



UPSE

**UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO**

TÍTULO

**MODELO DE CIBERSEGURIDAD PARA LA INFRAESTRUCTURA
TECNOLÓGICA DE LA EMPRESA FARMACÉUTICA
GLOBESER S.A.S.**

AUTOR

Liriano Ramírez, Alex Fabian

TRABAJO DE TITULACIÓN

**Previo a la obtención del grado académico en
MAGÍSTER EN CIBERSEGURIDAD**

TUTOR

Suarez Riofrio, Patricia Leonor

Santa Elena, Ecuador

Año 2026



**UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO
TRIBUNAL DE SUSTENTACIÓN**



Validar únicamente en FirmaEC.
Firmado electrónicamente por:
**ALICIA GERMANIA
ANDRADE VERA**

**Ing. Alicia Andrade Vera, Mgtr.
COORDINADORA DEL
PROGRAMA**



Validar únicamente en FirmaEC.
Firmado electrónicamente por:
**PATRICIA LEONOR
SUAREZ RIOFRIO**

**Ing. Patricia Suárez Riofrío, Ph.D.
TUTOR**



Validar únicamente en FirmaEC.
Firmado electrónicamente por:
**JAIME BENJAMIN
OROZCO IGUASNIA**

**Ing. Jaime Orozco Iguasnia, Mgtr.
DOCENTE
ESPECIALISTA**



Validar únicamente en FirmaEC.
Firmado electrónicamente por:
**CARLOS EFRAIN
SANCHEZ LEON**

**Ing. Carlos Sánchez León, Mgtr.
DOCENTE
ESPECIALISTA**



Validar únicamente en FirmaEC.
Firmado electrónicamente por:
**MARIA MARGARITA
RIVERA GONZALEZ**

**Abg. María Rivera González, Mgtr.
SECRETARIA GENERAL
UPSE**



**UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO**

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por **LIRIANO RAMÍREZ ALEX FABIAN**, como requerimiento para la obtención del título de Magíster en Ciberseguridad.

TUTOR



Ing. Patricia Suárez Riofrío, Ph.D.

Santa Elena, 3 de Julio del 2026



**UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO**

DECLARACIÓN DE RESPONSABILIDAD

Yo, **LIRIANO RAMÍREZ ALEX FABIAN**

DECLARO QUE:

El trabajo de Titulación, **“MODELO DE CIBERSEGURIDAD PARA LA INFRAESTRUCTURA TECNOLÓGICA DE LA EMPRESA FARMACÉUTICA GLOBESER S.A.S.”** previo a la obtención del título en Magíster en Ciberseguridad, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Santa Elena, 3 de Julio del 2026

EL AUTOR



Validar únicamente en FirmaEC.
Firmado electrónicamente por:
**ALEX FABIAN LIRIANO
RAMIREZ**

Liriano Ramírez Alex Fabian



UPSE

**UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO**

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado **“MODELO DE CIBERSEGURIDAD PARA LA INFRAESTRUCTURA TECNOLÓGICA DE LA EMPRESA FARMACÉUTICA GLOBESER S.A.S.”**, presentado por el estudiante, **LIRIANO RAMÍREZ ALEX FABIAN** fue enviado al Sistema Antiplagio COMPILATIO, presentando un porcentaje de similitud correspondiente al 3%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.



Analysis report
Compilatio Magister+ | UPSE-ECU

ALEX LIRIANO - Examen Complexivo - Componente Practico NOVENA REVISADO 01072026

ID : 7ad9a3734dd19f6dc0057bf9ad46e41b73d5de5c



3%
Suspicious texts

File name : ALEX LIRIANO - Examen Complexivo - Componente Practico
NOVENA REVISADO 01072026.txt
Original file size : 1.41 MB
Number of words : 16,233

Submitter : PATRICIA LEONOR SUAREZ RIOFRIO
Submission date : July 2, 2026
Upload type : interface
analysis end date : July 2, 2026

TUTOR



Validar únicamente en FirmaEC.
Firmado electrónicamente por:
**PATRICIA LEONOR
SUAREZ RIOFRIO**

Ing. Patricia Suárez Riofrío, Ph.D.



**UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO**

AUTORIZACIÓN

Yo, LIRIANO RAMÍREZ ALEX FABIAN

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de examen de carácter complejo con fines de difusión pública, además apruebo la reproducción de este examen de carácter complejo dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor.

Santa Elena, 3 de Julio del 2026

EL AUTOR



Verificar únicamente en FirmaBC.
Firmado electrónicamente por:
**ALEX FABIAN LIRIANO
RAMIREZ**

Liriano Ramírez Alex Fabian

AGRADECIMIENTO

Agradezco eternamente a mi dios mi creador, por darme la fortaleza necesaria, e iluminar mi mente y corazón, por la oportunidad que me ha brindado para demostrar que en esta vida nada es imposible.

A mi madre y a mi padre que siempre estuvieron motivándome para que no desmayara en mis metas planteadas, y que gracias a sus consejos pude obtener este importante logro.

De manera especial a la Ph.D. Patricia Suárez por toda la paciencia que me ha tenido en calidad de Tutor para la elaboración de la presente investigación.

A mis maestros de la Universidad Estatal Península de Santa Elena, por su formación académica recibida.

Alex Fabian Liriano Ramírez

DEDICATORIA

A Dios, por ser mi gran confidente en el diario vivir y darme esa fortaleza día a día para poder cumplir uno de mis sueños anhelados.

A mis padres, hermanos, esposa y mis 3 hijos por toda su ayuda y comprensión que de muchas maneras aportaron para culminar con éxito este proceso de formación académica y poder cumplir una etapa más de mi vida.

Alex Fabian Liriano Ramírez

ÍNDICE GENERAL

TRIBUNAL DE SUSTENTACIÓN.....	II
CERTIFICACIÓN	III
DECLARACIÓN DE RESPONSABILIDAD	IV
CERTIFICACIÓN DE ANTIPLAGIO	V
AUTORIZACIÓN.....	VI
AGRADECIMIENTO.....	VII
DEDICATORIA.....	VIII
ÍNDICE GENERAL.....	IX
ÍNDICE DE TABLAS.....	XII
ÍNDICE DE FIGURAS	XIII
RESUMEN	XIV
ABSTRACT.....	XV
INTRODUCCIÓN.....	1
CAPÍTULO I.....	4
1. FUNDAMENTACIÓN.....	4
1.1 ANTECEDENTES.....	4
1.2 PREGUNTA GENERAL	5
1.3 PREGUNTAS ESPECÍFICAS	5
1.4 DESCRIPCIÓN DEL PROYECTO.....	6
1.5 OBJETIVOS DEL PROYECTO	7
1.5.1 OBJETIVO GENERAL.....	8
1.5.2 OBJETIVOS ESPECÍFICOS.....	8
1.6 JUSTIFICACIÓN DEL PROYECTO.....	8

1.7	ALCANCE DEL PROYECTO.....	9
CAPÍTULO 2.....		11
2.	MARCO TEÓRICO Y METODOLOGÍA DEL PROYECTO.....	11
2.1	MARCO TEÓRICO	11
2.2	METODOLOGÍA DEL PROYECTO.....	23
2.2.1	DISEÑO Y ALCANCE DE LA INVESTIGACIÓN	24
2.2.2	METODOLOGÍA DE INVESTIGACIÓN.....	24
2.2.3	TIPO Y MÉTODOS DE INVESTIGACIÓN	25
2.2.4	TÉCNICAS DE ANÁLISIS DOCUMENTAL Y NORMATIVO ..	26
CAPÍTULO 3.....		30
3.	PROPUESTA.....	30
3.1	TEMA DE LA PROPUESTA	30
3.2	OBJETIVO	30
3.3	ANÁLISIS DOCUMENTAL Y TÉCNICO REFERENCIAL PARA EL DISEÑO DEL MODELO.....	30
3.3.1	Análisis normativo comparativo ISO 27001, NIST CSF y CIS Controls.....	31
3.3.2	Identificación de activos de información	32
3.3.3	Identificación de vulnerabilidades	32
3.3.4	Identificación de amenazas.....	33
3.3.5	Análisis de riesgos	33
3.3.6	Brechas frente a estándares de ciberseguridad	33
3.4	CRONOGRAMA.....	34
3.5	DISEÑO DEL MODELO DE CIBERSEGURIDAD	34
3.6	ESTRUCTURA DEL MODELO DE CIBERSEGURIDAD.....	35

3.7	MATRIZ DE TRAZABILIDAD DEL MODELO	36
3.8	INDICADORES PROPUESTOS (KPIs) PARA SEGUIMIENTO.....	37
3.9	VALIDACIÓN CONCEPTUAL REFERENCIAL DEL MODELO (PROPUESTA)	37
3.10	DEFINICIÓN OPERACIONAL MÍNIMA DE LOS COMPONENTES DEL MODELO.....	38
3.11	HALLAZGOS DEL ANÁLISIS DE ACTIVOS, RIESGOS Y CONTROLES	40
3.12	SÍNTESIS DIAGNÓSTICA PARA EL DISEÑO DEL MODELO	42
3.13	ESTIMACIÓN REFERENCIAL DE RECURSOS PARA LA ADOPCIÓN INSTITUCIONAL DEL MODELO DE CIBERSEGURIDAD.....	44
	CONCLUSIONES.....	45
	RECOMENDACIONES	47
	REFERENCIAS	48
	ANEXOS.....	50

ÍNDICE DE TABLAS

Tabla 1. Matriz comparativa de estándares de ciberseguridad -----	27
Tabla 2 Checklist de verificación -----	29
Tabla 3 Cronograma de Actividades-----	34
Tabla 4 Trazabilidad del Modelo-----	36
Tabla 5 Indicadores Propuestos -----	37
Tabla 6 Propuesta de Validación conceptual -----	38
Tabla 7 Propuesta definición operacional mínima del modelo -----	39
Tabla 8 Modelo de Inventario de Activos Tecnológicos -----	40
Tabla 9 Controles de Activos y Riesgo -----	42
Tabla 10 Matriz de análisis documental de estándares-----	52
Tabla 11 Escala de madurez -----	55
Tabla 12 Matriz de nivel de madurez por componente -----	55

ÍNDICE DE FIGURAS

Gráfica 1 Estructura ciberseguridad	11
Gráfica 2 Estructura PDCA-ISO 27001	14
Gráfica 3 Estructura del Modelo de Ciberseguridad	35

RESUMEN

El presente trabajo de investigación, “Modelo de ciberseguridad para la infraestructura tecnológica de la empresa farmacéutica GLOBESER S.A.S.”, tiene como objetivo diseñar un modelo que garantice la confidencialidad, integridad y disponibilidad de la información de la organización. Para su desarrollo, se analizan estándares, marcos y buenas prácticas en ciberseguridad, como ISO 27001, NIST y CONTROLES CIS, con el fin de seleccionar aquellos que se alineen a las necesidades de la empresa. La investigación es de tipo diseño, de carácter no experimental, con enfoque documental y técnico, utiliza los métodos inductivo, deductivo, analítico y sintético para evaluar la situación actual de la infraestructura tecnológica. A partir del análisis documental, técnico y normativo, se establecen de manera referencial los elementos necesarios para formular una propuesta metodológica de ciberseguridad adaptada al contexto de la empresa.

Palabras claves:

Ciberseguridad, seguridad de la información y gestión de riesgos

ABSTRACT

This research, entitled “Cybersecurity Model for the Technological Infrastructure of the pharmaceutical company GLOBESER S.A.S.”, aims to design a model to ensure the confidentiality, integrity, and availability of organizational information. The study analyzes internationally recognized standards and frameworks, such as ISO/IEC 27001, the NIST Cybersecurity Framework and the CIS Controls, to identify those aligned with the organization’s needs. The research follows a design-based, non-experimental approach with a documentary and technical focus, applying inductive, deductive, analytical, and synthetic methods to assess the current state of the technological infrastructure. Based on this analysis, key elements are defined to support the formulation of a cybersecurity methodological proposal adapted to the organizational context.

Keywords:

Cybersecurity, information security y risk management

INTRODUCCIÓN

La ciberseguridad se establece como un eje estratégico dentro de la seguridad integral organizacional, orientado a la protección de la información y a la continuidad del negocio. En este sentido, el desarrollo de un modelo metodológico de ciberseguridad se formula como una propuesta para abordar de manera estructurada los desafíos asociados a la gestión de la seguridad de la información en la empresa GLOBESER S.A.S., franquicia de la cadena de Farmacias Cruz Azul perteneciente al Grupo Difare S.A. en la Provincia de Santa Elena. Como insumos se toman como referencia los reportes técnicos del área de TI, en los que se describen incidentes de seguridad y debilidades relacionadas con la ausencia de controles de protección, deficiencias en la gestión de credenciales, equipos tecnológicos obsoletos, limitaciones en el control de accesos y necesidades de capacitación del personal. Estos elementos constituyen una base referencial para la formulación de una propuesta orientada a la gestión de riesgos de ciberseguridad en un entorno altamente sensible como el sector farmacéutico.

Por lo cual el estudio tiene como propósito diseñar un modelo de ciberseguridad que oriente la protección de la confidencialidad, integridad y disponibilidad (Caballero, 2022) de la infraestructura tecnológica de la empresa farmacéutica GLOBESER S.A.S., que comprende 15 farmacias Cruz Azul ubicadas en los tres cantones de la Provincia de Santa Elena y el área administrativa que se encuentra en la matriz principal en la ciudad de la Libertad. La infraestructura tecnológica se estructura desde la oficina matriz, donde se dispone de tres estaciones destinadas a funciones administrativas. En el departamento de sistemas se encuentra un servidor central de base de datos, el cual también cumple funciones de hosting, además de dos estaciones orientadas al monitoreo y soporte técnico. A nivel de cada farmacia, se cuenta con un servidor replicador de base de datos, estaciones de trabajo para la facturación al consumidor final, sistemas de videovigilancia y servicios de telefonía IP. La conectividad de su infraestructura se realiza a través del proveedor Telconet bajo un plan corporativo. En cuanto al entorno de software, la organización opera con el sistema de facturación denominado Neptuno, correo electrónico y sistemas de marcaciones.

El presente trabajo de investigación se desarrolla como una propuesta metodológica de diseño sustentada en análisis documental, técnico y normativo, sin contemplar implementación operativa ni aplicación de muestreos e instrumentos empíricos. En este marco, el modelo propuesto se fundamenta en el análisis de estándares, marcos de referencia y buenas prácticas (Ramírez Vargas & Pereda Otero, 2023), como ISO 27001, NIST CSF y CIS Controls, se seleccionan aquellos que mejor se alinean a las necesidades de la empresa farmacéutica GLOBESER S.A.S., sin incluir la implementación.

El modelo de ciberseguridad se establece como una propuesta metodológica orientada a estructurar criterios para la identificación y análisis de activos de información, así como las amenazas, vulnerabilidades y riesgos, con el propósito de orientar el fortalecimiento de la seguridad de la información y a la alineación con requisitos normativos aplicables.

Desde el ámbito social, este estudio se orienta a generar beneficios potenciales a los empleados y clientes de la comunidad, al establecer lineamientos enfocados en la protección de la información relacionada con la salud.

