Modelo de madurez en ciberseguridad para empresas que manejan datos de salud

UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS

FACULTAD DE INGENIERÍA

PROGRAMA ACADÉMICO DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN

Modelo de madurez en ciberseguridad para empresas que manejan datos de salud

TESIS

Para optar el título profesional de Ingeniero de Sistemas de Información

AUTOR(ES)

Pérez Navarro, Henry Bryan (0000-0002-0283-2965)

Salcedo Jara, Humberto Luis (0000-0003-2994-9263)

ASESOR

Vargas Medina, José Carlos (0000-0002-2101-5477)

Lima, 18 de Marzo de 2021

DEDICATORIA

[Dedicado a nuestras familias que nos apoyaron durante el transcurso de la carrera]

AGRADECIMIENTOS

A todos nuestros profesores, no solo de la carrera sino de toda la vida, mil gracias porque de alguna manera forman parte de lo que ahora somos. Especialmente a los que estuvieron en el desarrollo de esta investigación: Jose Carlos Vargas y Jimmy Armas.

Además, un pequeño agradecimiento especial a la familia Joestar y Dio Brando, ayudaron a que la etapa inicial de investigación del proyecto sea divertida y amena.

RESUMEN

El avance de la digitalización en distintas industrias trae consigo nuevos riesgos potenciales. Aquellas que pertenecen al sector salud se encuentran entre las que mayores riesgos deben enfrentar. La privacidad de los datos en el sector salud se encuentra regulada y las multas por el incumplimiento de normativas pueden afectar a las compañías, ya que esto indica que ponen en peligro los datos personales de sus clientes. Por ello, las industrias que pertenecen a este sector, necesitan una herramienta que facilite la identificación de capacidades en Ciberseguridad, Privacidad y gestión de datos de salud para cumplir con las normativas vigentes, y reducir los riesgos que comprometan la confidencialidad, integridad y accesibilidad de los datos.

En este trabajo se propone un modelo de madurez de capacidades que identifica el grado de fiabilidad de los elementos de Ciberseguridad y Privacidad aplicados al Sector Salud. Esto se realizó mediante la selección de modelos, frameworks y normativas, aumentando su complejidad mediante la integración de capacidades de privacidad y gestión de datos de salud.

El modelo se validó en una empresa del sector salud con una herramienta de diagnóstico y se observaron los resultados. Los resultados obtenidos se compararon con los componentes originales del modelo para verificar que los componentes se integraron holísticamente. Además, se entregó un formulario de evaluación del modelo a la empresa cliente para comprobar el nivel de satisfacción con respecto al uso del modelo y sus componentes.

Palabras clave**:** Ciberseguridad; Privacidad; Sector Salud; Modelo de Madurez.

Cybersecurity maturity model for businesses that interact with health data

ABSTRACT

The advancement of digitalization in different sectors brings along with it new potential risks. One of the sectors that have to confront said risks is the health sector. Data privacy in the health sector is heavily regulated and fines for non-compliance can affect the companies since it implies putting the client's personal data at risk. Because of this, businesses belonging to the health sector need a tool to help with the identification of capabilities in Cybersecurity, Privacy and Health data management to achieve compliance with the current norms and reduce risks that might compromise the Confidentiality, Integrity and Availability of data

This work proposes a capability maturity model that can identify the reliability of Cybersecurity and Privacy elements applied to the Health Sector. This was achieved through the use of models, frameworks and norms; allowing us to increase their complexity through the integration of privacy and health information management capacities.

The model was validated by using a diagnosis tool in a health sector business and observing the results. The obtained results were compared with the original components of the model to verify the holistic integration of said components. We also used a model evaluation form to measure the satisfaction level of the business regarding the use of the model and its components

Keywords: Cybersecurity; Privacy; Health Sector; Maturity Model

TABLA DE CONTENIDOS

CONTENIDO

INTRODUCCIÓN **1**

CAPÍTULO 1 - DEFINICIÓN DEL PROYECTO **2**

1.1 OBJETO DE ESTUDIO 3
1.2 DOMINIO DE LA NECESIDAD 3
1.3 MOTIVACIÓN A LA INVESTIGACIÓN 3
1.4 OBJETIVOS DE LA INVESTIGACIÓN 4
1.4.1 Objetivo General 4
1.4.2 Objetivos Específicos 4
1.5 INDICADORES DE ÉXITO 4
1.6 ALCANCE DEL PROYECTO 5

CAPÍTULO 2 - LOGROS DE LOS STUDENT OUTCOMES **7**

2.1 STUDENT OUTCOME 1 8
2.2 STUDENT OUTCOME 2 8
2.3 STUDENT OUTCOME 3 9
2.4 STUDENT OUTCOME 4 10
2.5 STUDENT OUTCOME 5 11
2.6 STUDENT OUTCOME 6 11
2.7 STUDENT OUTCOME 7 11

CAPÍTULO 3 - MARCO TEÓRICO **13**

3.1 SECTOR SALUD 14
3.2 ENTIDADES REGULADORAS 14
3.2.1 SUSALUD 14
3.3 HIPAA 15
3.4 LEY N° 29733 15
3.5 LEY N° 30024 15
3.6 NIST CF 15
3.7 NIST PF 16
3.8 NIST 800-53 16

3.9 AICPA/CICA Privacy Maturity Model 16
3.10 Modelos de madurez 16

CAPÍTULO 4 - DESARROLLO DEL PROYECTO 17

4.1 Propósito y Componentes 18
4.1.1 Taxonomía 18
4.1.2 Benchmark 19
4.1.3 Categorías 23
4.1.4 Subcategorías 24
4.1.5 Controles 24
4.1.6 Artefactos 25
4.2 Escala de madurez 26
4.3 Especificaciones por nivel de componente 27
4.3.1 Modelo de Madurez propuesto 28
4.4 Validación 29

CAPÍTULO 5 - RESULTADOS DEL PROYECTO 33

5.1 Organización 34
5.2 Implementación 34
5.3 Resultados 34
5.4 Plan de continuidad 40

CAPÍTULO 6 - GESTIÓN DEL PROYECTO 44

6.1 Ciclo de Vida del Proyecto 45
6.2 Enfoques de Desarrollo 45
6.3 Cronograma del proyecto 46
6.4 Entregables 48
6.5 Gestión de recursos humanos 48
6.6 Organigrama del Proyecto 49
6.7 Roles y Responsabilidades 50
6.8 Gestión de Riesgos 51
6.9 Frecuencia y Tiempo 51
6.10 Seguimiento de Riesgos 51
6.11 Gestión de comunicaciones 51

6.12 GESTIÓN DE ADQUISICIONES 54
6.13 GESTIÓN DE COSTO 55
6.14 GESTIÓN DE CALIDAD 55
6.15 GESTIÓN DE REQUERIMIENTOS 57
6.15.1 Reporte 58
6.15.2 Validación de Requerimientos 58
6.16 GESTIÓN DEL ALCANCE 58
6.16.1 EDT 58
6.16.2 Aceptación de Entregables 60
6.16.3 Alcance e integración de requerimientos 60
CONCLUSIONES 61
RECOMENDACIONES 62
GLOSARIO 63
BIBLIOGRAFÍA 63

ÍNDICE DE TABLAS

Tabla 1 - Indicadores de éxito 5
Tabla 2 - Cumplimiento de Student Outcome 1 8
Tabla 3 - Cumplimiento de Outcome 3 9
Tabla 4 - Benchmark de Herramientas de Ciberseguridad 19
Tabla 5 - Benchmark de Herramientas de Privacidad 19
Tabla 6 - Benchmark de Herramientas para Manejo de Datos de Salud 20
Tabla 7 - Criterio de puntaje para Benchmark 21
Tabla 8 - Elementos utilizados para la contrucción del Modelo 21
Tabla 9 - Criterios de medición 22
Tabla 10 - Categorías 23
Tabla 11 - Escala de Madurez 26
Tabla 12 - Resultados de implementación 30
Tabla 13 - Conceptos y métricas de Evaluación 31
Tabla 14 - Comparación de controles 1 35
Tabla 15 - Comparación de controles 2 35
Tabla 16 - Comparación de controles 3 35
Tabla 17 - Diagnótico 36
Tabla 18 - Dashboard de Revisión y Monitoreo 37
Tabla 19 - Dashboard de Procesos, políticas y procedimientos 37
Tabla 20 - Dashboard de Seguridad de Datos 38
Tabla 21 - Dashboard de Procesos y procedimientos de protección de información 38
Tabla 22 - Dashboard de Interoperabilidad 39
Tabla 23 - Resultados de formulario 40
Tabla 24 - Ciclo de vida del proyecto 45
Tabla 25 - Enfoques de desarrollo 46
Tabla 26 - Cronograma del proyecto 46
Tabla 27 - Entregables 48
Tabla 28 - Miembros del Equipo y Estimaciones 49
Tabla 29 - Fecha de Adquisiciones 54
Tabla 30 - Supuestos y restricciones de adquisiciones 54
Tabla 31 - Métricas de Plan de Continuidad 56
Tabla 32 - Entregables Plan de Continuidad 56

ÍNDICE DE FIGURAS

Figura 1 - Funcionamiento de Sector Salud 14
Figura 2 - Taxonomía basada en ACM 18
Figura 3 - Subcategorías elaboradas 24
Figura 4 - Controles 25
Figura 5 - Modelo de Madurez Propuesto 29
Figura 6 - Organigrama del Proyecto 50
Figura 7 - Roles y responsabilidades 50
Figura 8 - EDT 59

INTRODUCCIÓN

Este documento detalla el proceso de desarrollo del proyecto. Se divide en las siguientes partes:

En el Capítulo 1 se presenta la definición del proyecto. En este capítulo se explican los objetivos generales, necesidad, objetivos específicos e indicadores de éxito.

