA**

[1] SME: Subject Matter Expert

## INFORME DE OPINIÓN DE EXPERTOS O JUECES DEL INSTRUMENTO DE INVESTIGACIÓN

### I. DATOS GENERALES:

1.1 **Nombres y Apellidos del SME[1]:** José Roberto Hernández
1.2 **Grado Académico o tiempo de experiencia en el área** (como experto en Sistemas de Información, Sistemas de Calidad, Sistemas Computarizados, Data Integrity y Ciberseguridad), 15 años de experiencia en Aplicaciones y software, desarrollo y soluciones informáticas, Desarrollo analítico, Validación analítica, Data Integrity.
1.3 **Profesión:** Químico Farmacéutico Biólogo, Orientación Farmacia
1.4 **Institución donde Labora:** Deappharma - México
1.5 **Cargo que desempeña:** Director Ejecutivo
1.6 **Nombre del instrumento:** Ciberseguridad en el ciclo de vida de Sistema Computarizado y software de producto en la industria farmacéutica
1.7 **Autor del instrumento:** Rider Antonio Castillo Salirrosas

Estimado(a), se le invita a participar en el proceso de evaluación de un instrumento.
Para ello se adjunta el instrumento a evaluar y el formato que servirá para que usted pueda hacernos llegar sus apreciaciones.

Agradezco su opinión y feedback que permitirá validar el instrumento y así obtener información válida, el cual es un requerimiento para cualquier investigación.

Se solicita que lea el instrumento y luego identifique el ítem o pregunta y conteste marcando con un aspa en la casilla que usted considere conveniente.



25/02/2025

**Firma SME**

[1] SME: Subject Matter Expert

## INFORME DE OPINIÓN DE EXPERTOS O JUECES DEL INSTRUMENTO DE INVESTIGACIÓN

### I. DATOS GENERALES:

1.1 **Nombres y Apellidos del SME[1]:** Roel Alva Cuba
1.2 **Grado Académico o tiempo de experiencia en el área** (como experto en Sistemas de Información, Sistemas de Calidad, Sistemas Computarizados, Data Integrity y Ciberseguridad), 9 años de experiencia en Validaciones de procesos, Calificaciones, Validación de Sistemas Computarizados, Sistemas APC, Sistemas de Laboratorio.
1.3 **Profesión:** Químico Farmacéutico
1.4 **Institución donde Labora:** Abbott Laboratorios – Site Perú
1.5 **Cargo que desempeña:** Analista de Validación de Sistemas Computarizados
1.6 **Nombre del instrumento:** Ciberseguridad en el ciclo de vida de Sistema Computarizado y software de no producto en la industria farmacéutica
1.7 **Autor del instrumento:** Rider Antonio Castillo Salirrosas

Estimado(a), se le invita a participar en el proceso de evaluación de un instrumento.
Para ello se adjunta el instrumento a evaluar y el formato que servirá para que usted pueda hacernos llegar sus apreciaciones.

Agradezco su opinión y feedback que permitirá validar el instrumento y así obtener información válida, el cual es un requerimiento para cualquier investigación.

Se solicita que lea el instrumento y luego identifique el ítem o pregunta y conteste marcando con un aspa en la casilla que usted considere conveniente.



**Firma SME**

[1] SME: Subject Matter Expert

## INFORME DE OPINIÓN DE EXPERTOS O JUECES DEL INSTRUMENTO DE INVESTIGACIÓN

### I. DATOS GENERALES:

1.1 **Nombres y Apellidos del SME[1]:** Gerard Adanaque Manay
1.2 **Grado Académico o tiempo de experiencia en el área** (como experto en Sistemas de Información, Sistemas de Calidad, Sistemas Computarizados, Data Integrity y Ciberseguridad), 8 años de experiencia en soporte de TI, Validación de Sistemas Computarizados, Sistemas APC, Sistemas de Laboratorio.
1.3 **Profesión:** Ingeniería de Sistemas
1.4 **Institución donde Labora:** Abbott Laboratorios – Site Perú
1.5 **Cargo que desempeña:** Analista de Validación de Sistemas Computarizados
1.6 **Nombre del instrumento:** Ciberseguridad en el ciclo de vida de Sistema Computarizado y software de no producto en la industria farmacéutica
1.7 **Autor del instrumento:** Rider Antonio Castillo Salirrosas

Estimado(a), se le invita a participar en el proceso de evaluación de un instrumento. Para ello se adjunta el instrumento a evaluar y el formato que servirá para que usted pueda hacernos llegar sus apreciaciones.