Desde el ámbito profesional, el presente trabajo propone una metodología de diseño y modelado para la gestión de la ciberseguridad en empresas farmacéuticas a nivel nacional.

Desde el ámbito científico, propone un modelo estructurado que puede ser replicado o adaptado por otras organizaciones comerciales, fortaleciendo el conocimiento aplicado en ciberseguridad.

Finalmente, el modelo constituye una referencia metodológica para otras franquicias del Grupo Difare S.A. y empresas del sector farmacéutico de la Provincia de Santa Elena y a nivel nacional.

CAPÍTULO I

1. FUNDAMENTACIÓN

1.1 ANTECEDENTES

El sector farmacéutico experimenta un acelerado proceso de automatización, incorporando sistemas informáticos para la gestión de inventarios, ventas, control de recetas, facturación electrónica, bases de datos de clientes y proveedores. Este proceso ha permitido mejorar la eficiencia operativa, pero también incrementa de manera significativa la exposición de las organizaciones a riesgos de ciberseguridad, especialmente en empresas que no cuentan con políticas ni controles adecuados de protección de la información.

La empresa GLOBESER S.A.S., franquicia de la cadena Farmacias Cruz Azul perteneciente al Grupo Difare S.A., opera en la provincia de Santa Elena mediante una red de 15 farmacias y una oficina administrativa central, apoyándose de forma casi total en una infraestructura tecnológica para la ejecución de sus procesos críticos de negocio. La organización gestiona diariamente información altamente sensible, como datos personales de clientes, historiales de compra de medicamentos, inventarios farmacéuticos, registros de proveedores, transacciones financieras y reportes regulatorios exigidos por las autoridades sanitarias. Durante los últimos doce meses el personal de TI de la empresa dispone de un informe técnico considerado como un insumo de referencia de los problemas que afectan la seguridad informática, en el que se describen incidentes asociados a vulnerabilidades críticas, incluyendo accesos no autorizados, equipos obsoletos, infecciones de malware, uso indebido de credenciales, fallas de actualización de sistemas, dispositivos externos no controlados y debilidades en los controles de acceso físico y lógico. Estos incidentes pueden generar interrupciones operativas, riesgos de fuga de información, exposición a sanciones regulatorias y una creciente preocupación por parte de la gerencia sobre la confiabilidad de los sistemas. Entre los hechos más relevantes se encuentra la inexistencia de un firewall perimetral, el uso de sistemas operativos obsoletos en estaciones de trabajo, contraseñas débiles compartidas entre empleados, accesos activos de extrabajadores, ausencia de monitoreo en tiempo real de cámaras y servidores, y una nula capacitación formal del personal en temas de ciberseguridad. Estas

situaciones permiten evidenciar una posible infraestructura tecnológica vulnerable y una cultura organizacional limitada en materia de protección de la información.

Esta problemática no es un caso aislado. Estudios indican que el sector salud y farmacéutico es uno de los más atacados por cibercriminales, debido al alto valor de la información médica y financiera. Asimismo, investigaciones académicas basadas en los estándares ISO 27001, NIST CSF y CIS CONTROLS señalan que las organizaciones que carecen de una gestión de seguridad de la información presentan mayores índices de incidentes y pérdidas económicas. A nivel latinoamericano, diversos proyectos de investigación en ciberseguridad organizacional indican que el desarrollo de modelos basados en estándares internacionales propone reducir significativamente la cantidad de vulnerabilidades, contribuye a la gestión de riesgos y la continuidad del negocio. Sin embargo, en muchas empresas del sector farmacéutico ecuatoriano, no se cuenta con prácticas formales de ciberseguridad. Por lo tanto, la situación de GLOBESER S.A.S. representa un problema real y crítico, que plantea la necesidad de una solución estructurada, técnica y normativa.

Este contexto justifica plenamente la necesidad de desarrollar un diseño de modelo de ciberseguridad orientado a la protección de la infraestructura tecnológica de la empresa que cumple un rol estratégico en la salud y bienestar para la comunidad.

1.2 PREGUNTA GENERAL

¿De qué manera un modelo de ciberseguridad contribuye al fortalecimiento de la seguridad de la infraestructura tecnológica de la empresa farmacéutica GLOBESER S.A.S.?

1.3 PREGUNTAS ESPECÍFICAS

- ¿Qué vulnerabilidades, amenazas, riesgos y activos críticos requieren mayores controles de ciberseguridad en la infraestructura tecnológica de GLOBESER S.A.S.?

- ¿Qué estándares, buenas prácticas y marcos de referencia como ISO 27001, NIST CSF, CIS CONTROLS son aplicables al diseño del modelo de ciberseguridad orientado al fortalecimiento de la infraestructura tecnológica de la empresa?
- ¿Cuál es el alcance esperado del modelo de ciberseguridad propuesto para el fortalecimiento de la seguridad de la infraestructura tecnológica en la empresa?

1.4 DESCRIPCIÓN DEL PROYECTO

El presente proyecto de investigación tiene como propósito el diseño de un modelo de ciberseguridad orientado a fortalecer la infraestructura tecnológica de la empresa farmacéutica GLOBESER S.A.S., franquicia de la cadena Farmacias Cruz Azul del Grupo Difare S.A., la cual opera mediante una red de 15 farmacias en la provincia de Santa Elena.

La organización depende de manera crítica de sistemas informáticos para la gestión de ventas, inventarios, datos de clientes, proveedores y procesos administrativos, lo que la expone a diversos riesgos de ciberseguridad. El proyecto consiste en la elaboración de un modelo de ciberseguridad que se ajuste a las necesidades de la empresa, el mismo que a través de una propuesta metodológica, orientada a mejorar la gestión del estado actual de los activos de información, sistemas y redes. El modelo contempla la identificación de manera referencial activos, vulnerabilidades, amenazas y riesgos, que afectan la confidencialidad, integridad y disponibilidad de la información.

A partir del análisis propuesto, se orienta el desarrollo de un diseño de modelo de ciberseguridad basado en buenas prácticas y estándares internacionales, tales como ISO 27001, NIST y CIS Controls, seleccionando aquellos que mejor se alineen a las necesidades de la empresa. Este modelo tiene como finalidad establecer lineamientos, políticas y controles orientados a mejorar la gestión de la seguridad de la información en

la organización. Es importante señalar que el alcance del presente estudio se limita exclusivamente a una propuesta metodológica de diseño, sin considerar su implementación operativa.

El modelo propone políticas de seguridad, controles técnicos, procedimientos operativos, gestión de riesgos, monitoreo, respuesta a incidentes y un componente de capacitación del personal, adaptado a la realidad operativa de la infraestructura tecnológica de la empresa farmacéutica, y sirva como referencia en organizaciones similares del sector farmacéutico.

Desde el punto de vista tecnológico, el proyecto contempla aspectos relacionados con seguridad de redes, protección de servidores, control de accesos, seguridad de aplicaciones, gestión de usuarios, respaldo de información y monitoreo, apoyándose en buenas prácticas reconocidas internacionalmente. Asimismo, propone incorporar un componente de formación y concientización del personal, orientados al fortalecimiento de la cultura organizacional de ciberseguridad.

Este trabajo incorpora líneas de investigación de la carrera relacionadas con la Tecnología y Sistemas de la Información adaptadas a las sublíneas como TSI en las organizaciones y en la sociedad, Ingeniería y gestión de TSI, Redes y Seguridad de la Información, ya que aborda un problema real que depende críticamente de su infraestructura tecnológica. Además, el proyecto plantea una solución aplicable y replicable en otras franquicias del Grupo Difare S.A., con el propósito de contribuir al fortalecimiento de la seguridad digital y a la continuidad de los servicios de salud.

1.5 OBJETIVOS DEL PROYECTO

Diseñar un modelo de ciberseguridad, basado en estándares internacionales como ISO 27001, NIST CSF y CIS Controls, que permita fortalecer la protección de la infraestructura tecnológica de la empresa farmacéutica GLOBESER S.A.S., garantizando la confidencialidad, integridad y disponibilidad de la información.

1.5.1 OBJETIVO GENERAL

Diseñar un modelo de ciberseguridad que garantice la confidencialidad, integridad y disponibilidad de la infraestructura tecnológica de la empresa farmacéutica GLOBESER S.A.S.

1.5.2 OBJETIVOS ESPECÍFICOS

- Analizar los principales estándares, marcos y buenas prácticas de ciberseguridad, con el fin de identificar y seleccionar aquellos que mejor se alineen con las necesidades de GLOBESER S.A.S., garantizando la confiabilidad y disponibilidad de su infraestructura tecnológica.
- Definir un marco conceptual y metodológico para la identificación y análisis de activos de información, así como las amenazas, vulnerabilidades y riesgos asociados a la infraestructura tecnológica de la empresa, alineados en estándares internacionales, como fundamento para el diseño del modelo de ciberseguridad.
- Diseñar un modelo de ciberseguridad como propuesta metodológica adaptado a la realidad tecnológica, operativa y normativa de la empresa farmacéutica.

1.6 JUSTIFICACIÓN DEL PROYECTO

La empresa GLOBESER S.A.S., franquiciado de la cadena CRUZ AZUL perteneciente al Grupo Difare S.A. Empresa Distribuidora Farmacéutica en todo el país, dedicada a la venta de medicamentos y productos de consumo, enfrenta serias vulnerabilidades en su infraestructura tecnológica debido al uso inadecuado de los activos de información, la ausencia de controles efectivos y la falta de aplicación de normas y principios de diseño seguro.

Las empresas farmacéuticas manejan información crítica, regulada y de alto valor intelectual. Cualquier alteración o robo de datos puede afectar procesos de producción, inventarios, regulaciones sanitarias y el cumplimiento con entidades de control. Los ataques dirigidos a empresas del sector salud y

farmacéutico han aumentado globalmente. La infraestructura tecnológica de GLOBESER S.A.S. necesita mecanismos robustos para prevenir intrusiones, fugas de información y ataques de ransomware, una falla de seguridad puede generar interrupciones críticas en sus sistemas de la información, generando pérdidas económicas y afectando la cadena de suministro farmacéutica.

El proyecto desarrolla un modelo de ciberseguridad aplicable o adaptable a empresas similares del sector farmacéutico o comercial. Asimismo, el modelo se concibe como base técnica y normativa para la adopción institucional del modelo por parte de la organización, ya que establece políticas, controles y procedimientos orientados al cumplimiento de estándares internacionales, la reducción de riesgos frente a amenazas emergentes.

En este contexto, la presente investigación se justifica en plantear una propuesta de herramienta integral para salvaguardar la infraestructura tecnológica que involucra sus activos de información, orienta la optimización de procesos y una cultura de ciberseguridad que respalde la eficiencia y la innovación en la industria farmacéutica.

1.7 ALCANCE DEL PROYECTO

En el presente trabajo de investigación se tiene como alcance la elaboración de una propuesta metodológica de diseño de ciberseguridad para la infraestructura tecnológica de la empresa GLOBESER S.A.S. franquiciado del Grupo Difare S.A., la cual brinda servicio de venta de medicina y productos de consumo en cadenas de farmacias Cruz Azul mediante herramientas tecnológicas, donde se analizarán los estándares, marcos de referencia y buenas prácticas de ciberseguridad ya mencionados previamente, con el fin de identificar y seleccionar aquellos que mejor se alineen a las necesidades de la empresa y diseñar la estructura del modelo integral de ciberseguridad que garantice la confidencialidad, integridad y disponibilidad de la infraestructura tecnológica.

El modelo propuesto establece lineamientos conceptuales y procedimentales orientados a la gestión de incidentes y vulnerabilidades, sin que ello implique ejecución o implementación en el presente estudio.

Dentro del estudio técnico, la propuesta comprende los siguientes elementos:

- Revisión referencial del nivel de madurez de la infraestructura tecnológica, con fines de diseño del modelo.
- Identificación conceptual de sus activos tecnológicos críticos.
- Revisión teórica de amenazas y riesgos que afectan la infraestructura.
- Determinación referencial de posibles brechas respecto a estándares internacionales.
- Diseño de un modelo integral de ciberseguridad con base en estándares, marcos y buenas prácticas
- Valoración técnica referencial mediante matrices comparativas y de riesgos, como apoyo al diseño del modelo.

El modelo propone medidas de protección en:

- Redes internas y perimetrales.
- Servidores y servicios corporativos.
- Aplicaciones y bases de datos.
- Sistemas de acceso, autenticación y monitoreo.
- Buenas prácticas de ciberseguridad

Por tal motivo, con base en los lineamientos establecidos, el proyecto propone un diseño de modelo de ciberseguridad sustentado en una propuesta metodológica estructurada, orientada a establecer un marco para la formación conceptual del personal involucrado en la organización para el buen uso de sus activos de información, definición de procedimientos y buenas prácticas en la gestión de la seguridad de la información.

Con este alcance, el modelo constituye una referencia replicable para otras franquicias del Grupo Difare S.A

CAPÍTULO 2

2. MARCO TEÓRICO Y METODOLOGÍA DEL PROYECTO

2.1 MARCO TEÓRICO

Principios fundamentales de la ciberseguridad

La ciberseguridad se refiere al conjunto de políticas, procedimientos, tecnologías y prácticas diseñadas para proteger los sistemas informáticos, redes y datos frente a accesos no autorizados, ataques cibernéticos y daños intencionales o accidentales (Paez, 2025). Su objetivo principal es salvaguardar la información y garantizar la continuidad de las operaciones en las organizaciones.

En el contexto empresarial, la ciberseguridad se ha convertido en un elemento estratégico, especialmente en sectores críticos como el farmacéutico, donde se maneja información sensible relacionada con la salud, datos personales y transacciones comerciales (Caballero, 2022)

Confidencialidad: Garantiza que la información solo sea accesible a personas autorizadas.

Integridad: Asegura que la información no sea alterada de manera no autorizada.

Disponibilidad: Garantiza que la información esté accesible cuando se requiera.

Estos principios guían el diseño del modelo de ciberseguridad propuesto para GLOBESER S.A.S. (Mendizábal, 2018)



Gráfica 1 Estructura ciberseguridad

Infraestructura Tecnológica

La infraestructura tecnológica está conformada por el conjunto de recursos físicos y lógicos que permiten el funcionamiento de los sistemas de información dentro de una organización. Incluye hardware, software, redes, bases de datos y sistemas de comunicación (ISACA, 2012).

Una infraestructura tecnológica vulnerable puede comprometer la operación del negocio y facilitar ataques informáticos.

Amenazas, Vulnerabilidades y Riesgos

Una amenaza es cualquier evento potencial que puede causar daño a un sistema, como ataques de malware o errores humanos, una vulnerabilidad es una debilidad que puede ser explotada por una amenaza, y el riesgo es la probabilidad de que una amenaza aproveche una vulnerabilidad generando un impacto negativo en la organización (Fortinet, 2025).

El análisis conjunto de estos elementos permite establecer estrategias de mitigación dentro del modelo de ciberseguridad.