En el Capítulo 2 se detalla el cumplimiento de los Student Outcomes de ABET. Los Student Outcomes son indicadores para medir el cumplimiento del standard ABET para la facultad de ingeniería de sistemas de información.

En el Capítulo 3 se presenta el marco teórico trabajado durante el desarrollo del proyecto. Se explica el alcance y significado de los términos que se emplearán en el proyecto para poder entender claramente su valor diferencial.

En el Capítulo 4 se explica el desarrollo del proyecto. Desde la investigación de la necesidad, el establecimiento de la propuesta, la investigación de los posibles componentes de esta, la estructuración de la jerarquía del modelo y la escala de madurez de este.

En el Capítulo 5 se presenta el contexto de la empresa en la cual se aplicó el modelo, el proceso de implementación y los resultados obtenidos.

En el Capítulo 6 se detalla la gestión realizada para lograr el éxito del proyecto. Esto incluye elementos de organización como el ciclo de vida, enfoques, cronograma y entregables al igual que elementos de control como la gestión de riesgos, de comunicaciones y de adquisiciones.

CAPÍTULO 1 - DEFINICIÓN DEL PROYECTO

Se explicará la necesidad encontrada por la que este proyecto surge, el objetivo general con sus respectivos objetivos específicos, los indicadores de éxito que permitirán validar los objetivos mencionados y la planificación para terminar con un proyecto exitoso.

1.1 Objeto de Estudio

Implementar un modelo de madurez en ciberseguridad que integre de manera holística aspectos en privacidad y manejo de datos de salud cumpliendo normativas locales e internacionales.

1.2 Dominio de la Necesidad

Facilitar y optimizar la toma de decisiones en aspectos de ciberseguridad, privacidad y manejo de datos de salud por parte de altos directivos de compañías.

1.3 Motivación a la Investigación

Un reporte de IBM indica que, en los años transcurridos desde 2014, el coste total promedio de las data breach a nivel global en distintas industrias ha aumentado un 12% de $3,5 a $3,92 millones de dólares en 2019. Asimismo, las organizaciones sujetas a un mayor rigor en el cumplimiento de requerimientos regulatorios son las que enfrentan un mayor costo de un data breach. La industria de la salud ($6,45 mill), servicios financieros ($5.86 mill), energía ($5.60 mill) y farmacia ($5.20 mill) experimentaron un costo total promedio de una data breach significativamente mayor que otras industrias.(Security, 2019)

Los sistemas de atención de salud de todo el mundo han identificado el enorme potencial de la digitalización para mejorar los resultados clínicos y transformar la prestación del servicio de atención a los pacientes. No obstante, los recientes ataques al sector han demostrado que la ciberseguridad es un problema crítico para la seguridad de los pacientes y que requiere soluciones inmediatas.(Martin et al., 2017)

Por ello, proponemos un modelo de madurez en ciberseguridad que integre de manera holística aspectos de privacidad y gestión de datos de salud siguiendo regulaciones nacionales e internacionales. El modelo permitirá a las compañías del sector salud visualizar

y entender de una manera integrada su estado actual y poder mejorar las debilidades encontradas.

1.4 Objetivos de la Investigación

1.4.1 Objetivo General

Implementar un modelo de madurez en ciberseguridad que amplíe los modelos existentes uniendo holísticamente los conceptos, prácticas, criterios de privacidad y manejo de activos de datos de salud

1.4.2 Objetivos Específicos

- OE1: Analizar mediante benchmarking los distintos modelos en ciberseguridad, privacidad y criterios para el manejo de datos de salud a utilizarse como base en el modelo propuesto.
- OE2: Diseñar el modelo de madurez en ciberseguridad que integre holísticamente los conceptos, prácticas, criterios de privacidad y manejo de datos de salud.
- OE3: Validar el modelo de madurez mediante su implementación en la evaluación de un proceso de la empresa cliente.
- OE4: Elaborar un plan de continuidad y mejora continua que permita la viabilidad del modelo propuesto en el tiempo.

1.5 Indicadores de Éxito

Los indicadores de éxito que corresponden a cada objetivo específico se pueden observar en la Tabla 1.

Tabla 1 - Indicadores de éxito

Indicador de éxito		Objetivo Específico
I1	IE1: Aceptación de benchmark de las perspectivas de ciberseguridad, privacidad y normas de salud a utilizarse por parte del profesor cliente.	OE1
I2	IE2: Aprobación del documento de análisis por parte del profesor cliente.	
I8	IE3: Certificación de taxonomía basada en ACM Cybersecurity Curricular Framework	
I3	IE1: Validación de documento de integración de controles en el diseño del modelo de madurez.	OE2
I4	IE2: Acta de aceptación de diseño de modelo de madurez validada por parte del profesor cliente.	
I5	IE1: Documento de validación del modelo de madurez basado en análisis funcional	OE3
I7	IE2: Validación de modelo de madurez mediante la obtención de Certificado de calidad brindado por empresa IT-Service	
I6	IE1: Validación del plan de continuidad y mejora continua del modelo por el profesor cliente.	OE4

Fuente: Elaboración propia

1.6 Alcance del proyecto

El alcance del proyecto incluye lo siguiente:

- Diseño y validación de una taxonomía de estudios sobre ciberseguridad en distintas áreas de aplicación para identificar

- Diseño de modelo de madurez que integra elementos de Ciberseguridad, Privacidad y Gestión de Datos de Salud
- Validación de modelo de madurez
- Implementación de modelo mediante una herramienta que diagnostica el nivel de madurez en un proceso de una organización de salud seleccionada.

Las exclusiones son las siguientes:

- Implementación del modelo en organizaciones que no pertenecen al sector salud

CAPÍTULO 2 - LOGROS DE LOS STUDENT OUTCOMES

En este capítulo detallaremos el cumplimiento de los Student Outcomes de ABET a lo largo de todo el proyecto.

2.1 Student Outcome 1

Capacidad de identificar, formular y resolver problemas complejos de ingeniería mediante la aplicación de los principios de ingeniería, ciencias y matemáticas.

En la siguiente tabla se desarrolla cada conocimiento y la manera en que fue aplicado durante todo el proyecto.

Tabla 2 - Cumplimiento de Student Outcome 1

Conocimiento	Aplicación
Ingeniería	- Desarrollo del modelo de madurez propuesto priorizando la innovación en su planteamiento y desarrollo. - Analizar el resultado obtenido de la empresa a la que se contactó.
Matemáticas	- Uso de fórmulas matemáticas para la estimación del presupuesto del proyecto. - Uso de fórmulas matemáticas para la estimación de fechas de los hitos y actividades. - Uso de fórmulas matemáticas para la estimación del puntaje en el modelo de madurez propuesto. - Uso de fórmulas matemáticas en la estimación de las métricas de cumplimiento de controles del modelo.
Ciencias	Estudio y análisis de modelos de madurez actuales, mejores prácticas, estándares, normativas nacionales e internacionales y regulaciones.

Fuente: Elaboración propia

2.2 Student Outcome 2

Capacidad de aplicar diseño de ingeniería para producir soluciones que satisfagan necesidades específicas con consideración de salud pública, seguridad y bienestar, así como factores globales, culturales, sociales, ambientales y económicos

El modelo de madurez desarrollado se diseñó tomando en consideración factores como el cumplimiento de regulaciones nacionales e internacionales para proteger la información sanitaria y conservar la privacidad de los pacientes. Asimismo, asegurar la seguridad de la información y privacidad de los datos se puede observar en cada componente del modelo, ya que cada uno está construido para medir y mejorar capacidades de ciberseguridad y privacidad en el sector salud.

El proyecto tiene como producto final un modelo de madurez que permita a las compañías del sector salud conocer de manera integrada su nivel en ciberseguridad, privacidad y gestión de datos de salud. Del mismo modo, poder mejorar las debilidades encontradas.

2.3 Student Outcome 3

Capacidad de comunicarse efectivamente con un rango de audiencias

A lo largo del proyecto se ha comunicado y trabado de la mano de distintos tipos de audiencia. En la siguiente tabla se puede observar de manera detallada

Tabla 3 - Cumplimiento de Outcome 3

Contacto	Interacción
Portfolio Manager	- Consultas sobre mejores prácticas en gestión de proyectos (Definición de Project Charter) - Validación de documentos de gestión - Reuniones para recibir feedback seminal - Monitoreo de reuniones mediante el uso y firma de actas de reunión donde se establecía agenda, actividades pendientes, acuerdos y tareas para la siguiente semana.