Agradezco su opinión y feedback que permitirá validar el instrumento y así obtener información válida, el cual es un requerimiento para cualquier investigación.

Se solicita que lea el instrumento y luego identifique el ítem o pregunta y conteste marcando con un aspa en la casilla que usted considere conveniente.



**Firma SME**

[1] SME: Subject Matter Expert

# ANEXO II

| FORMATO DE EVALUACIÓN DEL INSTRUMENTO PARA DETERMINAR SU VALIDEZ | | | |
|---|---|---|---|
| | | | |
| **EVALUADOR:** | | | |
| **FECHA:** | | **INSTRUMENTO** | **IMPLEMENTACIÓN DE CIBERSEGURIDAD EN EL CICLO DE VIDA DEL SISTEMA COMPUTARIZADO Y SOFTWARE DE NO PRODUCTO** |

| INDICADORES | |
|---|---|
| **PERTINENCIA** | El ítem mide el grado de correspondencia entre el enunciado y lo que se pretende medir. |
| **CLARIDAD** | El ítem es claro (no genera confusión o contradicciones) |
| **ESCALA** | El ítem puede ser respondido de acuerdo con la escala que presenta el instrumento |
| **RELEVANCIA** | El ítem es relevante para cumplir con las preguntas y objetivos de investigación. |