Las vulnerabilidades tecnológicas son debilidades presentes en el hardware, software o procedimientos que pueden ser explotadas por atacantes para comprometer la seguridad. Estas pueden originarse por configuraciones incorrectas, falta de actualizaciones, malas prácticas de los usuarios o deficiencias en las políticas de seguridad. Por su parte, las amenazas informáticas se manifiestan en forma de malware, phishing, ransomware, entre otros. La combinación de amenazas y vulnerabilidades incrementa significativamente el nivel de riesgo dentro de las organizaciones, especialmente cuando no existen controles o auditorías periódicas de seguridad (Fortinet, 2025).

Gestión de Riesgos en Ciberseguridad

La gestión de riesgos es un proceso sistemático que permite identificar, analizar y evaluar los riesgos para tomar decisiones orientadas a su tratamiento. Este proceso incluye la identificación de activos, amenazas y vulnerabilidades, así como la evaluación del impacto y probabilidad (IDB, 2022).

Este enfoque es fundamental en el diseño de modelos de ciberseguridad, ya que permite priorizar los controles en función del nivel de riesgo.

Redes de Comunicación

Las redes de comunicación permiten la interconexión de sistemas dentro y fuera de la organización. En este contexto, las redes perimetrales actúan como una barrera de seguridad entre la red interna y redes externas como Internet.

La seguridad perimetral incluye mecanismos como firewalls, sistemas de detección de intrusos, segmentación de redes y control de accesos, los cuales ayudan a prevenir accesos no autorizados (IBM, Seguridad de la Red, 2025)

Control de Acceso y Autenticación

Consiste en restringir el acceso a los sistemas a usuarios autorizados, incluye gestión de usuarios, políticas de contraseñas, autenticación y autorización.

Una adecuada gestión de accesos puede reducir significativamente los riesgos de seguridad y es considerada una de las medidas más efectivas dentro de la protección de la información (Mendizábal, 2018).

Activos de información y gestión de riesgos

Los activos de información comprenden todos los recursos que poseen valor para la organización, como bases de datos, sistemas, redes, software, documentos o conocimientos internos. La correcta gestión de estos activos implica identificar las amenazas que los afectan y establecer controles de seguridad adecuados. para lograr esta protección de los activos se debe establecer y mejorar

un SGSI, el cual puede desarrollarse según el enfoque de los lineamientos de la norma ISO 27001

Modelos de Ciberseguridad

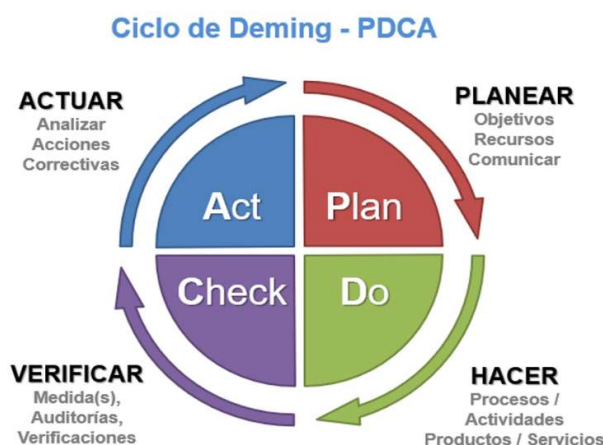
Un modelo de ciberseguridad es una estructura metodológica que integra políticas, controles, procedimientos y buenas prácticas con el fin de proteger la infraestructura tecnológica de una organización (Caballero, 2022)

Estos modelos permiten orientar a identificar riesgos, establecer controles y fortalecer la continuidad del negocio.

Estándares y Marcos de Referencia en Ciberseguridad

1.- Norma ISO 27001 – Sistema de Gestión de Seguridad de la Información

La ISO 27001 es la norma internacional que establece los requisitos para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Su objetivo es proporcionar un marco metodológico para identificar los riesgos y aplicar controles de seguridad adecuados a las necesidades de la organización (NQA, 2022). Esta norma se basa en el enfoque PDCA (Planificar, Hacer, Verificar y Actuar), ciclo que promueve la mejora continua y permite garantizar la eficacia del SGSI.



Gráfica 2 Estructura PDCA-ISO 27001

Planificar (Plan): Establecer políticas, objetivos y procesos de seguridad de la información basados en la gestión de riesgos.

Hacer (Do): Implementar y operar los controles de seguridad definidos.

Verificar (Check): Monitorear y evaluar el desempeño del sistema de seguridad.

Actuar (Act): Aplicar acciones correctivas y de mejora continua.

Componentes del Sistema de Gestión de Seguridad de la Información (SGSI)

El SGSI propuesto por la ISO 27001 está compuesto por diversos elementos claves que son:

- Política de seguridad de la información
- Gestión de riesgos
- Controles de seguridad
- Gestión de incidentes
- Auditorías internas
- Mejora continua

Estos componentes permiten establecer un marco organizacional estructurado para la protección de la información.

Controles de Seguridad (Anexo A)

La norma incluye un conjunto de controles organizados en dominios (Anexo A), los cuales sirven como referencia para la protección de la información.

En la versión actual, estos controles están agrupados en categorías como:

- Controles organizacionales
- Controles de personas
- Controles físicos
- Controles tecnológicos

Estos controles abordan aspectos como control de accesos, criptografía, seguridad en redes, gestión de activos, respaldo de información y protección contra malware (UNE-ISO, 2023)

Gestión de Riesgos en ISO 27001

La norma ISO 27001 permite a las empresas definir ampliamente sus propios procesos de gestión de riesgos. Los métodos comunes analizan todos los riesgos para activos o riesgos presentados en escenarios específicos. Existen cinco aspectos importantes de una evaluación de riesgos ISO 27001 (UNE-ISO, 2023) que son:

- Identificación de activos de información
- Identificación de amenazas y vulnerabilidades
- Evaluación del impacto y probabilidad
- Determinación del nivel de riesgo
- Selección de controles para su tratamiento

Este proceso permite priorizar los esfuerzos de seguridad en función del nivel de exposición al riesgo (UNE-ISO, 2023).

Importancia y fundamentos de ISO 27001:2022

Comprender cómo se interrelacionan los procesos y producen resultados puede ayudarle a identificar oportunidades de mejora y optimizar el rendimiento global. Esto también es aplicable cuando los procesos, o parte de ellos, se externalizan. Comprender cómo afecta o podría afectar esto al resultado, y comunicarlo claramente a la empresa que presta el servicio externalizado, garantiza la claridad y la responsabilidad en el proceso (NQA, 2022).

El último paso del proceso consiste en revisar el resultado de la auditoría y asegurarse de que la información obtenida se utiliza correctamente. Una revisión formal de la gestión es la oportunidad de reflexionar sobre el rendimiento del SGSI y de tomar decisiones sobre cómo y dónde mejorar

Sector salud y adaptaciones normativas en Ecuador

El sector salud en Ecuador ha sido foco de adaptaciones del estándar ISO 27001 para cumplir con exigencias específicas del manejo de datos clínicos. se aplica un modelo adaptado para asegurar la confidencialidad, integridad y disponibilidad de los historiales clínicos digitales, evaluando antes y después de la implementación para determinar mejoras reales. Asimismo, un proyecto local en hospital público analizó la metodología practicable para implantar un SGSI (Cuadra, 2023) basado en ISO 27001 en áreas administrativas y de atención, lo que permite aprender sobre la aplicación práctica y los ajustes requeridos según el contexto ecuatoriano.

Normativas aplicables:

- Ley Orgánica de Protección de Datos Personales (Ecuador)
- Ley de Comercio Electrónico, Firmas y Mensajes de Datos
- Normativa sectorial farmacéutica (BPM/GMP)
- ISO 27001: Seguridad de la información
- Lineamientos CIS Controls

2.- Norma ISO/IEC 27002

La ISO/IEC 27002:2022 proporciona directrices para la selección e implementación de controles de seguridad de la información. Sus controles se organizan en cuatro categorías principales: controles organizacionales, controles de personas, controles físicos y controles tecnológicos. Esta estructura permite orientar la selección de controles de acuerdo con las necesidades de la organización y complementa los requisitos establecidos por ISO/IEC 27001:2022.

En el presente estudio, la ISO/IEC 27002:2022 se utiliza como referencia complementaria para identificar controles aplicables al modelo de ciberseguridad propuesto, especialmente en aspectos relacionados con gestión de activos, control de accesos, respaldo de información, monitoreo, gestión de incidentes y continuidad operativa.

Desde una perspectiva general, la aplicación de buenas prácticas asociadas a ISO 27002 contribuye a mejorar el control de los activos, identificar puntos débiles, fortalecer procesos de seguridad, aumentar la confianza de clientes y proveedores, apoyar la eficiencia organizacional y reducción de costos (School, 2022).

3.- NIST Cybersecurity Framework (NIST CSF)

El NIST Cybersecurity Framework (CSF) es un marco de referencia desarrollado por el National Institute of Standards and Technology que proporciona un conjunto de lineamientos, buenas prácticas y estándares orientados a la gestión del riesgo en ciberseguridad. Su objetivo principal es ayudar a las organizaciones a identificar, proteger, detectar, responder y recuperarse de incidentes de seguridad de la información (NIST, 2018).

Las categorías y subcategorías proporcionan planes de acción más concretos para departamentos o procesos específicos dentro de una organización. Se basa en cinco funciones claves que son las siguientes:

Identificar: para protegerse contra los ataques cibernéticos, el equipo de ciberseguridad necesita una comprensión profunda de los activos y recursos más importantes de la organización. La función de identificación incluye categorías, como gestión de activos, entorno empresarial, gobernanza, evaluación de riesgos, estrategia de gestión de riesgos y gestión de riesgos de la cadena de suministro.

Proteger: la función de protección cubre gran parte de los controles de seguridad técnica y física para desarrollar e implementar salvaguardas adecuadas y proteger la infraestructura crítica. Estas categorías son gestión de identidad y control de acceso, concientización y capacitación, seguridad de datos, procesos y procedimientos de protección de la información, mantenimiento y tecnología de protección.

Detectar: la función de detección implementa medidas que alertan a una organización sobre ataques cibernéticos. Las categorías incluyen anomalías y eventos, seguridad, monitoreo continuo y procesos de detección.

Responder: Las categorías de funciones de respuesta garantizan la respuesta adecuada a los ciberataques y otros eventos de ciberseguridad. Categorías específicas incluyen planificación de respuesta, comunicaciones, análisis, mitigación y mejoras.

Recuperación: las actividades de recuperación implementan planes de resiliencia cibernética y garantizan la continuidad de negocio en caso de vulnerabilidades como un ataque cibernético, una violación de seguridad u otro evento de ciberseguridad. Las funciones de recuperación son mejoras en la planeación de la recuperación y comunicaciones.

Las referencias informativas del CSF del NIST establecen una correlación directa entre las funciones, categorías, subcategorías y los controles de seguridad específicos de otros marcos. El NIST es uno de los marcos más utilizados en el sector corporativo por su enfoque práctico, adaptable al ciclo completo de ciberseguridad. (IBM, Marco de ciberseguridad del NIST, 2025)

Enfoque basado en la gestión de riesgos

El NIST CSF (IBM, Marco de ciberseguridad del NIST, 2025) se fundamenta en un enfoque que permite a las organizaciones priorizar sus esfuerzos de seguridad en función de:

- Probabilidad de ocurrencia
- Impacto del incidente
- Valor de los activos

Este enfoque es coherente con otros estándares como ISO 27001 (Cuadra, 2023), facilitando su integración en modelos de ciberseguridad (NIST, 2018).

Importancia de NIST CSF en las organizaciones

La adopción del NIST CSF (CIS, 2021) proporciona múltiples beneficios:

- Mejora la gestión de riesgos de ciberseguridad
- Facilita la identificación de vulnerabilidades
- Fortalece la capacidad de respuesta ante incidentes
- Permite evaluar el nivel de madurez organizacional
- Es adaptable a diferentes contextos empresariales

Es importante destacar que el uso del NIST CSF (NIST, 2018) en este proyecto se limita al diseño metodológico del modelo, sin contemplar su implementación práctica dentro de la organización.

3.- CIS Controls

Los Controles Críticos de Seguridad CIS (Controles CIS) son un conjunto prescriptivo, priorizado y simplificado de mejores prácticas que puede utilizar para fortalecer su estrategia de ciberseguridad. Hoy en día, miles de profesionales de la ciberseguridad de todo el mundo utilizan los Controles CIS o contribuyen a su desarrollo mediante un proceso de consenso comunitario. (CIS, 2021).

Estos controles se caracterizan por ser prácticos, accionables y basados en experiencias reales de ataques, lo que los convierte en una guía efectiva para fortalecer la seguridad de la información, especialmente en organizaciones que requieren un enfoque estructurado pero adaptable.

los controles de CIS han sido desarrollados y perfeccionados por una comunidad internacional de personas e instituciones que:

- Comparten información sobre ataques y atacantes, identificar causas raíz y traducir eso en tipos de acciones defensivas.

- Documentan historias de adopción y compartir herramientas para resolver problemas.
- Comparten herramientas, ayudas de trabajo y traducciones.
- Identifican problemas comunes (como la evaluación inicial y los mapas de ruta de implementación) y resolverlos como una comunidad.

Estas actividades aseguran que los Controles CIS no son solo otra lista de buenas prácticas, sino un conjunto de acciones priorizadas y altamente focalizadas que tienen una red de soporte comunitario para hacerlas implementables, utilizables, escalables y compatibles con todos los requerimientos de seguridad gubernamental o industrial. El verdadero poder de los Controles CIS no se trata de crear la mejor lista de cosas para hacer, sino de aprovechar la experiencia de una comunidad de personas y empresas para realizar mejoras de seguridad mediante el intercambio de ideas y la acción colectiva.

Estructura de los CIS Controls V8

En su versión más reciente (CIS Controls v8), el marco está compuesto por 18 controles, organizados en tres categorías de implementación:

- **IG1 (Implementation Group 1)**

Controles básicos de ciberseguridad para organizaciones con recursos limitados.

- **IG2 (Implementation Group 2)**

Controles intermedios para organizaciones con mayor capacidad tecnológica.

- **IG3 (Implementation Group 3)**

Controles avanzados para organizaciones con alta madurez en ciberseguridad.

Los Controles CIS se seleccionan, descartan y priorizan en función de los datos, y del conocimiento específico del comportamiento del atacante y cómo detenerlo (Constrols, 2021), proporciona controles priorizados y altamente prácticos para disminuir la superficie de ataque de las cuales son los siguientes:

CIS Control 01 Inventario y Control de los Activos Empresariales

CIS Control 02 Inventario y Control de Activos de Software

CIS Control 03 Protección de los Datos

CIS Control 04 Configuración Segura de Activos y Software

CIS Control 05 Administración de Cuentas

CIS Control 06 Gestión de Control de Accesos

CIS Control 07 Gestión Continua de Vulnerabilidades

CIS Control 08 Gestión de Registros de Auditoría

CIS Control 09 Protección del Correo Electrónico y Navegador Web

CIS Control 10 Defensas contra Malware

CIS Control 11 Recuperación de Datos

CIS Control 12 Gestión de la Infraestructura de Red

CIS Control 13 Monitoreo y Defensa de la red

CIS Control 14 Concientización en Seguridad y Formación de Habilidades

CIS Control 15 Gestión de Proveedores de Servicios

CIS Control 16 Seguridad en el Software de Aplicación

CIS Control 17 Gestión de Respuesta a Incidentes

CIS Control 18 Pruebas de Penetración

Su enfoque práctico permite adaptar el modelo a la realidad de la empresa GLOBESER S.A.S., considerando sus limitaciones tecnológicas y organizacionales (CIS, 2021).