Cliente	- Guía y mentoría por parte del Cliente en su campo con el fin de entender la realidad del sector, los problemas y necesidades. - Monitoreo de reuniones mediante el uso y firma de actas de reunión donde se establecía agenda, acuerdos, actividades pendientes y tareas para la siguiente semana.
Recursos de QS	- Responsabilidad en labores de investigación mediante la elaboración de estados del arte y resúmenes que aporten al desarrollo del proyecto. - Monitoreo de reuniones mediante el uso y firma de actas de reunión donde se establecía agenda, actividades pendientes, acuerdos y tareas para la siguiente semana.
Contacto en Empresa	Comunicación con contacto de Empresa Sponsor para la validación del modelo de madurez.

Fuente: Elaboración propia

2.4 Student Outcome 4

Capacidad de reconocer responsabilidades éticas y profesionales en situaciones de ingeniería y hacer juicios informados, que deben considerar el impacto de las soluciones de ingeniería en contextos globales, económicos, ambientales y sociales

El modelo de madurez para el sector de salud que integra de manera holística aspectos de ciberseguridad, privacidad y gestión de datos de salud permitirá mejorar la toma de decisiones con respecto a los aspectos mencionados anteriormente, puesto que proporciona un puntaje único que permita conocer el estado actual de manera integrada.

2.5 Student Outcome 5

Capacidad de funcionar efectivamente en un equipo cuyos miembros en conjunto proporcionan liderazgo, crean un entorno de colaboración e inclusivo, establecen objetivos, planifican tareas y cumplen objetivos

Durante el desarrollo del proyecto se establecieron roles para poder tener una organización efectiva y priorizar actividades de acuerdo al rol y sus responsabilidades asociadas. Se establecieron dos roles, un Jefe de Proyectos que se encargó de la gestión y monitoreo del proyecto y un Jefe de Investigación que se encargó de la búsqueda de fuentes y estudios para la creación de la propuesta.

2.6 Student Outcome 6

Capacidad para desarrollar y llevar a cabo la experimentación apropiada, analizar e interpretar datos, y usar el juicio de ingeniería para sacar conclusiones

Durante el análisis de los distintos modelos de madurez existentes, correspondiente al Objetivo Específico 1: "Analizar mediante benchmarking los distintos modelos en ciberseguridad, privacidad y criterios para el manejo de datos de salud a utilizarse como base en el modelo propuesto", se recopilaron distintos modelos de madurez, estándares, buenas prácticas y leyes correspondientes para ser analizados y filtrados por criterios previamente establecidos. Luego, durante el diseño del modelo de madurez, correspondiente al Objetivo Específico 2: "Diseñar el modelo de madurez en ciberseguridad" se interpretó el contenido de los modelos, estándares y normas escogidas para posteriormente plantear la integración de estas en un solo modelo.

2.7 Student Outcome 7

La capacidad de adquirir y aplicar nuevos conocimientos según sea necesario, utilizando estrategias de aprendizaje adecuadas

Durante la realización del proyecto fue necesario aprender sobre regulaciones de manejo de datos de salud nacionales e internacionales. Asimismo, se necesitó analizar y entender los distintos frameworks y modelos de ciberseguridad y privacidad existentes utilizando dos estrategias:

- Utilizar como apoyo conferencias o videos explicativos de las normativas, frameworks y modelos.
- Empezar el análisis por los modelos y frameworks que abarcan un mayor número de regulaciones.

CAPÍTULO 3 - MARCO TEÓRICO

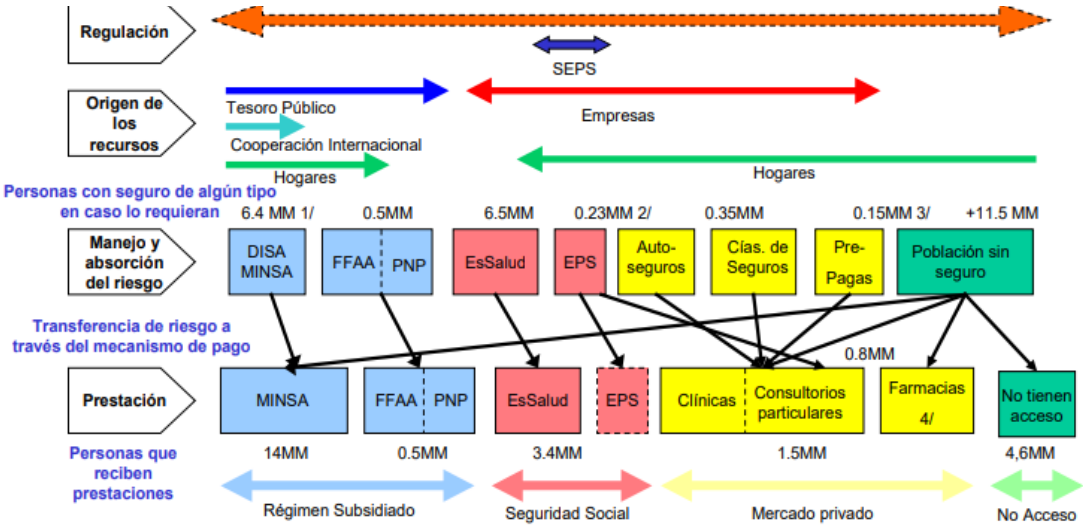
Es valioso conocer el alcance y significado de los términos que se emplearán en el proyecto para poder entender claramente su valor diferencial. Por ello, se explicarán los conceptos relacionados al proyecto con el fin de identificar claramente el aporte propuesto. De esta manera, se explicará acerca del sector de salud, peligros a los que enfrenta, modelos de madurez y regulaciones nacionales e internacionales.

3.1 Sector Salud

El Perú cuenta con un sistema de atención sanitaria descentralizado, administrado por cinco entidades: el Ministerio de Salud (MINSA), que ofrece servicios de salud para el 60% de la población; EsSalud, que cubre el 30% de la población; y las Fuerzas Armadas (FFAA), la Policía Nacional (PNP), y el sector privado, que proporcionan servicios sanitarios al 10% restante (Recursos humanos en salud al 2011). El resultado es un sistema que contiene numerosos proveedores de servicios y seguros, que cuentan con una coordinación deficiente y a menudo desempeñan funciones que se superponen. Los agentes de salud, por su parte, suelen tener diferentes trabajos en múltiples subsectores.(*OMS | El Perú*, n.d.)

En el Perú, la estructura del sector salud se descompone de la siguiente manera:

Figura 1 - Funcionamiento de Sector Salud



3.2 Entidades Reguladoras

3.2.1 SUSALUD

La Superintendencia Nacional de Salud (SUSALUD) es un organismo que pertenece al Ministerio de Salud del Perú, que cuenta con autonomía técnica, funcional, administrativa, económica y financiera. SUSALUD tiene potestad para actuar sobre todas las Instituciones Prestadoras de Salud (IPRESS) así como las Instituciones Administradoras de Fondos de Aseguramiento en Salud (IAFAS), públicas, privadas y mixtas del país.(*Visión y Misión | SUSALUD*, n.d.)

Para esto, desarrolla sus acciones en base a cuatro líneas de acción:

- Promoción, protección y restitución de los Derechos en Salud en el ámbito de todo el territorio nacional.(*Visión y Misión | SUSALUD*, n.d.)
- Prevención permanente de la vulneración de los Derechos en Salud frente al sistema de salud.(*Visión y Misión | SUSALUD*, n.d.)
- Coadyuvar la Gestión del Riesgo para alcanzar de manera más efectiva los logros institucionales de todos los integrantes del sistema de salud como IPRESS, IAFAS y UGIPRESS.(*Visión y Misión | SUSALUD*, n.d.)
- Modernizar la gestión institucional promoviendo espacios de articulación intersectorial y de integración de sistemas de información, para la óptima protección de los derechos en salud de la ciudadanía.(*Visión y Misión | SUSALUD*, n.d.)

3.3 HIPAA

Ley de Transferencia y Responsabilidad de Seguro Médico (Health Insurance Portability and Accountability Act) es una ley que establece lineamientos para proteger la confidencialidad y privacidad de datos médicos.(U.S. Dept. of Labor Employee Benefits Security Administration, 1996)

3.4 Ley N° 29733

Ley de protección de datos personales peruana tiene como finalidad garantizar el derecho fundamental a la protección de datos personales.(Empresa Peruana de Servicios Editoriales S.A., 2013)

3.5 Ley N° 30024

Ley de creación de historia clínica electrónica tiene como objetivo establecer lineamientos para la aplicación del registro nacional de historias clínicas electrónicas y su modificación.(Gobierno del Peru, 2017)

3.6 NIST CF

NIST Cybersecurity Framework es una herramienta elaborada por el Instituto Nacional de Normas y Tecnología (NIST) de Estados Unidos que tiene como objetivo guiar a las organizaciones a gestionar y reducir riesgos de ciberseguridad.(National Institute of Standards and Technolgy, 2014)

3.7 NIST PF

NIST Privacy Framework es una herramienta elaborada por el Instituto Nacional de Normas y Tecnología (NIST) de Estados Unidos que tiene como objetivo guiar a las organizaciones a gestionar y reducir riesgos de privacidad de información.(National Institute of Standards and Technolgy, 2020)

3.8 NIST 800-53

Es una serie de controles establecidos por el Instituto Nacional de Normas y Tecnología (NIST) de Estados Unidos que tienen como objetivo establecer lineamientos para lograr sistemas de información más seguros y gestión de riesgo más eficaz.(National Institute of Standards and Technology (NIST), 2014)

3.9 AICPA/CICA Privacy Maturity Model

Modelo de madurez en privacidad desarrollado por el Instituto Canadiense de Contadores Públicos (CICA) con el objetivo de ayudar a las organizaciones a fortalecer sus políticas y prácticas de privacidad.(AICPA/CICA, 2011)

3.10 Modelos de madurez

Los modelos de madurez son herramientas que permiten identificar el grado de fiabilidad o dependencia que una compañía puede colocar en un proceso para alcanzar metas u objetivos deseados.(*ISACA Interactive Glossary & Term Translations | ISACA*, n.d.)