**ESCALA DE VALORES**

**1 = DEFICIENTE, 2 = ACEPTABLE, 3 = REGULAR, 4 = BUENO, 5 = MUY BUENO**

**MARQUE CON UNA "X"**

| CONTENIDO | | EVALUACIÓN | | | | | OBSERVACIONES/COMENTARIOS |
|---|---|---|---|---|---|---|---|
| ÍTEM | INDICADORES | 1 | 2 | 3 | 4 | 5 | |
| **EVALUACIÓN DE LA FASE DE CONCEPTO** | | | | | | | |
| **ETAPA DE PLANIFICACIÓN** | | | | | | | |
| A.1 | COHERENCIA | | | | | | |
| | CLARIDAD | | | | | | |
| | ESCALA | | | | | | |
| | RELEVANCIA | | | | | | |
| A.2 | COHERENCIA | | | | | | |
| | CLARIDAD | | | | | | |
| | ESCALA | | | | | | |
| | RELEVANCIA | | | | | | |
| A.3 | COHERENCIA | | | | | | |
| | CLARIDAD | | | | | | |
| | ESCALA | | | | | | |
| | RELEVANCIA | | | | | | |
| A.4 | COHERENCIA | | | | | | |
| | CLARIDAD | | | | | | |
| | ESCALA | | | | | | |
| | RELEVANCIA | | | | | | |
| A.5 | COHERENCIA | | | | | | |
| | CLARIDAD | | | | | | |
| | ESCALA | | | | | | |
| | RELEVANCIA | | | | | | |
| A.6 | COHERENCIA | | | | | | |
| | CLARIDAD | | | | | | |
| | ESCALA | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | **RELEVANCIA** | | | | | | |
| **A.7** | **COHERENCIA** | | | | | | |
| | **CLARIDAD** | | | | | | |
| | **ESCALA** | | | | | | |
| | **RELEVANCIA** | | | | | | |
| **A.8** | **COHERENCIA** | | | | | | |
| | **CLARIDAD** | | | | | | |
| | **ESCALA** | | | | | | |
| | **RELEVANCIA** | | | | | | |
| **ETAPA DE ANÁLISIS DE REQUISITOS** | | | | | | | |
| **B.9** | **COHERENCIA** | | | | | | |
| | **CLARIDAD** | | | | | | |
| | **ESCALA** | | | | | | |
| | **RELEVANCIA** | | | | | | |
| **B.10** | **COHERENCIA** | | | | | | |
| | **CLARIDAD** | | | | | | |
| | **ESCALA** | | | | | | |
| | **RELEVANCIA** | | | | | | |
| **B.11** | **COHERENCIA** | | | | | | |
| | **CLARIDAD** | | | | | | |
| | **ESCALA** | | | | | | |
| | **RELEVANCIA** | | | | | | |
| **B.12** | **COHERENCIA** | | | | | | |
| | **CLARIDAD** | | | | | | |
| | **ESCALA** | | | | | | |
| | **RELEVANCIA** | | | | | | |
| **B.13** | **COHERENCIA** | | | | | | |
| | **CLARIDAD** | | | | | | |
| | **ESCALA** | | | | | | |
| | **RELEVANCIA** | | | | | | |
| **EVALUACIÓN DE LA FASE DE PROYECTO** | | | | | | | |
| **ETAPA DE DISEÑO** | | | | | | | |
| **C.14** | **COHERENCIA** | | | | | | |
| | **CLARIDAD** | | | | | | |
| | **ESCALA** | | | | | | |
| | **RELEVANCIA** | | | | | | |
| **C.15** | **COHERENCIA** | | | | | | |
| | **CLARIDAD** | | | | | | |
| | **ESCALA** | | | | | | |
| | **RELEVANCIA** | | | | | | |
| **C.16** | **COHERENCIA** | | | | | | |
| | **CLARIDAD** | | | | | | |
| | **ESCALA** | | | | | | |
| | **RELEVANCIA** | | | | | | |
| **C.17** | **COHERENCIA** | | | | | | |
| | **CLARIDAD** | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | **ESCALA** | | | | | | |
| | **RELEVANCIA** | | | | | | |
| **C.18** | **COHERENCIA** | | | | | | |
| | **CLARIDAD** | | | | | | |
| | **ESCALA** | | | | | | |
| | **RELEVANCIA** | | | | | | |
| **C.19** | **COHERENCIA** | | | | | | |
| | **CLARIDAD** | | | | | | |
| | **ESCALA** | | | | | | |
| | **RELEVANCIA** | | | | | | |
| **C.20** | **COHERENCIA** | | | | | | |
| | **CLARIDAD** | | | | | | |
| | **ESCALA** | | | | | | |
| | **RELEVANCIA** | | | | | | |
| **C.21** | **COHERENCIA** | | | | | | |
| | **CLARIDAD** | | | | | | |
| | **ESCALA** | | | | | | |
| | **RELEVANCIA** | | | | | | |
| **C.22** | **COHERENCIA** | | | | | | |
| | **CLARIDAD** | | | | | | |
| | **ESCALA** | | | | | | |
| | **RELEVANCIA** | | | | | | |
| **C.23** | **COHERENCIA** | | | | | | |
| | **CLARIDAD** | | | | | | |
| | **ESCALA** | | | | | | |
| | **RELEVANCIA** | | | | | | |
| **C.24** | **COHERENCIA** | | | | | | |
| | **CLARIDAD** | | | | | | |
| | **ESCALA** | | | | | | |
| | **RELEVANCIA** | | | | | | |
| **C.25** | **COHERENCIA** | | | | | | |
| | **CLARIDAD** | | | | | | |
| | **ESCALA** | | | | | | |
| | **RELEVANCIA** | | | | | | |