Importancia de CIS Controls en las organizaciones

La aplicación de los CIS Controls proporciona múltiples beneficios:

- Priorización de controles según nivel de riesgo
- Reducción efectiva de vulnerabilidades
- Fácil implementación conceptual
- Enfoque práctico y aplicable
- Complemento de estándares internacionales

Diversos estudios indican que la adopción de estos controles puede mitigar una gran parte de los ataques más comunes en ciberseguridad en cualquier organización. (CIS, 2021).

2.2 METODOLOGÍA DEL PROYECTO

El Núcleo del negocio se centra en la comercialización de productos farmacéuticos y de consumo, con un enfoque en la salud y el bienestar de la comunidad en la provincia de Santa Elena. Además, la empresa GLOBESER S.A.S., comprende 15 farmacias Cruz Azul, y es franquicia del Grupo Difare S.A. que es líder en la distribución farmacéutica en Ecuador y también se dedica a la gestión de farmacias, con un fuerte compromiso con la sostenibilidad y el desarrollo social.

La organización opera mediante farmacias Cruz Azul y el área administrativa. La infraestructura se encuentra centralizada en la oficina matriz, donde se dispone de tres estaciones de uso administrativo. En el departamento de sistemas se dispone de un servidor central de base de datos, el cual cumple funciones de hosting, así como dos estaciones destinadas a monitoreo y soporte técnico. A nivel de cada farmacia se dispone de un servidor replicador de base de datos, estaciones para facturación, sistemas de video vigilancia y servicios de telefonía IP. La red de la infraestructura opera a través del proveedor Telconet. En la parte de software trabajan con un sistema de facturación denominado Neptuno, correo electrónico y control de asistencias.

2.2.1 DISEÑO Y ALCANCE DE LA INVESTIGACIÓN

El método de investigación se enmarca en un diseño de carácter no experimental y alcance de tipo descriptivo–propositivo, orientado al análisis de referentes normativos y al diseño de un modelo de ciberseguridad, sin intervención práctica en la organización.

.

2.2.2 METODOLOGÍA DE INVESTIGACIÓN

La presente investigación se desarrolla bajo un enfoque documental y técnico, se sustenta en la revisión, análisis e interpretación de fuentes documentales, técnicas y normativas. No se consideran pruebas de campo, levantamiento empírico ni aplicación de instrumentos sobre personal o infraestructura. Los Instrumentos incorporados en anexos se presentan con carácter referencial como parte del entregable del componente práctico, sin aplicación a participantes en el marco de este estudio.

El enfoque documental se fundamenta en la revisión sistemática, el análisis crítico y la interpretación de fuentes secundarias especializadas, tales como estándares, marcos de referencia y buenas prácticas en ciberseguridad, seleccionando aquellos que mejor se alinean al contexto del estudio. Este proceso se orienta a la identificación de lineamientos, controles y estructuras metodológicas que constituyen como base para el diseño del modelo de ciberseguridad propuesto.

Por su parte, el enfoque técnico se orienta al análisis conceptual y estructurado de la seguridad de la infraestructura tecnológica, considerando criterios referenciales para la identificación de activos de información, amenazas, y riesgos desde una perspectiva teórica y referencial, sin la ejecución de pruebas o intervenciones directas sobre la organización.

2.2.3 TIPO Y MÉTODOS DE INVESTIGACIÓN

Tipo de investigación: diseño propositivo, de naturaleza documental, técnica y normativa. El estudio no incorpora medición estadística, encuestas, entrevistas aplicadas ni tabulación de datos.

Métodos de investigación: Inductivo, Deductivo, Analítico y Sintético

Inductivo: Se fundamenta en el análisis de estándares y buenas prácticas específicas en ciberseguridad para generar una propuesta general adaptada al contexto de la empresa.

Deductivo: Fundamenta la aplicación de principios y lineamientos normativos generales de ciberseguridad tales como ISO 27001, el NIST y los CIS Controls para el diseño del modelo propuesto.

Analítico: Facilita la descomposición de los marcos de referencia en sus componentes esenciales, como controles y procesos.

Sintético: Se orienta a la integración de elementos analizados en una estructura coherente que da forma al modelo de ciberseguridad.

Población y muestra

No aplica. Dado que el estudio es de carácter documental, técnico y propositivo, no se define población ni muestra, ya que no se contempla levantamiento empírico.

2.2.4 TÉCNICAS DE ANÁLISIS DOCUMENTAL Y NORMATIVO

Técnicas e instrumentos de apoyo metodológico

- Guía de entrevista semiestructurada propuesta como anexo metodológico de validación institucional.
- Análisis documental de estándares.
- Análisis normativo comparativo.
- Análisis documental de referencia sobre la infraestructura tecnológica.
- Matriz referencial de análisis y valoración conceptual de riesgos.
- Valoración técnica referencial del modelo propuesto.

INSTRUMENTOS PROPUESTOS

1.- **Entrevista.** - Guía de entrevista semiestructurada incorporada como anexo metodológico de apoyo a la validación del modelo.

Instrumento propuesto:

- Guía de entrevistas semiestructuradas. (ANEXO 1)

2.- **Análisis documental de estándares.** – Es una técnica de apoyo basada en la revisión sistemática de fuentes secundarias, tales como estándares, marcos de referencia, y documentación técnica en ciberseguridad. Se orienta al análisis referencial de lineamientos, controles y buenas prácticas aplicables al diseño del modelo.

Instrumento propuesto:

- Matriz de análisis documental de estándares (ANEXO 2)

3.- **Análisis normativo comparativo.** – Técnica orientada a la comparación estructurada de estándares internacionales. Permite el

análisis para seleccionar y adaptar los elementos más relevantes de cada marco para integrarlos en el modelo propuesto.

Instrumento propuesto:

- Matriz comparativa de estándares de ciberseguridad

Criterio	ISO 27001	ISO 27002:2022	NIST Cybersecurity Framework (CSF)	CIS Controls
Tipo de estándar	Norma internacional certificable	Guía de buenas prácticas	Marco de referencia	Buenas prácticas
Enfoque principal	Gestión de la seguridad de la información (SGSI)	Controles y directrices de seguridad de la información	Gestión de riesgos de ciberseguridad	Controles técnicos de seguridad
Nivel de aplicación	Estratégico y organizacional	Táctico y operativo	Táctico y estratégico	Operativo y técnico
Estructura	Cláusulas + Anexo A (controles)	14 dominios y 93 controles	Funciones: Identificar, proteger, detectar, responder, recuperar	18 controles priorizados
Gestión de riesgos	Basada en evaluación formal de riesgos	Orientada al tratamiento de riesgos	Basada en identificación y gestión continua de riesgos	Enfoque implícito mediante controles
Controles de seguridad	Amplios y estructurados	Detallados y orientados a la práctica	Definidos por categorías y subcategorías	Específicos, técnicos y priorizados
Flexibilidad	Moderada	Alta	Alta	Alta
Certificación	Sí	No	No	No
Facilidad de implementación	Compleja	Moderada	Moderada	Alta
Enfoque organizacional	Alto	Alto	Medio	Bajo
Enfoque técnico	Medio	Medio	Medio	Alto
Cobertura	Integral (procesos, personas y tecnología)	Integral (controles específicos por dominio)	Integral (enfoque de gestión)	Específica (tecnología y controles)
Ventajas	Estándar reconocido y estructurado	Guía práctica y detallada	Flexible y adaptable	Práctico y fácil de aplicar
Limitaciones	Requiere recursos y tiempo	No certificable	No certificable	No cubre gestión completa
Aporte al modelo	Base del sistema de gestión	Guía para la implementación de controles	Estructura funcional del modelo	Implementación de controles técnicos
Nivel de pertinencia	Alto	Alto	Alto	Alto

Tabla 1. Matriz comparativa de estándares de ciberseguridad

4.-Análisis documental referencial de la infraestructura tecnológica. – Técnica propuesta como apoyo metodológico para la caracterización estructural del entorno tecnológico, basado en información referencial en activos, que comprende la identificación de

componentes críticos, clasificación final, valoración en confidencialidad, integridad y disponibilidad, sin intervención directa en los sistemas.

Instrumento propuesto:

- Modelo de Matriz referencial de inventario de Activos ISO 27001 (ANEXO 3)
- Matriz de nivel de Madurez (ANEXO 4)

5.-Matriz referencial de análisis y valoración conceptual de riesgos.

- Utilizada como técnica de apoyo para estructurar el modelo propuesto, sin aplicación técnica en campo.

Instrumento propuesto:

- Matriz referencial de datos conceptuales de análisis de riesgo, tratamiento de riesgos y controles de seguridad informática ISO 27001 (ANEXO 5).

6.- Valoración técnica referencial del modelo propuesto. – Esta técnica consiste en el análisis y valoración conceptual de los controles referenciales basados en marcos, estándares y buenas prácticas como ISO 27001, el NIST Cybersecurity Framework (CSF) y los CIS Controls, orientado a la valoración conceptualmente su coherencia, pertinencia y alineación con los principios de confidencialidad, integridad y disponibilidad con base en las necesidades de la empresa.

Instrumento propuesto:

- Matriz de lista de verificación de cumplimiento de datos conceptuales, se adjunta en la siguiente tabla

Ítem	Control / Criterio	Descripción	Estándar de referencia	Cumple (✓)	No cumple(X)	Observaciones
1	Inventario de activos	Existe un inventario actualizado de equipos	ISO/IEC 27002:2022 5.9 / CIS 1			
2	Inventario de software	Registro de aplicaciones instaladas	CIS 2			
3	Control de accesos	Gestión de usuarios y permisos	ISO/IEC 27002:2022 5.15–5.18 / CIS 5–6			
4	Protección de datos	Clasificación y protección de información	ISO/IEC 27002:2022 5.12–5.13, 8.11–8.12 / CIS 3			
5	Seguridad de red	Uso de firewall y segmentación	ISO/IEC 27002:2022 8.20–8.22 / CIS 12–13			
6	Gestión de vulnerabilidades	Evaluación de vulnerabilidades	ISO/IEC 27002:2022 8.8 / CIS 7			
7	Monitoreo de eventos	Registro de logs y monitoreo	ISO/IEC 27002:2022 8.15–8.16 / CIS 8			
8	Detección de intrusos	Uso de IDS/IPS	ISO/IEC 27002:2022 8.16, 8.20 / CIS 13			
9	Respuesta a incidentes	Existe plan de respuesta	ISO/IEC 27002:2022 5.24–5.28 / CIS 17			
10	Copias de seguridad	Backups periódicos	ISO/IEC 27002:2022 8.13 / CIS 11			
11	Capacitación	Formación en seguridad	ISO/IEC 27002:2022 6.3 / CIS 14			
12	Gestión de proveedores	Control de terceros	ISO/IEC 27002:2022 5.19–5.22 / CIS 15			
13	Gestión de riesgos	Proceso de evaluación de riesgos	ISO/IEC 27001:2022 Cláusula 6			
14	Política de seguridad	Existe política de seguridad documentada	ISO/IEC 27001:2022 Cláusula 5			
15	Recursos	Asignación de recursos de seguridad	ISO/IEC 27001:2022 Cláusula 7			
16	Auditoría interna	Auditorías periódicas	ISO/IEC 27001:2022 Cláusula 9			
17	Gestión de incidentes	Respuesta a incidentes	ISO/IEC 27002:2022 5.24–5.28 / CIS 17			
18	Continuidad del negocio	Planes de recuperación	ISO/IEC 27002:2022 5.29–5.30 / CIS 11			

Tabla 2 Checklist de verificación

CAPÍTULO 3

3. PROPUESTA

3.1 TEMA DE LA PROPUESTA

Modelo de ciberseguridad basado en ISO 27001 y CIS CONTROLS para la infraestructura tecnológica de la empresa farmacéutica GLOBESER S.A.S.

3.2 OBJETIVO

Diseñar un modelo de ciberseguridad basado en ISO 27001 y CIS Controls, orientado a fortalecer la protección de la infraestructura tecnológica de GLOBESER S.A.S., bajo los principios de confidencialidad, integridad y disponibilidad de la información.

3.3 ANÁLISIS DOCUMENTAL Y TÉCNICO REFERENCIAL PARA EL DISEÑO DEL MODELO

El análisis documental, técnico y normativo, se establece como base referencial para el diseño del modelo de ciberseguridad propuesto.

Este proceso se fundamenta considerando un informe técnico elaborado por el departamento de TI y en base a las técnicas de apoyo metodológico propuesto como el análisis documental de estándares, análisis normativo comparativo, Análisis documental de referencia sobre la infraestructura tecnológica, matriz referencial de análisis y valoración conceptual de riesgos y validación técnica referencial. Sus instrumentos propuestos como la Matriz referencial de análisis documental de estándares, matriz comparativa de estándares de ciberseguridad, la matriz referencial de inventario de activos, Matriz referencial de análisis y valoración conceptual de riesgos y la matriz de lista de verificación de cumplimiento de datos conceptuales, sin la ejecución de pruebas técnicas ni intervención directa sobre los sistemas de la organización.

El análisis documental y técnico evidencia de manera referencial un nivel reducido de madurez en ciberseguridad dentro de la organización, caracterizado

por la presencia de controles básicos y una limitada cultura organizacional, el análisis permite deducir que los activos de información se encuentran expuestos a posibles vulnerabilidades, lo que incrementa la exposición a amenazas y riesgos que pueden comprometer la confidencialidad, integridad y disponibilidad de la información. En este contexto, se adopta la norma ISO 27001 como base para la gestión estructurada de la seguridad de la información, orientado al establecimiento de un Sistema de Gestión de Seguridad de la Información (SGSI). Complementariamente, se incorporan los CIS Controls como guía de controles técnicos priorizados, destinados a mitigar riesgos de manera práctica y efectiva.

Se fundamenta la pertinencia institucional del modelo de ciberseguridad, estructurado en estándares reconocidos como ISO 27001 y CIS Controls, orientado al fortalecimiento de la gestión de la seguridad de la información. Cabe destacar que la presente propuesta se limita al diseño del modelo, sin considerar su implementación.

3.3.1 Análisis normativo comparativo ISO 27001, NIST CSF y CIS Controls

El análisis establece como resultado en base a las técnicas propuestas como la matriz comparativa de estándares de ciberseguridad y la lista de verificación de cumplimiento, que se justifica la selección de ISO 27001 como base del modelo, debido a su capacidad para establecer un sistema formal de gestión de la seguridad de la información, complementado por los CIS Controls, que proporcionan lineamientos técnicos específicos, priorizados y aplicables para la protección de la infraestructura tecnológica. Por su parte, el NIST CSF no se adopta como estándar principal y solo se considera como complemento estructural, la técnica de apoyo metodológico fundamentada en la checklist de verificación de cumplimiento, establece de manera referencial que varios de los controles evaluados son abordados de manera más específica y efectiva mediante los CIS Controls, lo que refuerza su pertinencia como complemento técnico dentro del modelo propuesto.