CAPÍTULO 4 - DESARROLLO DEL PROYECTO

En este capítulo explicaremos el desarrollo del proyecto basándonos en la metodología planteada por Rose para la elaboración de un modelo de madurez.

Elaboramos el modelo en los siguientes pasos: Definir propósito y componentes, determinar la escala y desarrollar las especificaciones para cada nivel de componente.(Rose, 2013)

4.1 Propósito y Componentes

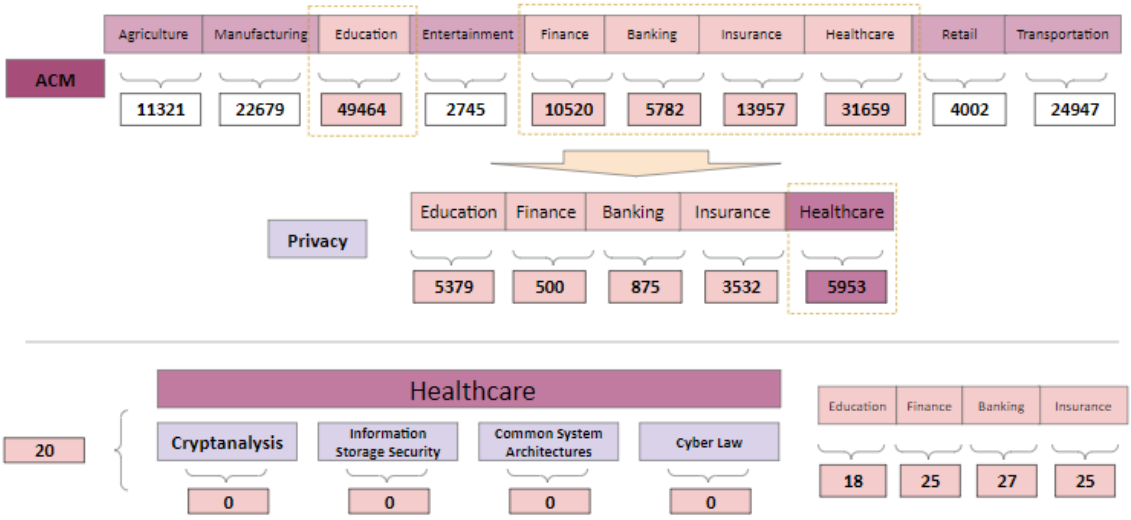
La solución propuesta busca evaluar de manera integrada tres perspectivas: Ciberseguridad, Privacidad y Gestión de Datos de Salud. La aplicación del modelo tiene como objetivo realizar un análisis completo de la organización y con ello mejorar el cumplimiento general, controles y gobernanza de la organización. Para lograrlo, este maneja controles que abarcan de manera unificada estas perspectivas y son utilizados como indicadores de cumplimiento de acuerdo a la categoría que pertenecen y el nivel de implementación del control.

4.1.1 Taxonomía

Para validar el propósito de la investigación elaboramos una taxonomía utilizando como base el ACM Cybersecurity Curricular Framework para identificar el número de estudios que contemplan aspectos de ciberseguridad, privacidad y salud de manera integrada.(*Cybersecurity Curricular Guidance for Associate-Degree Programs*, 2020)

Este análisis se puede observar en la siguiente figura:

Figura 2 - Taxonomía basada en ACM



Fuente: Elaboración propia

A partir de la taxonomía desarrollada se pudo validar que los estudios que contemplan aspectos de ciberseguridad, privacidad y salud son escasos. Asimismo, se pudo comprobar que existe una tendencia al aumento de los estudios en salud y ciberseguridad.

4.1.2 Benchmark

Para la elaboración de los controles realizamos un Benchmark de las herramientas más utilizadas para medir cumplimientos de controles en ciberseguridad privacidad y manejo de datos de salud. Asimismo, establecimos criterios de selección para determinar las más adecuadas para nuestra propuesta. Las herramientas de ciberseguridad evaluadas por criterio se pueden ver en la Tabla 4, las de privacidad en la Tabla 5 y las de manejo de datos de salud en la Tabla 6.

Tabla 4 - Benchmark de Herramientas de Ciberseguridad

HERRAMIENTA	Variable	Normativo	Profundidad Específica	Sector Empresas	Actualidad (>2013)	Relevancia	TOTAL
	Peso	**20%**	**30%**	**15%**	**15%**	**20%**	
NIST CSF	**Puntos**	1	1	2	2	2	**1,5**
	Resultado	0,2	0,3	0,3	0,3	0,4	
COBIT 5	**Puntos**	1	1	2	2	1	1,3
	Resultado	0,2	0,3	0,3	0,3	0,2	
NICE	**Puntos**	1	1	1	2	2	1,35
	Resultado	0,2	0,3	0,15	0,3	0,4	
ISO 27032:2012	**Puntos**	1	1	2	1	2	1,35
	Resultado	0,2	0,3	0,3	0,15	0,4	
ISO 27001:2013	**Puntos**	1	1	2	1	2	1,35
	Resultado	0,2	0,3	0,3	0,15	0,4	
C2M2 v 1.1	**Puntos**	1	2	2	2	2	**1,8**
	Resultado	0,2	0,6	0,3	0,3	0,4	
NIST 800-53	**Puntos**	1	2	1	2	2	**1,65**
	Puntos	0,2	0,6	0,15	0,3	0,4	

Tabla 5 - Benchmark de Herramientas de Privacidad

HERRAMIENTA	Variable	Normativo	Profundidad Específica	Sector Empresas	Actualidad (>2013)	Relevancia	TOTAL

	Peso	20%	30%	15%	15%	20%	
OASIS Privacy Management Reference Model V1.0 CS01	Puntos	1	1	2	2	1	1,3
	Resultado	0,2	0,3	0,3	0,3	0,2	
AICPA/CICA Privacy Maturity Model	Puntos	1	2	2	1	2	**1,65**
	Resultado	0,2	0,6	0,3	0,15	0,4	
ISO 29100:2011	Puntos	1	1	2	1	1	1,15
	Resultado	0,2	0,3	0,3	0,15	0,2	
Ley N° 29733	Puntos	2	2	2	1	2	**1,85**
	Resultado	0,4	0,6	0,3	0,15	0,4	
GDPR	Puntos	2	1	2	2	1	**1,5**
	Resultado	0,4	0,3	0,3	0,3	0,2	

Tabla 6 - Benchmark de Herramientas para Manejo de Datos de Salud

HERRAMIENTA	Variable	Normativo	Profundidad Específica	Sector Empresas	Actualidad (>2013)	Relevancia	TOTAL
	Peso	20%	30%	15%	15%	20%	
Ley N° 30024	Puntos	2	2	1	2	2	**1,85**
	Resultado	0,4	0,6	0,15	0,3	0,4	
HIPAA	Puntos	2	2	1	2	2	**1,85**
	Resultado	0,4	0,6	0,15	0,3	0,4	
ISO 27799:2016 Health Informatics	Puntos	1	2	1	2	2	**1,65**
	Resultado	0,2	0,6	0,15	0,3	0,4	
HISO 10029:2015	Puntos	1	2	1	2	1	1,45
	Resultado	0,2	0,6	0,15	0,3	0,2	
HITECH (HIPAA II)	Puntos	2	2	1	1	2	**1,7**
	Resultado	0,4	0,6	0,15	0,15	0,4	
HiTRUST	Puntos	1	2	1	2	2	**1,65**
	Resultado	0,2	0,6	0,15	0,3	0,4	

Asimismo, para el criterio de evaluación de las herramientas, establecimos puntajes que consideran 5 aspectos: Si la herramienta es normativa, el nivel de profundidad en el campo que aplica, el sector hacia donde se dirige su implementación, su actualidad y relevancia con el presente proyecto.

Tabla 7 - Criterio de puntaje para Benchmark

Puntaje	Normativo	Profundidad Específica	Sector Empresas	Actualidad (>2013)	Relevancia
1	No es normativo	Profundidad general	Otro sector	Menor a 2013	Relacionado parcialmente a Investigación
2	Es Normativo	Profundidad específica (salud)	Sector Empresas	Mayor a 2013	Relacionado directamente a Investigación

Construimos los controles, categorías y sub-categorías del modelo considerando la estructura de NIST CF y NIST PF.(National Institute of Standards and Technolgy, 2014, 2020) Asimismo, elaboramos una categoría adicional para controles específicos de Sector Salud. Utilizamos frameworks de NIST, debido a que tienen alta compatibilidad con los elementos utilizados para la construcción del modelo y que se muestran en la Tabla 8.