| **C.26** | **COHERENCIA** | | | | | | |
| | **CLARIDAD** | | | | | | |
| | **ESCALA** | | | | | | |
| | **RELEVANCIA** | | | | | | |
| **C.27** | **COHERENCIA** | | | | | | |
| | **CLARIDAD** | | | | | | |
| | **ESCALA** | | | | | | |
| | **RELEVANCIA** | | | | | | |
| **C.28** | **COHERENCIA** | | | | | | |
| | **CLARIDAD** | | | | | | |
| | **ESCALA** | | | | | | |
| | **RELEVANCIA** | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| C.29 | COHERENCIA | | | | | | |
| | CLARIDAD | | | | | | |
| | ESCALA | | | | | | |
| | RELEVANCIA | | | | | | |
| C.30 | COHERENCIA | | | | | | |
| | CLARIDAD | | | | | | |
| | ESCALA | | | | | | |
| | RELEVANCIA | | | | | | |
| C.31 | COHERENCIA | | | | | | |
| | CLARIDAD | | | | | | |
| | ESCALA | | | | | | |
| | RELEVANCIA | | | | | | |
| C.32 | COHERENCIA | | | | | | |
| | CLARIDAD | | | | | | |
| | ESCALA | | | | | | |
| | RELEVANCIA | | | | | | |
| C.33 | COHERENCIA | | | | | | |
| | CLARIDAD | | | | | | |
| | ESCALA | | | | | | |
| | RELEVANCIA | | | | | | |
| C.34 | COHERENCIA | | | | | | |
| | CLARIDAD | | | | | | |
| | ESCALA | | | | | | |
| | RELEVANCIA | | | | | | |
| C.35 | COHERENCIA | | | | | | |
| | CLARIDAD | | | | | | |
| | ESCALA | | | | | | |
| | RELEVANCIA | | | | | | |
| C.36 | COHERENCIA | | | | | | |
| | CLARIDAD | | | | | | |
| | ESCALA | | | | | | |
| | RELEVANCIA | | | | | | |
| C.37 | COHERENCIA | | | | | | |
| | CLARIDAD | | | | | | |
| | ESCALA | | | | | | |
| | RELEVANCIA | | | | | | |
| C.38 | COHERENCIA | | | | | | |
| | CLARIDAD | | | | | | |
| | ESCALA | | | | | | |
| | RELEVANCIA | | | | | | |
| C.39 | COHERENCIA | | | | | | |
| | CLARIDAD | | | | | | |
| | ESCALA | | | | | | |
| | RELEVANCIA | | | | | | |
| C.40 | COHERENCIA | | | | | | |
| | CLARIDAD | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | **ESCALA** | | | | | | |
| | **RELEVANCIA** | | | | | | |
| **ETAPA DE CODIFICACIÓN Y CONSTRUCCIÓN** | | | | | | | |
| **D.41** | **COHERENCIA** | | | | | | |
| | **CLARIDAD** | | | | | | |
| | **ESCALA** | | | | | | |
| | **RELEVANCIA** | | | | | | |
| **D.42** | **COHERENCIA** | | | | | | |
| | **CLARIDAD** | | | | | | |
| | **ESCALA** | | | | | | |
| | **RELEVANCIA** | | | | | | |
| **D.43** | **COHERENCIA** | | | | | | |
| | **CLARIDAD** | | | | | | |
| | **ESCALA** | | | | | | |
| | **RELEVANCIA** | | | | | | |
| **ETAPA DE IMPLEMENTACIÓN Y PRUEBAS** | | | | | | | |
| **E.44** | **COHERENCIA** | | | | | | |
| | **CLARIDAD** | | | | | | |
| | **ESCALA** | | | | | | |
| | **RELEVANCIA** | | | | | | |
| **EVALUACIÓN DE LA FASE DE OPERACIÓN** | | | | | | | |
| **ETAPA DE OPERACIÓN Y MANTENIMIENTO** | | | | | | | |
| **F.45** | **COHERENCIA** | | | | | | |
| | **CLARIDAD** | | | | | | |
| | **ESCALA** | | | | | | |
| | **RELEVANCIA** | | | | | | |
| **F.46** | **COHERENCIA** | | | | | | |
| | **CLARIDAD** | | | | | | |
| | **ESCALA** | | | | | | |
| | **RELEVANCIA** | | | | | | |
| **F.47** | **COHERENCIA** | | | | | | |
| | **CLARIDAD** | | | | | | |
| | **ESCALA** | | | | | | |
| | **RELEVANCIA** | | | | | | |
| **F.48** | **COHERENCIA** | | | | | | |
| | **CLARIDAD** | | | | | | |
| | **ESCALA** | | | | | | |
| | **RELEVANCIA** | | | | | | |
| **F.49** | **COHERENCIA** | | | | | | |
| | **CLARIDAD** | | | | | | |
| | **ESCALA** | | | | | | |
| | **RELEVANCIA** | | | | | | |
| **F.50** | **COHERENCIA** | | | | | | |
| | **CLARIDAD** | | | | | | |
| | **ESCALA** | | | | | | |
| | **RELEVANCIA** | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| F.51 | COHERENCIA | | | | | | |
| | CLARIDAD | | | | | | |
| | ESCALA | | | | | | |
| | RELEVANCIA | | | | | | |
| EVALUACIÓN DE LA FASE DE RETIRO | | | | | | | |
| ETAPA DE DECOMISIONAMIENTO | | | | | | | |
| G.52 | COHERENCIA | | | | | | |
| | CLARIDAD | | | | | | |
| | ESCALA | | | | | | |
| | RELEVANCIA | | | | | | |