3.3.2 Identificación de activos de información

Con base en la información disponible y en el análisis documental realizado, se establece de manera referencial los principales activos tecnológicos vinculados al contexto organizacional:

- Servidor central de base de datos
- Servidores replicadores en cada farmacia
- Estaciones de trabajo administrativas y operativas
- Sistema de facturación (Neptuno)
- Red de comunicación corporativa
- Sistemas de videovigilancia
- Servicios de correo electrónico
- Sistema de Marcaciones (Only Control)

Estos activos representan elementos críticos para la operación del negocio, ya que soportan procesos esenciales como la facturación, gestión de inventarios y atención al cliente.

3.3.3 Identificación de vulnerabilidades

A partir del análisis técnico referencial, se consideran como posibles vulnerabilidades relevantes las siguientes:

- Ausencia de firewall perimetral
- Uso de antivirus inactivos o desactualizados
- Contraseñas débiles y compartidas
- Equipos con sistemas operativos obsoletos
- Hardware obsoleto
- Falta de control de accesos físicos y lógicos
- Ausencia de políticas formales de seguridad
- Deficiencia en la capacitación del personal

Estas vulnerabilidades pueden evidenciar una limitada gestión de la seguridad de la información dentro de la organización.

3.3.4 Identificación de amenazas

En función del análisis documental y técnico desarrollado, se establecen como amenazas potenciales las siguientes:

- Ataques de malware y ransomware
- Accesos no autorizados
- Pérdida o fuga de información
- Errores humanos
- Fallas en los sistemas o interrupciones del servicio
- Uso indebido de credenciales

Estas amenazas pueden representar riesgos significativos para la continuidad del negocio.

3.3.5 Análisis de riesgos

El análisis de riesgos se desarrolla de manera conceptual y referencial, considerando la relación entre activos, amenazas y vulnerabilidades como base para el diseño del modelo, los principales riesgos se asocian a:

- Compromiso de la confidencialidad de datos sensibles
- Alteración de información crítica (integridad)
- Interrupción de servicios tecnológicos (disponibilidad)

Se establece de manera referencial un nivel de riesgo alto, debido a la ausencia de controles de seguridad estructurados y a la exposición constante a amenazas internas y externas.

3.3.6 Brechas frente a estándares de ciberseguridad

A partir del análisis documental, técnico y normativo, se identifica la presencia de brechas en relación con estándares bajo ISO 27001 y CIS Controls, entre las cuales se destacan:

- Inexistencia de un Sistema de Gestión de Seguridad de la Información (SGSI)
- Falta de inventario formal de activos

- Ausencia de gestión estructurada de riesgos
- Deficiencia en controles de acceso
- Falta de monitoreo y registro de eventos
- Ausencia de políticas y procedimientos documentados

Estas posibles brechas justifican la necesidad de diseñar el modelo de ciberseguridad orientado a establecer lineamientos y controles adecuados.

3.4 CRONOGRAMA

FASE	ACTIVIDAD	SEMANAS	PRODUCTO
1	Análisis documental y técnico referencial	1-2	-Análisis referencial del estado de ciberseguridad, -Identificación de activos de información, -Detección de vulnerabilidades, amenazas y riesgos, - Revisión del nivel de madurez.
2	Fundamentación Teórica	2-3	-Análisis de estándares como ISO 27001, -Revisión de CIS Controls -Identificación de buenas prácticas en ciberseguridad.
3	Diseño del Modelo	3-4	-Gobierno -Activos -Riesgos -Controles y capacitación - Integración bajo mejora continua
4	Validación Teórica	5-6	-Revisión del modelo frente a estándares. -Revisión referencial de consistencia metodológica y técnica del modelo (si aplica validación por expertos) -Comparación con buenas prácticas
5	Propuesta y Documentación	7-8	-Definición de lineamientos de uso -Informe Final

Tabla 3 Cronograma de Actividades

3.5 DISEÑO DEL MODELO DE CIBERSEGURIDAD

El modelo de ciberseguridad propuesto se fundamenta en la integración de la norma ISO 27001 y los CIS Controls, con el propósito de diseñar una estructura metodológica orientada a la gestión de la seguridad de la información para la empresa.

El diseño del modelo no contempla su implementación, permitiendo definir lineamientos, políticas y controles que contribuyan a fortalecer la protección de la infraestructura tecnológica.

El modelo se orienta conceptualmente a la identificación de los activos de información, la evaluación de los riesgos asociados a la infraestructura tecnológica y la definición de controles de seguridad para proteger los sistemas informáticos de la organización.

3.6 ESTRUCTURA DEL MODELO DE CIBERSEGURIDAD

El modelo propuesto se estructura en cinco componentes: gobierno, activos, riesgos, controles y capacitación, alineados a ISO 27001 para la gestión y a CIS Controls para la aplicación técnica, integrados bajo un ciclo de mejora continua, los cuales se muestran en la siguiente gráfica.



Gráfica 3 Estructura del Modelo de Ciberseguridad

Técnicas propuestas:

- 1.-Modelo de Matriz referencial de inventario de Activos ISO 27001 (ANEXO 3)
- 2.- Matriz de análisis documental de estándares
- 3.-Matriz de nivel de Madurez (ANEXO 4)
- 4.- Matriz referencial de datos conceptuales de análisis de riesgo, tratamiento de riesgos y controles de seguridad informática ISO 27001 (ANEXO 5)
- 5.- Matriz de lista de verificación de cumplimiento de datos conceptuales

3.7 MATRIZ DE TRAZABILIDAD DEL MODELO

Con el propósito de evidenciar la integración normativa del modelo propuesto, se incorpora una matriz de trazabilidad que vincula los componentes del modelo (gobierno, activos, riesgos, controles y capacitación) con las cláusulas de ISO/IEC 27001, los controles de ISO/IEC 27002 y los CIS Controls v8. Esta matriz se presenta como soporte documental del diseño, sin implicar implementación operativa. La matriz se presenta a continuación:

COMPONENTE DEL MODELO	ELEMENTO DEL MODELO	ISO/IEC 27001:2022 (CLÁUSULA)	ISO/IEC 27002:2022 (CONTROL)	CIS CONTROLS v8	ENTREGABLE / EVIDENCIA (DOCUMENTAL)
GOBIERNO	Política de seguridad de la información	Cl. 5 (Liderazgo) / Cl. 6 (Planificación)	5.1 Políticas de seguridad de la información	CIS 17 (Concienciación en Seguridad y Capacitación en Habilidades) (complementa cultura) / CIS 18 (Gestión de Proveedores de Servicios) (gobernanza con terceros)	Política de SI (plantilla), roles y responsabilidades, lineamientos
ACTIVOS	Inventario y clasificación de activos	Cl. 8 (Operación)	5.9 Inventario de información y otros activos asociados / 5.12 Clasificación de la información	CIS 1 (Inventario y control de activos empresariales), CIS 2 (Activos de software)	Matriz inventario de activos (ANEXO), criterio de criticidad CIA
RIESGOS	Metodología de valoración de riesgos	Cl. 6.1 (Acciones para abordar riesgos y oportunidades)	5.4 Responsabilidades de la dirección / 5.7 Inteligencia de amenazas (si aplica)	CIS 7 (Gestión Continua de Vulnerabilidades) (apoya riesgo técnico)	Matriz referencial de riesgos (activo-amenaza-vulnerabilidad-impacto-prob.)
CONTROLES	Control de accesos / cuentas	Cl. 8 (Operación)	5.15 Control de acceso / 5.16 Gestión de identidades / 5.17 Información de autenticación / 5.18 Derechos de acceso	CIS 5 (Gestión de cuentas), CIS 6 (Gestión de control de acceso)	Checklist de controles, lineamientos de contraseñas, matriz de permisos
CONTROLES	Copias de seguridad y recuperación	Cl. 8 (Operación)	8.13 Copia de seguridad de la información	CIS 11 (Recuperación de datos)	Política de copias de seguridad (referencial), periodicidad sugerida, responsables
CONTROLES	Registro y monitoreo	Cl. 9 (Evaluación del desempeño)	8.15 Registro / 8.16 Actividades de monitoreo	CIS 8 (Gestión de registros de auditoría)	Lineamientos de registros, lista mínima de eventos, plan de revisión
CAPACITACIÓN	Programa de concienciación	Cl. 7 (Soporte)	6.3 Concienciación, educación y formación en seguridad de la información	CIS 14 (Concienciación sobre seguridad y capacitación en habilidades)	Plan de capacitación (temas, frecuencia, evidencia documental)

Tabla 4 Trazabilidad del Modelo

3.8 INDICADORES PROPUESTOS (KPIs) PARA SEGUIMIENTO

Como parte del diseño metodológico del modelo, se proponen indicadores de desempeño (KPIs) orientados a evaluar su adopción institucional. Los indicadores se definen de forma operacional mediante fórmula de cálculo, periodicidad y meta referencial, con finalidad de seguimiento conceptual del modelo, sin medición empírica dentro del presente estudio. La tabla se muestra a continuación:

COMPONENTE	KPI PROPUESTO	DEFINICIÓN OPERATIVA	FÓRMULA / CÓMO SE CALCULA	FRECUENCIA SUGERIDA	META REFERENCIAL
ACTIVOS	% activos inventariados	Porcentaje de activos registrados vs activos identificados	$(\text{Activos en inventario} / \text{Activos totales}) * 100$	Mensual	$\geq 95\%$
RIESGOS	% riesgos con tratamiento definido	Riesgos priorizados que tienen acción/control asociado	$(\text{Riesgos con tratamiento} / \text{Riesgos totales}) * 100$	Trimestral	$\geq 90\%$
CONTROLES	% cumplimiento checklist	Nivel de cumplimiento de controles del checklist referencial	$(\text{Ítems "cumple"} / \text{Total ítems}) * 100$	Trimestral	$\geq 80\%$
CONTROLES	Tiempo de respuesta a incidentes (MTTR)	Tiempo promedio desde detección hasta contención/cierre	Promedio (hora cierre – hora detección)	Mensual	↓ tendencia
CONTROLES	% equipos con parches al día	Equipos con SO y apps actualizadas	$(\text{Equipos actualizados} / \text{Total equipos}) * 100$	Mensual	$\geq 90\%$
CAPACITACIÓN	% personal capacitado	Personal que ha completado capacitación de seguridad	$(\text{Personal capacitado} / \text{Total personal}) * 100$	Trimestral	$\geq 95\%$
GOBIERNO	% políticas vigentes revisadas	Políticas revisadas/actualizadas en el periodo	$(\text{Políticas revisadas} / \text{Políticas totales}) * 100$	Semestral	100%

Tabla 5 Indicadores Propuestos

3.9 VALIDACIÓN CONCEPTUAL REFERENCIAL DEL MODELO (PROPUESTA)

Se plantea un mecanismo de validación conceptual del modelo por juicio experto, orientado a evaluar coherencia, pertinencia, completitud y alineación normativa. La validación se presenta como procedimiento institucional propuesto, sin aplicación empírica en el presente estudio. El instrumento de apoyo se incorpora como anexo metodológico.

Criterios de validación (rúbrica):

Coherencia: consistencia lógica entre componentes del modelo y sus elementos.

Pertinencia: relevancia de controles y lineamientos respecto al contexto de GLOBESER S.A.S.

Compleitud: cobertura mínima de gobierno, activos, riesgos, controles y capacitación.

Alineación normativa: correspondencia con ISO 27001/27002 y CIS Controls v8.

Claridad: redacción, estructura y facilidad de interpretación.

Criterio de aceptación sugerido:

Promedio $\geq 3.0/4.0$ y sin observaciones críticas en alineación normativa.

La tabla propuesta de validación se muestra a continuación:

CRITERIO	DESCRIPCIÓN	ESCALA (1–4)	EVIDENCIA A REVISAR	OBSERVACIONES DEL EXPERTO
Coherencia	El modelo mantiene consistencia entre componentes y controles	1–4	Diagrama del modelo + Cap. 3.6–3.7	
Pertinencia	El modelo corresponde a necesidades del sector farmacéutico	1–4	Activos/riesgos propuestos + controles	
Compleitud	Cubre mínimo de gobierno, activos, riesgos, controles, capacitación	1–4	Tabla de trazabilidad + checklist	
Alineación normativa	Trazabilidad con ISO 27001/27002 y CIS v8	1–4	Matriz de trazabilidad	
Claridad	Es entendible y aplicable como guía institucional	1–4	Documento completo	

Tabla 6 Propuesta de Validación conceptual

3.10 DEFINICIÓN OPERACIONAL MÍNIMA DE LOS COMPONENTES DEL MODELO

Con el propósito de precisar el funcionamiento metodológico del modelo propuesto, se definen operacionalmente sus componentes, especificando objetivo, entradas, proceso, salidas y responsable referencial. Esta definición se presenta como guía estructural del diseño, sin implicar implementación operativa dentro del presente estudio

COMPONENTE	OBJETIVO	ENTRADAS (INSUMOS)	PROCESO (PASOS MÍNIMOS)	SALIDAS (ENTREGABLES)	RESPONSABLE REFERENCIAL
GOBIERNO	Establecer el marco directivo y normativo de la seguridad de la información.	Requisitos normativos aplicables; estructura organizacional; roles existentes; políticas internas disponibles.	(1) Definir política de seguridad. (2) Asignar roles y responsabilidades. (3) Establecer alcance del modelo. (4) Definir lineamientos de cumplimiento y mejora continua.	Política de seguridad (plantilla); matriz de roles; alcance del modelo; calendario de revisión.	Dirección/gerencia + responsable de TI/seguridad.
ACTIVOS	Identificar y organizar los activos de información y tecnológicos según criticidad (CIA).	Inventario referencial de activos; descripción de sistemas/servicios; ubicación/área; tipo de información asociada.	(1) Listar activos (hardware, software, datos, servicios). (2) Clasificar por criticidad CIA (confidencialidad, integridad, disponibilidad). (3) Priorizar activos críticos.	Matriz de inventario; clasificación CIA; lista priorizada de activos críticos.	TI/soporte técnico + responsable de proceso (farmacias/administración).
RIESGOS	Valorar conceptualmente la exposición al riesgo a partir de activos, amenazas y vulnerabilidades.	Lista de activos críticos; amenazas referenciales; vulnerabilidades referenciales; criterios de impacto/probabilidad.	(1) Relacionar activo–amenaza–vulnerabilidad. (2) Asignar impacto y probabilidad (escala). (3) Estimar nivel de riesgo (matriz). (4) Priorizar riesgos altos.	Matriz referencial de riesgos; mapa de calor (si aplica); lista priorizada de riesgos.	Responsable de TI/seguridad + apoyo directivo.
CONTROLES	Definir controles administrativos y técnicos alineados a ISO 27001/27002 y CIS Controls v8 para tratar riesgos priorizados.	Riesgos priorizados; checklist de controles; matriz de trazabilidad; requisitos legales; capacidades tecnológicas actuales.	(1) Seleccionar controles por riesgo. (2) Mapear controles a ISO/CIS. (3) Definir lineamientos de aplicación (qué, quién, cuándo). (4) Establecer verificación documental (checklist).	Lista de controles propuestos; checklist de verificación; matriz de trazabilidad; lineamientos de control de acceso, backup, logs, etc.	TI/seguridad + administración (para controles organizacionales).
CAPACITACIÓN	Establecer lineamientos de concienciación y buenas prácticas para reducir riesgo humano.	Temas críticos (contraseñas, phishing, uso de activos); roles del personal; brechas culturales identificadas referencialmente.	(1) Definir contenidos mínimos por rol. (2) Establecer frecuencia y modalidad. (3) Definir evidencia de cumplimiento (registro). (4) Integrar al ciclo de mejora continua.	Plan de capacitación; temario por rol; registro modelo de asistencia/evaluación (plantilla).	RR.HH. + TI/seguridad.