Tabla 8 - Elementos utilizados para la contrucción del Modelo

Enfoque	**Herramienta**	
	Tipo	***Nombre***
Ciberseguridad	Framework	NIST CSF
	Modelo de Madurez	C2M2 v1.1
	Controles	NIST 800-53 SP
Privacidad	Modelo de Madurez	AICPA/CICA Privacy Maturity Model
	Framework	NIST PF
	Normativa	Reglamento de Ley de Protección de Datos Personales (Ley N° 29733)
Salud	Normativa	Reglamento de Registro Nacional de Historias Clínicas Electrónicas (Ley N° 30024)
	Normativa	Health Insurance Portability and Accountability Act (HIPAA)

Cabe resaltar que decidimos considerar las normativas locales como Ley N°29733 y N°30024, debido a que el caso de estudio se sitúa en Perú. El resultado final del modelo es un indicador de madurez que indica el estado actual de la organización.

Construimos los componentes considerando los Enablers que propone COBIT 5, debido a que permiten identificar el funcionamiento óptimo de Gobierno y Gestión de TI.(Ti et al., 2012)

Los criterios elaborados se muestran en la Tabla 9

.

Tabla 9 - Criterios de medición

Criterios	**Definición**
Políticas y procedimientos	Define comportamiento esperado con respecto a la práctica para la gestión diaria.
Roles y responsabilidades	Define responsables clave para completar con éxito las actividades y tomar decisiones correctas.
Alcance de implementación del control	Define el nivel de implementación del control o práctica.
Informes	Define toda la información producida y utilizada por la organización.
Procesos	Define prácticas organizadas en conjunto y actividades para lograr objetivos. Permite el logro de objetivos relacionados con TI.
Automatización	Define el nivel de automatización de control o práctica.

4.1.3 Categorías

El agrupamiento de controles sigue una estructura de categorías. Esto permite que la organización pueda enfocar sus esfuerzos según la categoría que se desee mejorar. Las categorías elaboradas se pueden observar en la siguiente tabla.

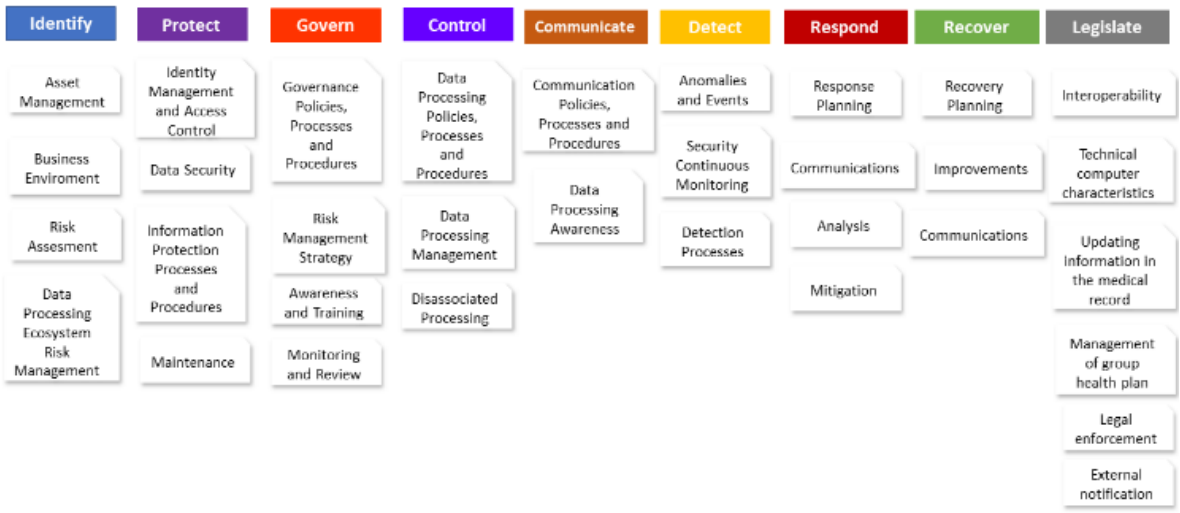
Tabla 10 - Categorías

Categorías	**Enfoque**
Identificar	Desarrollar un entendimiento a nivel organizacional respecto a los riesgos de ciberseguridad, privacidad y salud presentes en las actividades de la empresa y el procesamiento de datos
Controlar	Desarrollar e implementar actividades que permitan a la organización controlar riesgos de privacidad
Comunicar	Desarrollar e implementar actividades que permitan a la organización asegurar el entendimiento y dialogo con respecto al procesamiento de datos y riesgos de privacidad.
Proteger	Garantizar el procesamiento seguro de datos y entrega de servicios críticos
Detectar	Desarrollar actividades para reconocer el suceso de un evento de ciberseguridad
Responder	Desarrollar e implementar actividades a efectuar al detectar un incidente de ciberseguridad
Recuperar	Desarrollar e implementar actividades y métodos de resiliencia y restauración de funciones posterior a un incidente de ciberseguridad
Gobernar	Desarrollar e implementar actividades que permitan la alineación de las prioridades de la gestión de riesgos organizacional con los riesgos de privacidad dentro de la estructura de gobierno organizacional.
Legislar	Desarrollar actividades que midan el cumplimiento con respecto a las leyes y regulaciones aplicadas a ciberseguridad y privacidad en el entorno de salud

4.1.4 Subcategorías

D de cada categoría se agrupan subcategorías, las cuales contienen los controles. Con la finalidad de que el modelo realice una evaluación y diagnóstico de manera integral y holística, se definieron 33 subcategorías. Las subcategorías elaboradas se pueden observar en la siguiente figura.

Figura 3 - Subcategorías elaboradas



4.1.5 Controles

Los controles han sido agrupados en las subcategorías definidas previamente. El objetivo es utilizar los niveles de capacidad obtenidos por control para definir el nivel por subcategoría y categoría mediante un promedio simple. En total se elaboraron 172 controles agrupados en tres elementos: Ciberseguridad, Privacidad y Normativas de gestión de datos de salud. Esta agrupación se pude observar en la siguiente figura.

Figura 4 - Controles

Los controles integrados fueron elaborados resaltando que algunos consideraban el mismo alcance en distintos frameworks, eran ambiguos y no abarcaban el alcance buscado para nuestra propuesta. Teniendo en cuenta esto, y con el objetivo de no tener redundancia a nivel de controles y obtener una evaluación integral, la elaboración de controles siguió las siguientes fases:

- Identificar controles que abarcan el mismo alcance y controles que se repiten.
- Depurar controles repetidos y con alcance similar
- Adaptar definición de controles al enfoque planteado para el modelo
- Integrar controles de frameworks seleccionados considerando un enfoque en Ciberseguridad y Privacidad aplicados al Sector Salud.
- Ordenar controles por categorías y subcategorías

4.1.6 Artefactos

4.1.6.1 Herramienta de diagnóstico

La herramienta desarrollada permite una visión integral del estado actual de la organización con respecto a Ciberseguridad, Privacidad y Gestión de Datos de Salud. La herramienta se conforma de un grupo de controles, evaluados por criterios, que al responderse con el nivel

de cumplimiento del control se obtiene el nivel de madurez a nivel de Categoría y Subcategoría.

4.1.6.2 Matriz de controles

La matriz elaborada contiene los controles del modelo, señalando su pertenencia con respecto a Ciberseguridad, Privacidad y Gestión de Datos de Salud. Esto permite una identificación clara del alcance de cada categoría y subcategoría al igual que facilita futuras actualizaciones a los componentes del modelo.

4.1.6.3 Reporte final

El modelo contempla un reporte final que representa la situación actual de la organización en base al diagnóstico realizado. Tiene un nivel de madurez en cada categoría, la justificación de estos niveles y recomendaciones para mejorar el resultado.

4.2 Escala de madurez

Se estableció una escala con un nivel 1 como nivel básico y nivel 5 como el nivel más alto de madurez. Esto se puede observar en la Tabla 7.

Tabla 11 - Escala de Madurez

NIVELES					
CRITERIO	**Nivel 1 - Básico**	**Nivel 2 - En Desarrollo**	**Nivel 3 - Definido**	**Nivel 4 - Diferenciado**	**Nivel 5 - Mejora continua**
Políticas y procedimientos	Ausencia de políticas y procedimientos	Políticas y procedimientos limitados e incompletos	Política y procedimientos integrales definidos y publicados	Política y procedimientos son publicados y revisados en una frecuencia continua	Revisión y mejora continua de la política. Se accionan planes y mejoras en el documento y se realizar seguimiento en la implementación de las políticas publicadas.
Roles y responabilidades	No hay definición de roles y responsabilidades	Roles parcialmente definidos	Roles y responsabilidades determinados y definidos	Roles y responsabilidades son revisadas en una frecuencia establecida	Roles y responsabilidades revisados continuamente
Alcance de implementación del control	Sin alcance	Limitado	Activos core	Alcance revisado en una frecuencia establecida	Revisión y mejora continua del alcance
Informes	No se realizan informes	Limitado	Informes definidos	Informes revisados y enviados a alta gerencia en una	Requerimientos de informes revisados y

				frecuencia establecida	actualizados continuamente
Procesos	Proceso impredecible y con poco control	Procesos caracterizados	Procesos estandarizados y repetibles	Proceso medido y controlado en una frecuencia establecida	Los procesos son enfocados a la mejora continua y automatización
Automatización	Controles manuales en su totalidad	Controles manuales	Controles manuales	Presencia de controles manuales y automatizados	Automatización de controles y mejora continua para cumplir cobertura total

4.3 Especificaciones por nivel de componente

1) Nivel 1 - Básico: La organización cuenta con procesos impredecibles y con poco control. Existe ausencia de políticas, procedimientos, y definición de roles y responsabilidades. Asimismo, no existe un alcance claro en la implementación de controles de protección, los controles son manuales en su totalidad y no se realizan informes.