# ANEXO III

## ENCUESTA

**1.-** **Objetivo:**
La presente encuesta tiene como objetivo recopilar la información sobre la experiencia de la presente herramienta o "guía para la implementación de ciberseguridad en el ciclo de vida de sistema computarizado y software de no producto" con un enfoque basado en los indicadores de la operacionalización de las variables o documentos mínimos que se pueden formar parte de la implementación de ciberseguridad.

**2.- Escala de Valores:**
1 = Deficiente, 2 = Aceptable, 3 = Regular, 4 = Bueno, 5 = Muy bueno

**3.- Instrucciones**
Estimado(a) participante la presente encuesta sirve para recoger sus apreciaciones acerca de la "guía para la implementación de ciberseguridad en el ciclo de vida de sistema computarizado y software de no producto".
Marque una "X" según crea conveniente.

| ÍTEM | ETAPAS | Aspecto a Evaluar | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1 | **PLANIFICACIÓN:** Plan de implementación de ciberseguridad. | ¿Se puede implementar un plan que permita establecer lineamientos específicos ante amenazas y vulnerabilidades en sistemas computarizados y software de no producto? | | | | | |
| 2 | **ANÁLISIS DE REQUISITOS** Especificación de requisitos de usuario (URS) / funcionales (FRS) | ¿Es posible gestionar documento técnico que especifique los requisitos de usuario y funcionales? | | | | | |
| 3 | **DISEÑO** Seguridad por diseño. | ¿Se puede gestionar un documento técnico que especifique el diseño para los sistemas computarizados y software de no producto, incluyendo la arquitectura del sistema personalizado? cuando aplique | | | | | |
| 4 | **CODIFICACIÓN Y CONSTRUCCIÓN** Desarrollo de Código Seguro | ¿Es posible gestionar un documento de desarrollo de código seguro? | | | | | |
| 5 | **CODIFICACIÓN Y CONSTRUCCIÓN** Verificación de los controles de ciberseguridad | ¿Se puede gestionar la verificación de los controles de ciberseguridad? | | | | | |
| 6 | **IMPLEMENTACIÓN Y PRUEBAS** Implementación y configuración | ¿Es posible gestionar un plan para la implementación y configuración? | | | | | |
| 7 | **OPERACIÓN Y MANTENIMIENTO** Operación y Mantenimiento | ¿Se puede gestionar un plan de manejo, uso y operación y de mantenimiento de seguridad cibernética? | | | | | |
| 8 | **DECOMISIONAMIENTO** Retiro | ¿Se puede gestionar un plan de decomisionamiento con las actividades para el retiro? | | | | | |