Tabla 7 Propuesta definición operacional mínima del modelo

3.11 HALLAZGOS DEL ANÁLISIS DE ACTIVOS, RIESGOS Y CONTROLES

Análisis de Activos. -Desde el enfoque analítico, la infraestructura tecnológica de GLOBESER S.A.S. se presenta de manera referencial a través de los siguientes componentes:

- Servidor central de base de datos en la matriz, con funciones de hosting.
- Estaciones de uso administrativo en oficina matriz.
- Estaciones de monitoreo y soporte técnico.
- Servidores replicadores en cada farmacia (15 puntos de operación).
- Estaciones de facturación, cámaras de seguridad y telefonía IP en cada farmacia.
- Red corporativa a través de Telconet.

Hallazgo referencial: el análisis permite inferir la existencia de un inventario básico de activos; no obstante, se evidencia la necesidad de incorporar un esquema de clasificación formal por criticidad y tipo de información, orientado a la priorización de controles de seguridad conforme a los principios de confidencialidad, integridad y disponibilidad.

Tipo de Activo	Activo	Descripción	Nivel de Criticidad
Hardware	Servidor central	Almacena bases de datos y sistemas corporativos	Alto
Hardware	Servidor Replicador	Replicador de base de datos y uso de estación para punto de venta en cada farmacia	Alto
Hardware	Equipos de usuarios	Computadoras utilizadas por personal administrativo y de ventas en cada farmacia	Medio
Hardware	Equipos de red	Routers y switches en cada farmacia	Alto
Hardware	Equipo de video conferencia	Dvr y cámaras en cada farmacia	Medio
Hardware	Telefonía Ip	Telefono Ip para cada Farmacia	Medio
Software	Sistema de facturación	Sistema Neptuno utilizado para, facturación y inventario en farmacias	Alto
Software	Sistema operativo	Plataforma de los sistemas (Windows 10)	Medio
Información	Base de datos	Información de transacciones comerciales	Alto
Información	Información administrativa	Documentos financieros y administrativos	Alto
Servicios	Internet	Comunicación entre farmacias y sistema central	Alto

Tabla 8 Modelo de Inventario de Activos Tecnológicos

Análisis de Riesgos

Amenazas (teóricas y referenciales):

- Internas: errores del personal administrativo, accesos no autorizados, mala gestión de contraseñas.
- Externas: ataques de ransomware, phishing, vulnerabilidades en software de facturación Neptuno y en servidores replicadores.

Vulnerabilidades:

- Fallas en la red interna asociadas a condiciones operativas deficientes.
- Políticas de seguridad documentadas insuficientes.
- Controles de acceso y gestión de permisos parcialmente definidos.
- Falta de monitoreo centralizado de logs y eventos.

Hallazgo referencial: El análisis evidencia un nivel alto de riesgo en la integridad y disponibilidad de la información, especialmente en replicación de bases de datos y operaciones de facturación.

Análisis de Controles

El análisis referencial considera a los controles ISO 27001/27002 y CIS Controls según la matriz de cumplimiento:

- Controles administrativos (políticas, gestión de riesgos, auditorías internas).
- Controles técnicos (firewalls, backups).
- Controles operativos (capacitación)

Hallazgo referencial: Se establece la existencia potencial de una brecha entre la aplicación de controles y los estándares internacionales, lo cual orienta la incorporación de un modelo que integre la gestión de activos, la evaluación de riesgos y controles alineados a ISO 27002 y CIS.

Propuesta de controles referenciales en base al análisis de Activos y Riesgos

Activo	Riesgo identificado	Control referencial propuesto	Nivel de riesgo
Servidor central de base de datos	Pérdida o corrupción de información crítica	ISO/IEC 27002:2022 8.13 / CIS 11	Alto
Estaciones administrativas (oficina matriz)	Accesos no autorizados / errores humanos	ISO/IEC 27002:2022 5.15–5.18 / CIS 5–6	Medio
Servidores replicadores en farmacias	Fallos de replicación o ataque externo	ISO/IEC 27002:2022 7.10 (+8.8) / CIS 7	Alto
Estaciones de facturación	Robo o manipulación de datos de clientes	ISO/IEC 27002:2022 5.12 / CIS 3 (+ CIS 2 si aplica)	Medio
Cámaras de seguridad y telefonía IP	Intercepción o acceso indebido	ISO/IEC 27002:2022 8.20–8.22 / CIS 13	Medio
Red corporativa	Ataques externos, ransomware, malware	ISO/IEC 27002:2022 8.20–8.22 / CIS 12 (+CIS 13)	Alto
Personal TI y administrativo	Falta de capacitación y conciencia en seguridad	ISO/IEC 27002:2022 6.3 / CIS 14	Medio

Tabla 9 Controles de Activos y Riesgo

3.12 SÍNTESIS DIAGNÓSTICA PARA EL DISEÑO DEL MODELO

Los siguientes elementos analíticos justifican la necesidad del diseño de un modelo de ciberseguridad adaptado a la organización.

- Alto nivel de exposición a riesgos de ciberseguridad
- Ausencia de controles estructurados
- Deficiencia en la gestión de accesos
- Falta de políticas y procedimientos formales
- Limitada cultura de seguridad

El análisis documental, técnico y normativo de la infraestructura tecnológica de la empresa GLOBESER S.A.S. permite inferir la existencia potencial de debilidades estructurales en la gestión de la seguridad de la información, lo cual sugiere adoptar un modelo de ciberseguridad alineado a estándares internacionales

La organización se caracteriza por disponer de una infraestructura tecnológica de alta relevancia, conformada por un servidor central, sistemas de replicación de bases de datos, estaciones de trabajo y redes distribuidas en 15 farmacias, lo que incide en una mayor superficie de exposición a riesgos de ciberseguridad. En este contexto, se evidencia la ausencia de un inventario formal de activos y de una clasificación de la información basada en criterios de confidencialidad, integridad y disponibilidad.

El análisis de riesgos se desarrolla de forma conceptual y referencial, considerando la relación entre activos, amenazas y vulnerabilidades como base para el diseño del modelo.

Adicionalmente, el análisis evidencia que los controles de seguridad existentes presentan un carácter parcial y carecen de una estructuración basada en un marco normativo definido, lo cual permite advertir una posible brecha en relación con estándares internacionales como ISO 27001 y CIS Controls. De igual manera, se sugiere la presencia potencial de una limitada cultura organizacional en ciberseguridad, asociada a la ausencia de programas formales de capacitación y concientización del personal.

En este contexto, la síntesis diagnóstica referencial permite sustentar la necesidad de diseñar un modelo de ciberseguridad alineado con estándares internacionales integrado por ISO 27001 y CIS Controls, bajo un ciclo de mejora continua.

Por lo tanto, se justifica el desarrollo de la propuesta metodológica de modelado en ciberseguridad basado en ISO 27001 y CIS Controls, el cual establece lineamientos, políticas y controles alineados a buenas prácticas internacionales, orientados a mejorar la protección de la infraestructura tecnológica y garantizar los principios de confidencialidad, integridad y

disponibilidad de la información, como base para la adopción institucional del modelo por parte de la organización.

3.13 ESTIMACIÓN REFERENCIAL DE RECURSOS PARA LA ADOPCIÓN INSTITUCIONAL DEL MODELO DE CIBERSEGURIDAD

Se presenta una estimación presupuestaria referencial de \$13,600.00 como referencia económica para la adopción institucional del modelo.

CONCLUSIONES

El trabajo de investigación tuvo como resultado la formulación de una propuesta metodológica de diseño de un modelo de ciberseguridad orientado a fortalecer la protección de la infraestructura tecnológica de la empresa GLOBESER S.A.S., a partir del análisis de estándares como la ISO 27001, el NIST y los CIS Controls.

El principal aporte del estudio consiste en la formulación de una propuesta metodológica de ciberseguridad sustentada en estándares internacionales, sin contemplar implementación operativa ni validación empírica en la organización.

El análisis comparativo de los estándares permitió determinar que ISO 27001 constituye la base más adecuada para la gestión estructurada de la seguridad de la información, los CIS Controls aportan un enfoque técnico y práctico. Por otra parte, el NIST CSF se posiciona como un marco complementario que fortalece la estructura funcional del modelo.

El análisis documental, técnico y normativo establece una base referencial para el diseño del modelo, determinando la integración de ISO 27001 complementado con ISO 27002 como base del modelo, para establecer un sistema formal de gestión de la seguridad de la información, complementado por los CIS Controls, que ofrecen un conjunto de controles técnicos y prácticos.

El NIST Cybersecurity Framework (CSF) no se adopta como estándar principal, sino como un complemento estructural dentro del modelo propuesto. En este contexto, se concluye que varios de los controles evaluados pueden ser abordados con mayor precisión mediante los CIS Controls.

Se ha diseñado un modelo de ciberseguridad adaptado a la realidad de GLOBESER S.A.S., estructurado en componentes de gobierno, activos, riesgos, controles y capacitación, alineados a buenas prácticas. Este modelo establece lineamientos claros

para la gestión de la seguridad de la información, constituyéndose en una propuesta metodológica aplicable y replicable en organizaciones similares del sector farmacéutico.

RECOMENDACIONES

Se recomienda a la empresa GLOBESER S.A.S., valorar la ejecución de procesos de fortalecimiento institucional en ciberseguridad conforme a los lineamientos del modelo propuesto.

Validar técnicamente el modelo de ciberseguridad mediante mecanismos institucionales de contraste y verificación, complementados con el levantamiento de información en el ámbito operativo, a fin de asegurar su consistencia metodológica y pertinencia organizacional.

Se recomienda considerar la adopción progresiva de estándares internacionales como ISO/IEC 27001, ISO/IEC 27002, NIST CSF y CIS Controls, con el fin de establecer un enfoque estructurado, basado en riesgos y alineado a buenas prácticas para la gestión de la seguridad de la información, que sirva de fundamento para el desarrollo de propuestas metodológicas de diseño en ciberseguridad.

Contemplar el modelo con un levantamiento más detallado de activos, riesgos, controles y dependencias críticas, con el fin de ajustar el modelo a la realidad operativa de la organización.

Se considera pertinente la incorporación progresiva de mecanismos de seguimiento, evaluación y mejora continua del modelo mediante indicadores de desempeño, con el fin de fortalecer la cultura organizacional y sostenibilidad del modelo propuesto.

Finalmente, el modelo de ciberseguridad propuesto se establece como base de referencia para la gestión organizacional de la seguridad de la información, aplicable a otras franquicias del Grupo Difare S.A., y contribuye a la estandarización de prácticas de seguridad en el sector farmacéutico.

REFERENCIAS

- Alvarado, C. (2024). *Sistema de Gestión de Seguridad de la Información*.
<https://gestion.pensempos.com/sistema-de-gestion-de-seguridad-de-la-informacion-que-es-etapas>.
- Caballero, M. A. (2022). *CIBERSEGURIDAD PASO A PASO*.
https://anayamultimedia.es/primer_capitulo/ciberseguridad-paso-a-paso.pdf.
- CIS. (2021). *CIS Critical Security Controls Version 8*.
<https://www.cisecurity.org/controls/v8>.
- Cuadra, M. E. (2023). *DISEÑO DE UN SGSI EN ISO 27001*.
<https://dspace.ups.edu.ec/bitstream/123456789/26680/1/UPS-CT011078.pdf>.
- Fortinet. (2025). *Ciberseguridad, amenazas y riesgos*.
<https://www.fortinet.com/lat/resources/cyberglossary/what-is-cybersecurity>.
- Gavilanes, C. A. (2023). *Proyecto de investigación en Gerencia Informática*.
<https://repositorio.puce.edu.ec/server/api/core/bitstreams/f4759b2e-d64b-4b88-8e3c-cbf6c40b7065/content>.
- IBM. (2025). *Marco de ciberseguridad del NIST*. <https://www.ibm.com/mx-es/think/topics/nist>.
- IBM. (2025). *Seguridad de la Red*. <https://www.ibm.com/mx-es/think/topics/network-security>.
- IDB. (2022). *Gestión de Riesgos en Ciberseguridad*.
<https://publications.iadb.org/publications/spanish/document/Gestion-de-riesgos-ciberneticos-en-entornos-de-tecnologias-operativas-OT-guia-para-juntas-directivas.pdf>.
- ISACA. (2012). *COBIT 5*. <https://www.isaca.org/resources/cobit>.
- Mendizábal, D. G. (2018). *REDES CONFIABLES*. <https://techriders.tajamar.es/redes-confiables/>.
- NIST. (2018). *Framework for improving critical infrastructure*.
<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.

- NQA. (2022). *ISO27001:2022*. <https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf>.
- Paez, J. (2025). *Ciberseguridad*. <https://tesa.edu.ec/ciberseguridad-en-ecuador-guia-completa-sobre-su-importancia-y-oportunidades-profesionales/>.
- Ramírez Vargas, J. A., & Pereda Otero, L. R. (2023). *modelo de ciberseguridad para la defensa contra ataques cibernéticos*. https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/672290/Ramirez_VJ.pdf?sequence=1&isAllowed=y.
- School, E. B. (2022). *NORMA ISO 27002*. <https://www.ealde.es/iso-27002-buenas-practicas-ciberseguridad/>.
- UNE-ISO. (2023). *Sistemas de gestión de la seguridad de la información* . https://campusvirtual.cenoeder.com/wp-content/uploads/2025/03/norma-ISO-27001_2022_NOEDER.pdf.

ANEXOS

Anexo 1:

Entrevista

Nombre: _____

Cargo: Gerente General

Área: Dirección General

Años en la empresa: _____

Fecha de la entrevista: _____

1.- Desde su perspectiva como gerente general, ¿qué importancia tiene la ciberseguridad para la operación y continuidad del negocio en la empresa?

2.- ¿Cuáles considera que son los principales riesgos o amenazas que enfrenta la empresa en relación con la seguridad de la información?

3.- ¿La empresa cuenta actualmente con políticas o estrategias formales para proteger la información y los sistemas tecnológicos?