2) Nivel 2 - En Desarrollo: La organización cuenta con procesos caracterizados. Las políticas y procedimientos son limitados e incompletos y los roles están parcialmente definidos. Asimismo, el alcance de implementación de controles es limitado, los controles son manuales y los informes son limitados.

3) Nivel 3 - Definido: La organización cuenta con procesos estandarizados y repetibles. Las políticas y procedimientos se encuentran integrados, definidos, publicados y los roles y responsabilidades están determinados y definidos. Asimismo, el alcance de implementación de controles abarca los activos core, los controles son manuales y se realizan informes definidos.

4) Nivel 4 - Diferenciado: La organización cuenta con procesos medidos y controlados en una frecuecia establecida. Las políticas y procedimientos son publicados y revisados en una frecuencia continua, y los roles y responsabilidades son revisados en una frecuencia estalecida. Asimismo, el alcance de implementación de controles es revisado en una

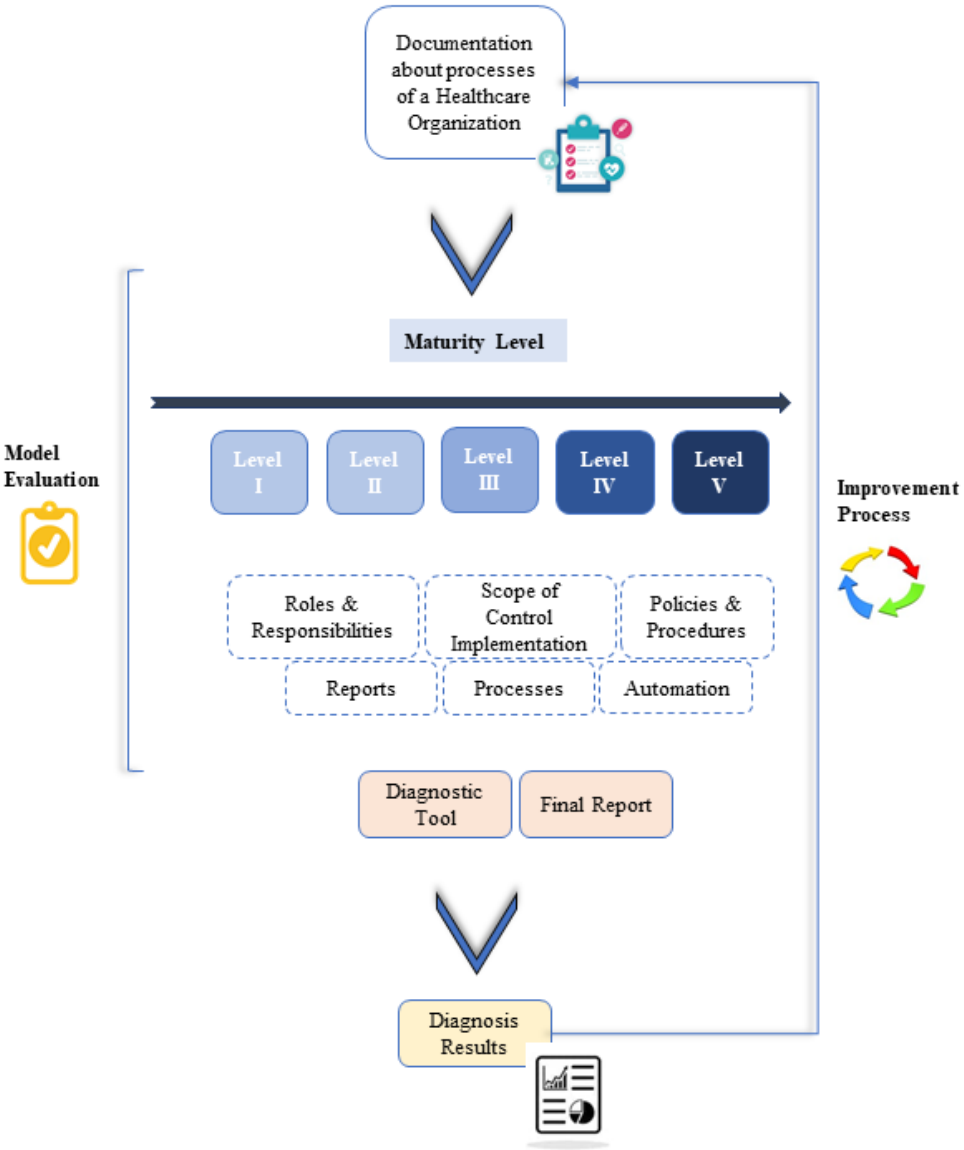
frecuencia establecida. Existen controles manuales y automatizados, y los informes son revisados y enviados a la alta gerencia en una frecuencia establecida.

5) Nivel 5 - Mejora Continua: Los procesos de la organización son enfocados a la mejora continua y automatización. Existen revisiones y mejora continua de las políticas. Se accionan planes y mejoras de las políticas y se realiza seguimiento durante la implementación de las políticas publicadas. Los roles y responsabilidades son revisados continuamente. Asimismo, el alcance de implementación de controles es revisado y mejorado continuamente. Los controles se encuentran automatizados y son mejorados continuamente para cumplir cobertura total. Los requerimientos de informes son revisados y actualizados continuamente.

El uso del modelo contempla 3 etapas: En la etapa de análisis, la información recolectada de los procesos se clasifica de acuerdo a una categoría correspondiente del control. Con ello, los procesos serán evaluados a nivel de control y componente. Luego, en la etapa de diagnóstico, el evaluador determina el nivel de madurez. Finalmente, con el diagnóstico, el evaluador puede identificar y elaborar propuestas de mejora de manera integrada. Asimismo, el modelo propuesto cuenta con artefactos que permiten al usuario realizar el diagnóstico de manera sencilla.

4.3.1 Modelo de Madurez propuesto

Figura 5 - Modelo de Madurez Propuesto



4.4 Validación

Fue realizado mediante el análisis del proceso de backups de la Clinica “A” utilizando 7 controles aplicables de nuestro modelo. Los pasos de Implementación fueron los siguientes:

- Adquirir la documentación del proceso: Enviamos una solicitud formal a la clínica para recibir la documentación relacionada a sus procesos internos
- Selección de Escenario: Seleccionamos un proceso el cual nos permita evaluar múltiples aspectos del modelo y comparar los resultados con sus componentes originales.

- Implementación de Modelo de Madurez: El modelo es utilizado para evaluar el proceso seleccionado, considerando los controles actuales y sus componentes
- Obtener Nivel de Madurez: Concluida la implementación, obtenemos los niveles de madurez

Según la información obtenida, podemos apreciar el valor de un análisis el cual considera aspectos de Ciberseguridad, Privacidad y Gestión de Datos de Salud de forma completa. El modelo de madurez facilito el control, monitoreo y cumplimiento de controles, prácticas y regulaciones. Encontramos que el escenario seleccionado presenta una madurez de nivel "en progreso" (nivel 2). Esto indica que el hospital privado "A" aún tiene aspectos por mejorar. Adicionalmente, observamos los resultados a nivel de control en la Tabla 12

Tabla 12 - Resultados de implementación

Categoría	Subcategoría	Control	Nivel
Gobernar	Politicas, procesos y procedimientos de gobernancia	GV.PO-1	2
	Politicas, procesos y procedimientos de gobernancia	GV.PO-4	2
Gobernar	Revision y monitoreo	GV.MT-5	2
Proteger	Seguridad de datos	PR.DSI-4	2
Proteger	Procesos y procedimientos de proteccion de informacion	PR.IPI-3	3
		PR.IPI-7	3
Legislar	Interoperabilidad	LE.IN-3	1

Los resultados indican que la necesidad principal del hospital privado es el de preparar y estandarizar los procesos puesto que estos no han logrado un nivel de capacidad de 3 en 4 controles. Asimismo, necesitan mejorar el cumplimiento de regulaciones de salud porque es el único control de nivel 1 – Basico.

Además, se entregó un formulario de evaluación considerando un estudio previo para la evaluación de modelos de madurez que abarca en sus criterios de evaluación principios de diseño, desarrollo y evaluación de los modelos de madurez. Asimismo, se elaboraron 7 métricas para medir la efectividad del modelo.(Salah et al., 2014)

Este formulario fue utilizado para comprobar el nivel de satisfacción con respecto al uso del modelo y componentes. Los conceptos y métricas elaboradas se pueden observar en la siguiente tabla.