## ANEXO IV

<table>
<tr><td colspan="3">FASE CONCEPTO</td></tr>
<tr><td>A</td><td colspan="2">PLANIFICACIÓN</td></tr>
<tr><td>-</td><td colspan="2">Inventario</td></tr>
<tr><td>1</td><td>¿Equipo está conectado a red? ¿red con salida a internet? (mencionar IP/link)</td><td rowspan="8">Actividad/operación/variable<br><br>Plan de implementación de ciberseguridad<br><br>Objetivo:<br><br>Implementar un plan que permita establecer lineamientos específicos ante amenazas y vulnerabilidades en sistemas computarizados y software de no producto</td></tr>
<tr><td>2</td><td>¿Se encuentra instalado en PC? Mencionar RAM/Procesador / capacidad Disco Duro</td></tr>
<tr><td>3</td><td>¿Cuenta con monitor/PC/laptop o HMI?</td></tr>
<tr><td>4</td><td>¿El software se encuentra en más de 01 PC?</td></tr>
<tr><td>5</td><td>¿Cuenta con Sistema operativo? Indicar versión</td></tr>
<tr><td>6</td><td>¿Software cuenta con actualizaciones y parches de seguridad? ¿Se tiene algún plan/procedimiento?</td></tr>
<tr><td>7</td><td>¿Se cuenta con planes/procedimientos de recuperación ante desastres de software? Indicar</td></tr>
<tr><td>8</td><td>¿Se cuenta con un plan de implementación de ciberseguridad en la organización? Indicar</td></tr>
<tr><td>B</td><td colspan="2">ANÁLISIS DE REQUISITOS</td></tr>
<tr><td>-</td><td colspan="2">Especificación de requisitos de usuario (URS) / funcionales (FRS)</td></tr>
<tr><td>9</td><td>Gestionar documentos técnicos para establecer requisitos del usuario con lineamientos de ciberseguridad (data integrity, vulnerabilidad, parches de seguridad, requisitos de recuperación, gestión de interfaces, entre otros</td><td rowspan="5">Actividad/operación/variable<br><br>Especificación de requerimientos de usuario (Especificación de requerimientos funcionales.<br><br>Objetivo:<br><br>Gestionar documento técnico que especifique los requisitos de usuario y funcionales (ítem 9).</td></tr>
<tr><td>10</td><td>Identificar necesidades y expectativas del sistema computarizado y software de no producto</td></tr>
<tr><td>11</td><td>Requisitos de la seguridad física, cuando sea apropiado</td></tr>
<tr><td>12</td><td>Consideraciones para los componentes de hardware y software</td></tr>
<tr><td>13</td><td>Establecer requisitos bajo concepto básico de ciberseguridad: Confidencialidad, integridad y disponibilidad.</td></tr>
<tr><td colspan="3">FASE PROYECTO</td></tr>
</table>

| | | |
|---|---|---|
| **C** | **DISEÑO** | |
| - | **Seguridad por diseño** | |
| 14 | Gestionar la revisión de la seguridad por diseño para los sistemas computarizados y software de no producto, incluyendo la arquitectura del sistema personalizado cuando aplique. | |
| 15 | Datos del Proveedor:<br><br>Fabricante/Desarrollador, cuando aplique | |
| 16 | ¿Tiene puertos USB activos? ¿Cuántos? | |
| 17 | ¿Se utilizan los puertos durante la operación rutinaria del equipo o durante su mantenimiento? | |
| 18 | ¿Se pueden bloquear los puertos disponibles para dispositivos de almacenamiento masivo y eliminarlos del uso? | |
| 19 | ¿El Proveedor se encuentra calificado con criterios de ciberseguridad (data integrity, vulnerabilidad, parches de seguridad, requisitos de recuperación, gestión de interfaces, entre otros)? | |
| 20 | ¿Se accede remotamente? ¿El activo tiene una conexión remota como una conexión de escritorio remoto? | **Actividad/operación/variable**<br><br>Seguridad por diseño<br><br>**Objetivo:**<br><br>Gestionar documento técnico que especifique el diseño para los sistemas computarizados y software de no producto, incluyendo la arquitectura del sistema personalizado cuando aplique. |
| 21 | **Parches y actualizaciones de software**<br><br>¿El activo tiene un método/plan controlado para la realización de parches y actualizaciones? | |
| 22 | **Protección de Malware**<br><br>¿El activo cuenta con herramientas de protección contra malware? | |
| 23 | **Interfaces seguras**<br><br>¿El activo tiene interfaces con otros sistemas/dispositivos? | |
| 24 | **Seguridad Física**<br><br>¿El activo está ubicado físicamente en un área con acceso controlado? (por ejemplo, una ubicación que requiere controles de acceso únicos)<br><br>**Nota:** La tarjeta de acceso a la instalación no es suficiente como acceso de control. | |
| 25 | **Control de Accesos** | |