4.- ¿La empresa ha sufrido incidentes de seguridad informática que hayan afectado sus operaciones o la información de clientes?

5.- ¿Considera que el personal de la empresa tiene el conocimiento suficiente para manejar adecuadamente los riesgos relacionados con la seguridad informática?

6.- ¿La empresa destina recursos económicos o estratégicos para fortalecer la seguridad de sus sistemas informáticos?

7.- ¿Considera que sus equipos de su infraestructura actual cumplen con las necesidades de su negocio?

8.- ¿Qué recomendaciones considera importantes para mejorar la seguridad de la información y la protección de la infraestructura tecnológica de la empresa?

Anexo 2.- Matriz de análisis documental de estándares de ciberseguridad

Tipo de fuente	Estándar / Documento	Entidad	Año	Enfoque	Estructura	Componentes clave	Ventajas	Limitaciones	Aporte al modelo propuesto	Nivel de pertinencia
Norma internacional	ISO 27001	ISO	2022	Gestión de seguridad de la información (SGSI)	Cláusulas + Anexo A	Contexto organizacional, liderazgo, planificación, soporte, operación, evaluación y mejora	Certificable, integral, reconocido internacionalmente	Complejo de implementar	Base estructural del modelo, gestión de riesgos y políticas	Alto
Marco de referencia	NIST Cybersecurity Framework (CSF)	NIST	2018	Gestión de riesgos de ciberseguridad	Funciones (Identificar, Proteger, Detectar, Responder, Recuperar)	Categorías y subcategorías de seguridad	Flexible, adaptable, fácil comprensión	No certificable	Permite estructurar el modelo por funciones de seguridad	Alto
Buenas prácticas	CIS Controls	Center for Internet Security	2021	Controles técnicos de ciberseguridad	18 controles priorizados	Inventario de activos, control de accesos, monitoreo, protección de datos	Práctico, priorizado, enfoque técnico	No cubre gestión completa	Fortalece los controles operativos del modelo	Alto
Buenas prácticas (ISO)	ISO 27002	ISO	2022	Directrices de controles de seguridad	Categoría de controles	Controles organizacionales, de personas, físicos y tecnológicos	Complementa ISO 27001	No certificable	Apoya la selección e implementación de controles	Alto
Complementario	Anexo A de ISO 27001	ISO	2022	Controles de seguridad	Lista de controles	Controles de seguridad basados en riesgos	Estructurado y alineado a SGSI	Requiere interpretación técnica	Define controles específicos del modelo	Alto

Tabla 10 Matriz de análisis documental de estándares

Anexo 3.- Modelo de Matriz de inventario de Activos

Proceso :	Identificación de Activos																								
Fecha :	26/5/2026																								
Área:	TI - Infraestructura, Ventas, administrativo																								
Responsable	ALEX LIRIANO RAMÍREZ																								
INFORMACIÓN ACTIVOS																									
No ACTIVO	PROPIEDAD					TIPO								VALORACIÓN				ACCESO		UBICACIÓN		Clasificació n Final	Importanci a del Activo		
	Nombre Activo	Descripción del Activo	Custodio (Asignación de Inventario/dueno de aplicación)	Propietario (quien administra)	Responsab le (quien aplica)		Informacion física/digital	Aplicaciones de Software	Equipos informáticos	Redes de Comunicación	Soporte de la información	Equipamiento auxiliar	Instalaciones	Personal	Intangible	Confidencialidad	Integridad	Disponibilidad	Total Propiedades del Activo	Usuarios con acceso	Permisos de Acceso			Físico	Electrónico
LDFMTIFT11	HP ProBook 450 15.6 inch G10	13th Gen Intel(R) Core(TM) i7-1255U	Director Infraestructura	Responsable del Centro de Datos	Jhonny Yuquilema				X							3	3	3	3	1. Especialista	1. L,E,M	Centro de Datos principal	192.3.3.86	Confidencial	Grave
SGDF00AS05	REPLICADOR BASE DE DATOS	13th Gen Intel(R) Core(TM) i7-11500	Operador de ti	Responsable del Base de datos	Jhon Villavicencio								X			3	3	3	3	1. Especialista 2. Analista 3. Auditoria	1. L,E,M 2. L 3. L 4. L	FARMACIA	192.3.3.198	Confidencial	Grave
SGDF00AS07	ProLiant DL380 G6,	Intel(R) Xeon(R) CPU E5530 @ 2.40GHz	Especialista en seguridad	Responsable de seguridad	Jhon Villavicencio			X								3	3	3	3	1. Analista 2. Lideres 3. Auditoria 4. Director	1. L,E,M 2. L 3. L 4. L	Seguridad Informática	192.3.3.6	Confidencial	Grave
EDFMTSIFT24	LENOVO - 1120-	Intel(R) Core(TM) i5-1100M CPU @ 2.50GHz	Analista de Infraestructura	Responsable de red Corporativa	Jhonny Yuquilema					X						2	2	2	2	1. Analista 2. Lideres 3. Auditoria	1. L,E,M 2. L 3. L	Matriz Corporativa	192.3.3.34	Uso Interno	Importante
LDFMTCMA02	HP ProBook 450 15.6 inch G10 Notebook PC	13th Gen Intel(R) Core(TM) i7-1355U	Soporte técnico	Soporte Técnico	Jhon Villavicencio						X					2	2	2	2	1. Analita 2. Auditoria	1. L,E,M 2. L 3. L	Soporte	192.3.3.24	Uso Interno	Importante
LDFMTGRH05	LENOVO - 1120-	13th Gen Intel(R) Core(TM) i7-1355U	Jefe Ventas	Responsable de Ventas	Roger Cedillo								X			3	3	3	3	1. Analista 2. Lideres 3. Auditoria	1. L,E,M 2. L 3. L	FARMACIA	192.3.3.74	Confidencial	Grave

LDFMTGRH06	LENOVO - 1120-	13th Gen Intel(R) Core(TM) i7-1355U	AUXILIAR DE VENTAS	VENTAS	Karina Gómez									X		2	3	2	2	1. Auxiliar de ventas	1. L	FARMACIA	192.3.3.74	Confidencial	Importante
LDFMTGRH07	LENOVO - 1120-	13th Gen Intel(R) Core(TM) i7-1355U	AUXILIAR DE VENTAS	VENTAS	Magdalena Gonzabay									X		2	3	2	2	1. Auxiliar de ventas	1. L	FARMACIA	192.3.3.74	Confidencial	Importante

Anexo 4.- Matriz de nivel de madurez

Escala de madurez

Nivel	Descripción
0 - Inexistente	No existen controles ni procesos
1 - Inicial	Controles informales, no documentados
2 - Repetible	Controles definidos pero no estandarizados
3 - Definido	Controles documentados y aplicados
4 - Gestionado	Controles medidos y monitoreados
5 - Optimizado	Mejora continua y madurez alta

Tabla 11 Escala de madurez

Nivel de madurez por componente

Componente	Criterio evaluado	Nivel actual	Nivel objetivo	Evidencia
Gobierno	Políticas de seguridad documentadas	2	4	ISO 27001
Activos	Inventario de activos	2	4	CIS 1 y CIS 2
Riesgos	Evaluación de riesgos formal	1	4	ISO 27001
Controles	Implementación de controles técnicos	2	5	CIS Controls
Capacitación	Formación en seguridad	1	4	CIS 14
Monitoreo	Registro y análisis de eventos	1	4	CIS 8
Mejora	Mejora continua implementada	1	5	PDCA

Tabla 12 Matriz de nivel de madurez por componente

Anexo 5.- Matriz de riesgo, Tratamiento de riesgos y controles de seguridad informática																						
Fecha:		16/5/2026																				
Area:		TI - Infraestructura, Administración y Farmacias																				
Responsable:		ALEX LIRIANO RAMÍREZ																				
Análisis del Riesgo						Evaluación del Riesgo			Tratamiento del Riesgo de la Seguridad de la Información					Riesgo Residual			Implementación de Controles de Seguridad de la Información					Auditorías
Información Activo Identificado		Identificación de Amenazas/Vulnerabilidades/Consecuencias/Controles Existentes				Riesgo Actual																
No ACTIVO	Activo de Información	Amenaza	Vulnerabilidad	Consecuencias	Controles Existentes	Probabilidad	Impacto	Nivel de Riesgo	Opciones de Tratamiento	Tipo de control	Objetivo de Control	Responsable	Áreas que participan	Probabil idad	Impacto	Nivel Riesgo Residual	Fecha inicio	Fecha fin	Recursos	Monto de inversión aproxima do	Observaciones	Entregable
LDFMTIFT11	Computadora de escritorio de operación de Infraestructura como servidor central	Errores de mantenimiento / actualización de programas (software)	Ausencia de un eficiente control de cambios en la configuración	Problemas de infraestructur a, Interrupción de servicios	Programas periódicos de mantenimiento preventivo de los equipos del centro de control	3	2	Riesgo Moderado	Mitigar	Preventivo	Dominio 4. Seguridad física y del entorno, ítem 4.9 Mantenimiento de los equipos, numeral c.	Operador de Ti	TIC	1	3	Riesgo Bajo	1/7/2026	2/7/2026	INFRAESTRUTURA	\$200	Mano de obra personal interno de la Empresa (1 funcionario a cargo) procedimiento se ejecuta diariamente.	Proteger la red interna y los puntos de acceso externos.
		Errores de mantenimiento / actualización de equipos (hardware)	Errores que pudieran presentarse después de una tarea de mantenimiento	Equipos bloqueados	Implementación de medidas de seguridad	3	3	Riesgo Alto	Mitigar	Correctivo	Dominio 4. Seguridad física y del entorno, ítem 4.9 Mantenimiento de los equipos, numeral c.	Operador de Ti	TIC	1	3	Riesgo Bajo	1/7/2026	2/7/2026	INFRAESTRUTURA	\$500	Mano de obra personal interno de la Corporación (2 funcionarios a cargo) procedimiento se ejecuta semestralmente	Registro de mantenimientos preventivos y correctivos
		Manipulación de la configuración	Conexiones de red pública sin protección	apagado de equipos	Gestión de Incidentes	1	3	Riesgo Bajo	Evitar	Preventivo	Dominio 5. Uso adecuado de estaciones de trabajo, ítem 5.4 Protección de los puertos de configuración y diagnóstico remoto, numeral b.	Operador de Ti	TIC	1	2	Riesgo Bajo	1/7/2026	2/7/2026	INFRAESTRUTURA	\$400	Mano de obra personal interno de la Corporación (1 funcionario a cargo) procedimiento se ejecuta trimestralmente	Registro de mantenimientos preventivos y correctivos
		Difusión de software dañino	Descarga y uso no controlados de software	Equipo inhabilitado por un malware	Antivirus	3	2	Riesgo Moderado	Mitigar	Preventivo	Dominio 5. Uso adecuado de estaciones de trabajo, ítem 5.6 Trabajo remoto, numeral c.	Operador de Ti	TIC	1	2	Riesgo Bajo	2/7/2026	3/7/2026	INFRAESTRUTURA	\$600.00	Mano de obra personal interno de la Corporación (1 funcionario a cargo) procedimiento rutinario.	Registro de los agentes que administra la consola máster del antivirus Corporativo. Informe de los equipos de cómputo en los centros de operación que tienen instalado un antivirus.
		Acceso no autorizado	Tablas de contraseñas sin protección	Bloqueo de puertos y accesos a lose servidor	Formación	4	3	Riesgo Alto	Mitigar	Correctivo	Dominio 6. Control de acceso a los sistemas de información, ítem 6.1 Control de acceso, numeral a.	Analista de Ti	TIC	1	2	Riesgo Bajo	2/7/2026	3/7/2026	INFRAESTRUTURA	\$800	Mano de obra personal interno de la Corporación (1 funcionario a cargo) ejecución periódica trimestral.	Informe de los equipos de cómputo en los centros de operación que tienen configuradas cuentas de usuario.

		Fugas de información	Tablas de contraseñas sin protección	Extorsión	Concienciación	4	5	Riesgo Extremo	Mitigar	Correctivo	Dominio 9. Gestión de la Continuidad del Negocio, ítem 9.3 Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información, numeral c.	Analista de Ti	TIC	3	5	Riesgo Extremo	2/7/2026	3/7/2026	INFRAESTRUTURA	\$300	Adquisición de equipos, servicio y mano de obra de personal interno.	Check list de los requisitos definidos como estrategias
SGDF00AS05	Computadora de escritorio de operación replicador Base de Datos Farmacia FW001	Errores de mantenimiento / actualización de equipos (hardware)	Ausencia o insuficiencia de pruebas de sw	Problemas de infraestructura, Interrupción de servicios	Programas periódicos de mantenimiento preventivo de los equipos del centro de control	3	2	Riesgo Moderado	Mitigar	Preventivo	Dominio 4. Seguridad física y del entorno, ítem 4.9 Mantenimiento de los equipos, numeral c.	Analista de Tic	TIC	1	3	Riesgo Bajo	4/7/2026	5/7/2026	INFRAESTRUTURA	\$300	Mano de obra personal interno de la Corporación (1 funcionario a cargo) procedimiento se ejecuta diariamente.	Registro de mantenimientos preventivos y correctivos
		Errores del administrador	Habilitación de servicios innecesarios	Problemas de infraestructura, Interrupción de servicios	Implementación de medidas de seguridad	3	3	Riesgo Alto	Evitar	Preventivo	Dominio 4. Seguridad física y del entorno, ítem 4.9 Mantenimiento de los equipos, numeral c.	Supervisor de Operaciones	TIC	1	3	Riesgo Bajo	4/7/2026	5/7/2026	INFRAESTRUTURA	\$300	Mano de obra personal interno de la Corporación 1 funcionarios a cargo) procedimiento se ejecuta semestralmente	Registro de mantenimientos preventivos y correctivos
		Corte del suministro eléctrico	Susceptibilidad a las variaciones de voltaje	apagado de equipos	Implementación de medidas de seguridad	3	3	Riesgo Alto	Evitar	Correctivo	Dominio 4. Seguridad física y del entorno, ítem 4.9 Mantenimiento de los equipos, numeral c.	Supervisor de Operaciones	TIC	1	2	Riesgo Bajo	4/7/2026	5/7/2026	INFRAESTRUTURA	\$400	Mano de obra personal interno de la Corporación (1 funcionario a cargo) procedimiento se ejecuta trimestralmente	Registro de mantenimientos preventivos y correctivos
		Difusión de software dañino	Descarga y uso no controlados de software	Equipo inhabilitado por un malware	Antivirus	4	4	Riesgo Extremo	Mitigar	Preventivo	Dominio 6. Control de acceso a los sistemas de información, ítem 6.1 Control de acceso, numeral a.	Supervisor de Operaciones	TIC	1	2	Riesgo Bajo	4/7/2026	5/7/2026	INFRAESTRUTURA	\$300	Mano de obra personal interno de la Corporación (1 funcionario a cargo) procedimiento se ejecuta trimestralmente	Registro de mantenimientos preventivos y correctivos
SGDF00AS07	Computadora de escritorio de operación de Infraestructura PERSONAL TI	Análisis de tráfico	Ausencia de mecanismos de identificación y autenticación, como la autenticación de usuario	bloque de equipo	Monitoreos	2	2	Riesgo Moderado	Mitigar	Preventivo	Dominio 4. Seguridad física y del entorno, ítem 4.9 Mantenimiento de los equipos, numeral c.	Analista de Tic	TIC	1	3	Riesgo Bajo	6/7/2026	7/7/2026	INFRAESTRUTURA	\$300	Mano de obra personal interno de la Corporación (1 funcionario a cargo) procedimiento se ejecuta diariamente.	Registro de mantenimientos preventivos y correctivos
		Errores del administrador	Habilitación de servicios innecesarios	Problemas de infraestructura, Interrupción de servicios	Implementación de medidas de seguridad	2	2	Riesgo Moderado	Mitigar	Correctivo	Dominio 5. Uso adecuado de estaciones de trabajo, ítem 5.4 Protección de los puertos de configuración y diagnóstico	Supervisor de Operaciones	TIC	2	3	Riesgo Moderado	6/7/2026	7/7/2026	INFRAESTRUTURA	\$400	Mano de obra personal interno de la Corporación 1 funcionarios a cargo) procedimiento se ejecuta semestralmente	Establecer un plan de respuesta a incidentes (

										remoto, numeral b.												
		Acceso no autorizado	Gestión deficiente de las contraseñas	Contraseñas débiles o reutilizadas	Implementación de medidas de seguridad	3	3	Riesgo Alto	Mitigar	Preventivo	Dominio 5. Uso adecuado de estaciones de trabajo, ítem 5.4 Protección de los puertos de configuración y diagnóstico remoto, numeral b.	Supervisor de Operaciones	TIC	1	2	Riesgo Bajo	6/7/2026	7/7/2026	INFRAESTRUTURA	\$300	Mano de obra personal interno de la Corporación (1 funcionario a cargo) procedimiento se ejecuta trimestralmente	Establecer políticas de contraseñas seguras
		Difusión de software dañino	Software nuevo o inmaduro	Equipo inhabilitado por un malware	Antivirus	3	3	Riesgo Alto	Evitar	Preventivo	Dominio 5. Uso adecuado de estaciones de trabajo, ítem 5.4 Protección de los puertos de configuración y diagnóstico remoto, numeral b.	Supervisor de Operaciones	TIC	1	2	Riesgo Bajo	6/7/2026	7/7/2026	INFRAESTRUTURA	\$400	Mano de obra personal interno de la Corporación (1 funcionario a cargo) procedimiento se ejecuta trimestralmente	Registro de mantenimientos preventivos y correctivos
EDFMTSIFT24	Computadora de escritorio de operación de red corporativa	Análisis de tráfico	Tráfico sensible sin protección	Perdida de conexión	Monitoreos	2	2	Riesgo Moderado	Mitigar	Preventivo	Dominio 4. Seguridad física y del entorno, ítem 4.9 Mantenimiento de los equipos, numeral c.	Analista de Tic	TIC	1	3	Riesgo Bajo	8/6/2025	9/6/2026	INFRAESTRUTURA	\$300	Mano de obra personal interno de la Corporación (1 funcionario a cargo) procedimiento se ejecuta diariamente.	Registro de mantenimientos preventivos y correctivos
		Interrupción de otros servicios y suministros esenciales	Habilitación de servicios innecesarios	Problemas de infraestructura, Interrupción de servicios	Implementación de medidas de seguridad	3	3	Riesgo Alto	Mitigar	Correctivo	Dominio 4. Seguridad física y del entorno, ítem 4.9 Mantenimiento de los equipos, numeral c.	Soporte Técnico	TIC	1	3	Riesgo Bajo	10/6/2025	11/6/2027	INFRAESTRUTURA	\$300	Mano de obra personal interno de la Corporación 1 funcionarios a cargo) procedimiento se ejecuta semestralmente	Registro de mantenimientos preventivos y correctivos
		Acceso no autorizado	Ausencia de control de cambios eficaz	Acceso a la red de usuarios no permitidos	Implementación de medidas de seguridad	2	3	Riesgo Moderado	Mitigar	Preventivo	Dominio 5. Uso adecuado de estaciones de trabajo, ítem 5.4 Protección de la red física b.	Soporte Técnico	TIC	1	2	Riesgo Bajo	10/6/2025	11/6/2027	INFRAESTRUTURA	\$300	Mano de obra personal interno de la Corporación (1 funcionario a cargo) procedimiento se ejecuta trimestralmente	Establecer un plan de respuesta a incidentes
		Caída del sistema por agotamiento de recursos	Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)	Redes Wi-Fi inseguras	Implementación de medidas de seguridad	4	4	Riesgo Extremo	Evitar	Preventivo	Dominio 5. Uso adecuado de estaciones de trabajo, ítem 5.4 Protección de la red física b.	Supervisor de Operaciones	TIC	3	3	Riesgo Alto	10/6/2025	11/6/2027	INFRAESTRUTURA	\$800	Mano de obra personal interno de la Corporación (1 funcionario a cargo) procedimiento se ejecuta trimestralmente	Registro de mantenimientos preventivos y correctivos

LDFMTGRH02	Computadora de escritorio de operación del Director Financiero	Escapes de información	Falta de cuidado en la disposición final	Accesos no controlados	Protección por antivirus	3	3	Riesgo Alto	Evitar	Preventivo	Dominio 5. Uso adecuado de estaciones de trabajo, ítem 5.4 Protección de los puertos de configuración y diagnóstico remoto, numeral b.	Directora Financiero	Financiero	1	3	Riesgo Bajo	12/6/2025	13/6/2026	Financiero	\$400	Mano de obra personal interno de la Corporación (1 funcionario a cargo) procedimiento se ejecuta diariamente.	garantizar el cumplimiento normativo y mantener la confianza de sus clientes y socios comerciales.
		Errores de los usuarios	Asignación errada de los derechos de acceso	Interrupción de servicios	Implementación de medidas de seguridad	3	3	Riesgo Alto	Mitigar	Preventivo	Dominio 4. Seguridad física y del entorno, ítem 4.9 Mantenimiento de los equipos, numeral c.	Directora Financiero	Financiero	1	3	Riesgo Bajo	12/6/2025	13/6/2026	Financiero	\$400	Mano de obra personal interno de la Corporación 1 funcionarios a cargo) procedimiento se ejecuta semestralmente	garantizar el cumplimiento normativo y mantener la confianza de sus clientes y socios comerciales.
		Ataque destructivo	Descarga y uso no controlados de software	Acceso a la red de usuarios no permitidos	Capacitar al personal	3	3	Riesgo Alto	Evitar	Preventivo	Dominio 5. Uso adecuado de estaciones de trabajo, ítem 5.4 Protección de los puertos de configuración y diagnóstico remoto, numeral b.	Directora Financiero	Financiero	1	2	Riesgo Bajo	12/6/2025	13/6/2026	Financiero	\$300	Mano de obra personal interno de la Corporación (1 funcionario a cargo) procedimiento se ejecuta trimestralmente	Capacitar en el uso seguro de herramientas y sistemas
		Robo	Falta de conciencia acerca de la seguridad	Software malicioso	Revisión de políticas y procedimientos	5	4	Riesgo Extremo	Mitigar	Preventivo	Dominio 5. Uso adecuado de estaciones de trabajo, ítem 5.4 Protección de los puertos de configuración y diagnóstico remoto, numeral b.	Directora Financiero	Financiero	2	3	Riesgo Moderado	12/6/2025	13/6/2026	Financiero	\$400	Mano de obra personal interno de la Corporación (1 funcionario a cargo) procedimiento se ejecuta trimestralmente	Implementar sistemas de monitoreo para detectar actividades sospechosas
LDFMTGRH05	Computadora de escritorio de operación ventas Farmacias FW013	Escapes de información	Falta de cuidado en la disposición final	Accesos no controlados	Protección por antivirus	3	3	Riesgo Alto	Evitar	Preventivo	Dominio 5. Uso adecuado de estaciones de trabajo, ítem 5.4 Protección de los puertos de configuración y diagnóstico remoto, numeral b.	Jefe de ventas	ventas	1	3	Riesgo Bajo	14/6/2025	15/6/2026	Ventas	\$400	Mano de obra personal interno de la Corporación (1 funcionario a cargo) procedimiento se ejecuta diariamente.	garantizar el cumplimiento normativo y mantener la confianza de sus clientes y socios comerciales.
		Errores del administrador	Asignación errada de los derechos de acceso	Interrupción de servicios	Implementación de medidas de seguridad	4	4	Riesgo Extremo	Mitigar	Preventivo	Dominio 4. Seguridad física y del entorno, ítem 4.9 Mantenimiento de los equipos, numeral c.	Jefe de ventas	ventas	1	3	Riesgo Bajo	14/6/2025	15/6/2026	ventas	\$300	Mano de obra personal interno de la Corporación 1 funcionarios a cargo) procedimiento se ejecuta semestralmente	Capacitar en el uso seguro de herramientas y sistemas
		Ataque destructivo	Descarga y uso no controlados de software	Acceso a la red de usuarios no permitidos	Implementación de medidas de seguridad	3	3	Riesgo Alto	Evitar	Correctivo	Dominio 5. Uso adecuado de estaciones de trabajo, ítem	Jefe de ventas	ventas	1	2	Riesgo Bajo	14/6/2025	15/6/2026	ventas	\$400	Mano de obra personal interno de la Corporación (1	Implementar sistemas de monitoreo para detectar

										5.4 Protección de la red física b.									funcionario a cargo) procedimiento se ejecuta trimestralmente	actividades sospechosas		
		Alteración accidental de la información	Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento	Software malicioso	Implementación de medidas de seguridad	3	3	Riesgo Alto	Mitigar	Preventivo	Dominio 5. Uso adecuado de estaciones de trabajo, ítem 5.4 Protección de los puertos de configuración y diagnóstico remoto, numeral b.	Jefe de ventas	ventas	1	2	Riesgo Bajo	14/6/2025	15/6/2026	ventas	\$800	Mano de obra personal interno de la Corporación (1 funcionario a cargo) procedimiento se ejecuta trimestralmente	Implementar sistemas de monitoreo para detectar actividades sospechosas
LDFMTGRH06	Computadora de escritorio de operación de ventas Farmacia FW001	Destrucción de información	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Perdida de información	Implementación de medidas de seguridad	4	4	Riesgo Extremo	Mitigar	Preventivo	Dominio 5. Uso adecuado de estaciones de trabajo, ítem 5.4 Protección de los puertos de configuración y diagnóstico remoto, numeral b.	Analista de ventas	ventas	1	3	Riesgo Bajo	14/6/2025	15/6/2026	ventas	\$300	Mano de obra personal interno de la Corporación (1 funcionario a cargo) procedimiento se ejecuta diariamente.	garantizar el cumplimiento normativo y mantener la confianza de sus clientes y socios comerciales.
		Errores de los usuarios	Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo	Interrupción de servicios	Implementación de medidas de seguridad	3	3	Riesgo Alto	Mitigar	Preventivo	Dominio 5. Uso adecuado de estaciones de trabajo, ítem 5.4 Protección de los puertos de configuración y diagnóstico remoto, numeral b.	Analista de ventas	ventas	1	3	Riesgo Bajo	14/6/2025	15/6/2026	ventas	\$300	Mano de obra personal interno de la Corporación 1 funcionarios a cargo) procedimiento se ejecuta semestralmente	Capacitar en el uso seguro de herramientas y sistemas
		Ataque destructivo	Descarga y uso no controlados de software	Acceso a la red de usuarios no permitidos	Implementación de medidas de seguridad	3	3	Riesgo Alto	Evitar	Correctivo	Dominio 5. Uso adecuado de estaciones de trabajo, ítem 5.4 Protección de la red física b.	Analista de ventas	ventas	2	4	Riesgo Alto	14/6/2025	15/6/2026	ventas	\$400	Mano de obra personal interno de la Corporación (1 funcionario a cargo) procedimiento se ejecuta trimestralmente	Implementar sistemas de monitoreo para detectar actividades sospechosas
		Alteración accidental de la información	Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento	Software malicioso	Protección por antivirus	3	3	Riesgo Alto	Evitar	Preventivo	Dominio 5. Uso adecuado de estaciones de trabajo, ítem 5.4 Protección de los puertos de configuración y diagnóstico remoto, numeral b.	Analista de ventas	ventas	1	2	Riesgo Bajo	14/6/2025	15/6/2026	ventas	\$400	Mano de obra personal interno de la Corporación (1 funcionario a cargo) procedimiento se ejecuta trimestralmente	garantizar el cumplimiento normativo y mantener la confianza de sus clientes y socios comerciales.
LDFMTGRH07	Computadora de escritorio de operación de ventas Farmacia fw002	Destrucción de información	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Perdida de información	Implementación de medidas de seguridad	4	4	Riesgo Extremo	Mitigar	Preventivo	Dominio 5. Uso adecuado de estaciones de trabajo, ítem 5.4 Protección de los puertos de configuración y diagnóstico	Analista de ventas	ventas	3	3	Riesgo Alto	15/6/2025	16/6/2026	ventas	\$400	Mano de obra personal interno de la Corporación (1 funcionario a cargo) procedimiento se ejecuta diariamente.	garantizar el cumplimiento normativo y mantener la confianza de sus clientes y socios comerciales.

										remoto, numeral b.												
		Errores de los usuarios	Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo	Interrupción de servicios	Implementación de medidas de seguridad	3	3	Riesgo Alto	Mitigar	Preventivo	Dominio 5. Uso adecuado de estaciones de trabajo, ítem 5.4 Protección de los puertos de configuración y diagnóstico remoto, numeral b.	Analista de ventas	ventas	1	3	Riesgo Bajo	15/6/2025	16/6/2026	ventas	\$400	Mano de obra personal interno de la Corporación 1 funcionarios a cargo) procedimiento se ejecuta semestralmente	Capacitar en el uso seguro de herramientas y sistemas
		Ataque destructivo	Descarga y uso no controlados de software	Acceso a la red de usuarios no permitidos	Implementación de medidas de seguridad	3	3	Riesgo Alto	Evitar	Correctivo	Dominio 5. Uso adecuado de estaciones de trabajo, ítem 5.4 Protección de la red física b.	Analista de ventas	ventas	3	3	Riesgo Alto	15/6/2025	16/6/2026	ventas	\$400	Mano de obra personal interno de la Corporación (1 funcionario a cargo) procedimiento se ejecuta trimestralmente	Implementar sistemas de monitoreo para detectar actividades sospechosas
		Alteración accidental de la información	Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento	Software malicioso	Protección por antivirus	3	3	Riesgo Alto	Evitar	Preventivo	Dominio 5. Uso adecuado de estaciones de trabajo, ítem 5.4 Protección de los puertos de configuración y diagnóstico remoto, numeral b.	Analista de ventas	ventas	1	2	Riesgo Bajo	15/6/2025	16/6/2026	ventas	\$400	Mano de obra personal interno de la Corporación (1 funcionario a cargo) procedimiento se ejecuta trimestralmente	garantizar el cumplimiento normativo y mantener la confianza de sus clientes y socios comerciales.