| | | |
|---|---|---|
| | ¿Cuenta con control de accesos? | |
| 26 | ¿Usuarios son gestionados por un administrador de accesos? | |
| 27 | ¿El activo requiere autenticación de usuario individual para acceder? | |
| 28 | ¿Se pueden deshabilitar/inhabilitar cuentas? | |
| 29 | **Fortalecimiento del Sistema**<br><br>¿Cuenta la organización con herramientas para el fortalecimiento del sistema bajo un enfoque en ciberseguridad (Eliminar archivos y contraseñas predeterminadas, proteger archivos con información crítica para el negocio, violentar algoritmos confidenciales, eliminar aplicaciones y servicios innecesarios)? | |
| 30 | ¿Puede el activo eliminar el acceso de los usuarios que no lo utilizaron durante 90 días? | |
| 31 | ¿Existe algún documento estandarizado activo de gestión de accesos? | |
| 32 | ¿Se puede crear más de 01 usuario? ¿Permite realizar cuentas individualizadas? | |
| 33 | ¿Existen usuarios compartidos? | |
| 34 | ¿Existen roles diferenciados por nivel de acceso? ¿Cuáles? | |
| 35 | ¿Permite la creación de grupos o roles? | |
| 36 | ¿El software permite asignar/definir privilegios específicos? | |
| 37 | ¿Se puede establecer /definir una contraseña? | |
| 38 | ¿Las contraseñas se encuentran encriptadas? | |
| 39 | ¿Se puede modificar complejidad de la contraseña? | |
| 40 | ¿Existe bloqueo por inactividad / Logout? | |
| **D** | **CODIFICACIÓN Y CONSTRUCCIÓN** | |
| - | **Desarrollo de código seguro** | |
| 41 | ¿La organización desarrolla sistemas personalizados de software de no producto? ***Nota:*** *Aplica para sistemas computarizados y software de no producto para desarrollos in house.* | **Actividad/operación/variable**<br><br>Código seguro |
| 42 | Gestionar el diseño para los sistemas computarizados y software de no producto, considerando estándares de | |

| | | |
|---|---|---|
| | codificación de seguridad cibernética, comprobaciones de seguridad, exploraciones de vulnerabilidades de los componentes y herramientas de análisis de códigos estáticos. | **Objetivo:**<br>Gestionar un documento de desarrollo de código seguro. |
| - | **Verificación de controles de ciberseguridad** | |
| 43 | ¿Está codificado, construido, instalado y verificado en todas las pruebas para su uso previsto (de acuerdo con los requerimientos de usuario), incluir pruebas de penetración?<br>***Nota:*** *Las pruebas deben ser ejecutadas por probadores capacitados.* | **Actividad/operación/variable**<br>Controles de ciberseguridad<br>**Objetivo:**<br>Gestionar la verificación de los controles de ciberseguridad |
| **E** | **IMPLEMENTACIÓN Y PRUEBAS** | |
| - | **Implementación y configuración** | |
| 44 | ¿Se tiene establecido un plan para ejecutar pruebas y controles de seguridad cibernética? | **Actividad/operación/variable**<br>Implementación y configuración<br>**Objetivo:**<br>Gestionar un plan para la implementación y configuración |
| **FASE OPERACIÓN** | | |
| **F** | **OPERACIÓN Y MANTENIMIENTO** | |
| - | **Operación** | |
| 45 | ¿Permite modificar zona horaria, fecha y hora sistema operativo y/o software? | **Actividad/operación/variable**<br>Operación y Mantenimiento<br>**Objetivo:** |
| 46 | ¿Cuenta con un documento estandarizado para el manejo, uso y operación del equipo que relacione al software? | |
| 47 | ¿Cuenta con UPS? | |
| 48 | ¿Existe algún documento estandarizado para la gestión de recetas? Indicar código | |
| 49 | ¿El Sistema de alarmas monitorea y registra en el software? Indicar alarmas | |
| - | **Mantenimiento** | |

| | | |
|---|---|---|
| 50 | Establecer un plan para identificar, monitorear, comunicar y elevar las señales de seguridad cibernética, incluidos los roles y responsabilidades definidos para cada uno. | Gestionar un plan de manejo, uso y operación y de mantenimiento de seguridad cibernética. |
| 51 | ¿Existe algún documento estandarizado de copias de seguridad y restauración de datos? | |
| **FASE RETIRO** | | |
| **G** | **DECOMISIONAMIENTO** | |
| - | **Baja de activos** | |
| 52 | Establecer un plan de decomisionamiento con las actividades para el retiro: documentación, conversión y migración de datos. | **Actividad/operación/variable**<br><br>Decomisionamiento<br><br>**Objetivo:**<br><br>Gestionar un plan de decomisionamiento con las actividades para el retiro. |