Tabla 13 - Conceptos y métricas de Evaluación

Concepto	Métrica
La normativa de salud presente en el modelo es relevante para la organización	Relevancia
Los niveles de madurez presentados son suficientes para la descripción de madurez de cada categoría	Suficiencia
No existen similitudes en las descripciones de los niveles de la escala de madurez	Precisión
Los controles son relevantes a las categorías y subcategorías a las cuales pertenecen	Relevancia
Los controles cubren todos los aspectos presentes en sus categorías y subcategorías	Alcance
Los controles son claramente distintos	Precisión
Los procesos y prácticas están asignados a un nivel de madurez apropiado	Precisión
Los niveles de madurez se entienden	Comprensión
El método de evaluación se entiende	Comprensión
La documentación brindada se entiende	Comprensión
El sistema de calificación es fácil de usar	Facilidad de uso
La herramienta es fácil de usar	Facilidad de uso

La documentación del modelo es fácil de utilizar	Facilidad de uso
El modelo de madurez es útil para la toma de decisiones	Practicidad
El modelo de madurez es útil para ser utilizado en la industria	Practicidad

Se estableció que la evaluación sea calculada en un rango de 1 a 5, siendo el significado de estos: “Muy en desacuerdo” y “Muy de acuerdo” respectivamente.

CAPÍTULO 5 - RESULTADOS DEL PROYECTO

En el presente capítulo se detallan los resultados obtenidos al implementar el modelo de madurez propuesto en una organización de salud.

5.1 Organización

La Clínica Privada “A” fue la organización de salud donde se validó el modelo. Esta clínica es un servicio ofrecido por la Cooperativa de Servicios “B” y al ser el servicio más lucrativo de la cooperativa, B necesita asegurar que el funcionamiento de esta sea el mejor. Además, la misión de “A” es la satisfacción de las necesidades de salud de sus miembros y comunidad. Por lo que está en sus intereses mejorar el funcionamiento y calidad de sus procesos. Por estos motivos, la aplicación de nuestro modelo en este escenario será ideal. Nuestra solución identificará las carencias y fortalezas actuales de “A”, permitiendo elaborar estrategias que mejoren y mantengan la calidad de los servicios que brinda.

5.2 Implementación

La implementación del proyecto siguió los siguientes pasos:

- Obtener documentación de procesos: Se solicitó de manera formal los procesos internos de la clínica.
- Recepción de documentación: Se obtuvo la documentación solicitada para poder comenzar el análisis de los procesos con el modelo.
- Selección de escenario aplicable: Se escogió un proceso que nos permita evaluar todos los aspectos del modelo y posteriormente comparar el resultado con otros modelos para validar su eficacia.
- Utilizar modelo de madurez: Se utilizó el modelo para la evaluación del escenario seleccionado a nivel de implementación de controles y componentes.
- Obtener nivel de madurez: Luego de utilizar el modelo se obtuvo los resultados de madurez.

5.3 Resultados

Se realizó una comparación utilizando nuestros criterios de medición entre los controles utilizados en nuestro modelo y las fuentes en NIST Cybersecurity Framework, NIST Privacy Framework and the Health Insurance Portability and Accountability Act (HIPAA) para confirmar la integración coherente entre las fuentes. Consideraríamos la integración como exitosa si el resultado se encontraba en el margen de error de ±1 punto. Algunos de los resultados se pueden observar en las tablas 14, 15 y 16.

Tabla 14 - Comparación de controles 1

ID	Fuente	Criterio de Medición					
		P&P	**R&R**	**AIC**	**Reportes**	**Procesos**	**Automatización**
PR.IPI-3	Modelo Propuesto	4	3	4	3	2	3
PR.IP-4	NIST CSF	4	3	4	3	2	3

Tabla 15 - Comparación de controles 2

ID	Fuente	Criterio de Medición					
		P&P	**R&R**	**AIC**	**Reportes**	**Procesos**	**Automatización**
GV.PO-P5	Modelo Propuesto	2	2	2	1	1	2
164.524(a)(1),(b)(1), (b)(2),(c)(2),(c)(3), (c)(4),(d)(1),(d)(3)	HIPAA	2	2	2	1	1	2

Tabla 16 - Comparación de controles 3

ID	Fuente	Criterios de Medición					
		P&P	**R&R**	**AIC**	**Reportes**	**Procesos**	**Automatización**
PR-IPI-7	Modelo Propuesto	4	3	4	3	2	3
PR.IP-9	NIST CSF	4	3	4	2	2	3

Como se observa, los resultados obtenidos en cada criterio de medición fueron los mismos para PR.IPI-3 y GV.PO-4 mientras que existió una mínima diferencia en el criterio de "Reports" para PR-IPI-7. Esta diferencia se encuentra dentro del margen de error establecido por lo cual el resultado sigue siendo válido.

En base a la información recogida, se pudo observar que un análisis que considere los aspectos de Ciberseguridad, Privacidad y Gestión de Datos de Salud de manera integrada es valioso. El modelo de madurez facilitó el control, monitoreo y cumplimiento de controles, prácticas y normativas. Encontramos que el escenario seleccionado presentaba un nivel de madurez en desarrollo (nivel 2). Lo cual nos indica que la clínica "A" tiene aspectos por

mejorar. Asimismo, a nivel de controles, podemos observar los resultados en la siguiente tabla.

Tabla 17 - Diagnóstico

Categoría	**Subcategoría**	**Control**	**Nivel**
Gobernar	Politicas, procesos y procedimientos de gobernancia	GV.PO-1	2
	Politicas, procesos y procedimientos de gobernancia	GV.PO-4	2
Gobernar	Revision y monitoreo	GV.MT-5	2
Proteger	Seguridad de datos	PR.DSI-4	2
Proteger	Procesos y procedimientos de proteccion de informacion	PR.IPI-3	3
		PR.IPI-7	3
Legislar	Interoperabilidad	LE.IN-3	1

Por otra parte, se elaboró a nivel de control un gráfico para la toma de decisiones. Es importante señalar que cada gráfico corresponde a un control implementado en el proceso. Podemos observar los resultados en las siguientes figuras:

Tabla 18 - Dashboard de Revisión y Monitoreo

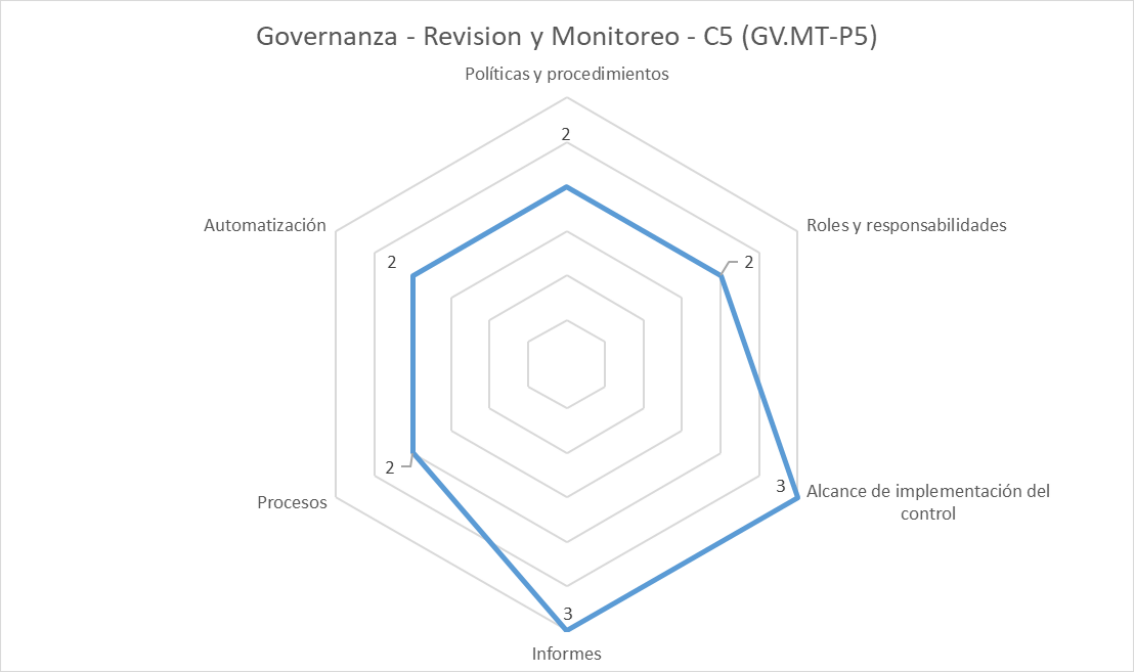


Tabla 19 - Dashboard de Procesos, políticas y procedimientos

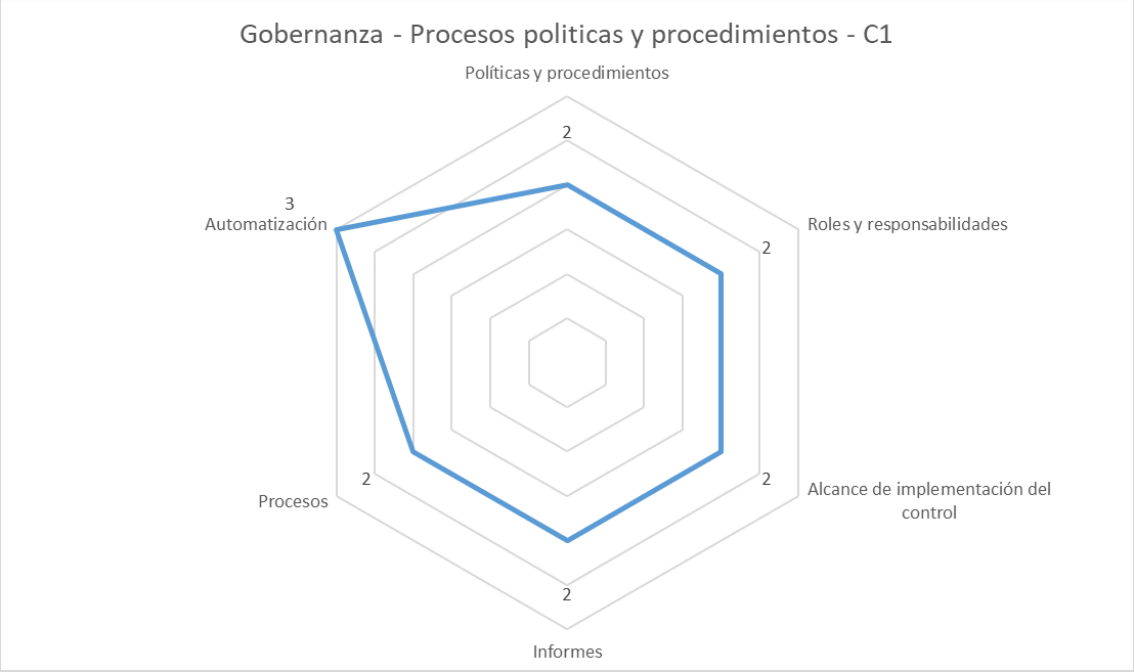


Tabla 20 - Dashboard de Seguridad de Datos

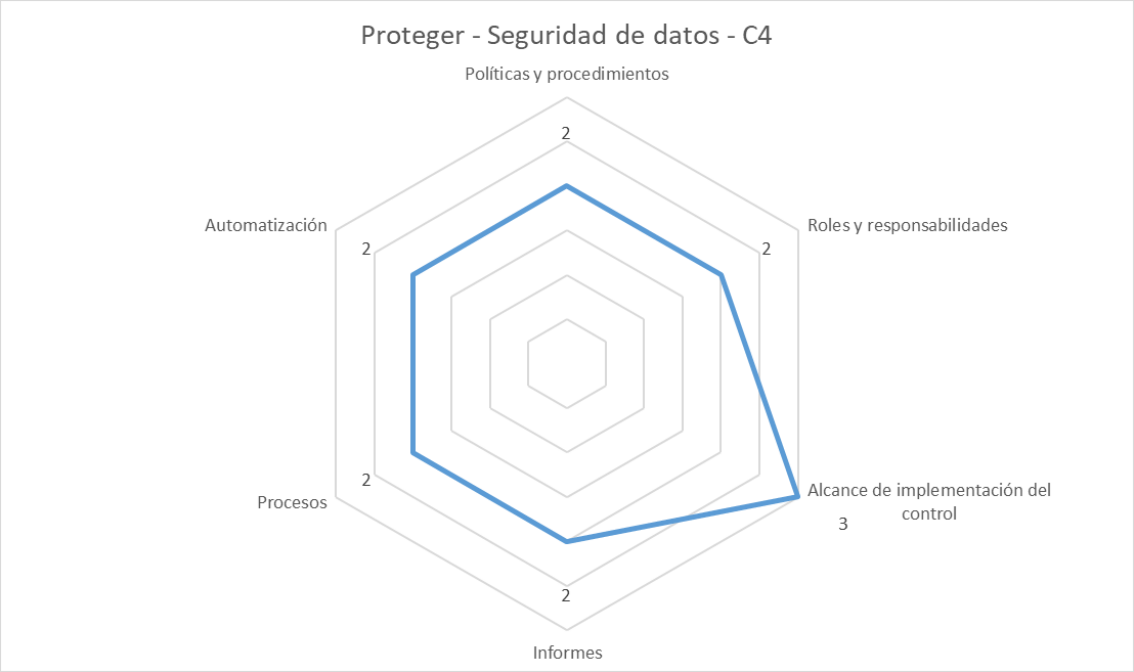


Tabla 21 - Dashboard de Procesos y procedimientos de protección de información

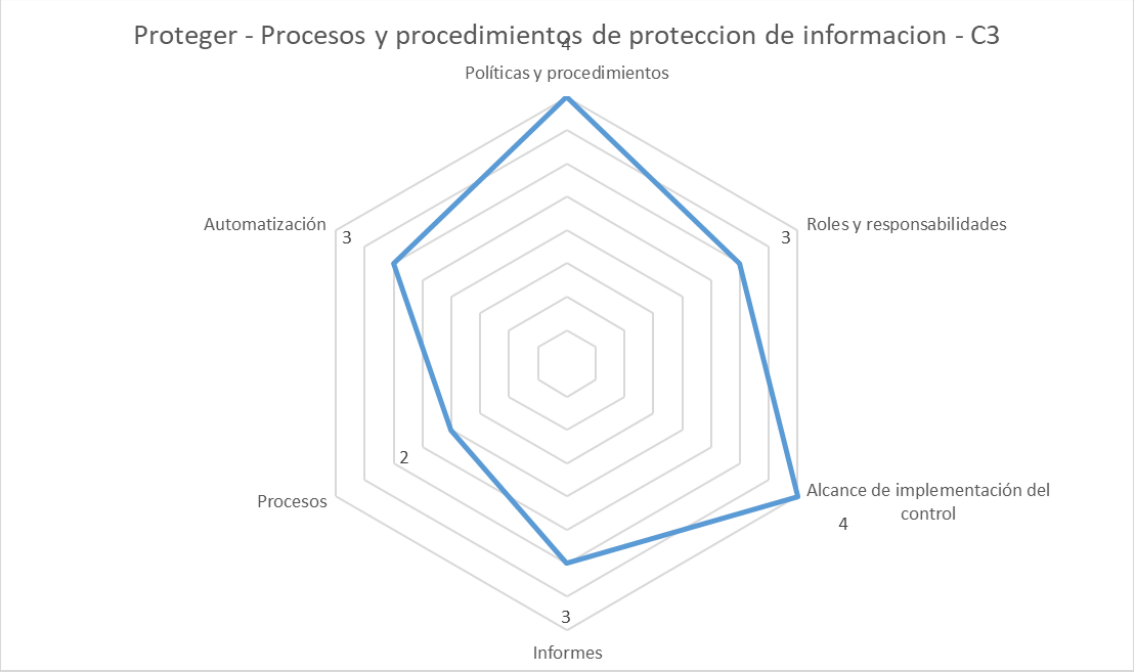
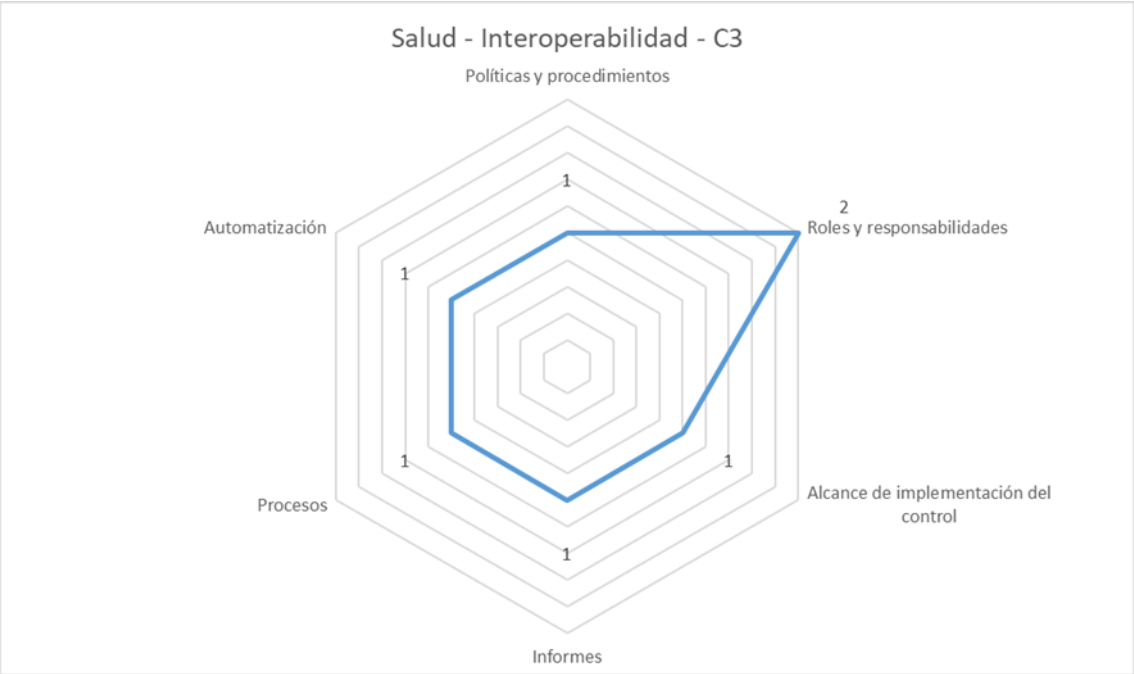


Tabla 22 - Dashboard de Interoperabilidad



Los resultados indican que es importante mejorar el cumplimiento de normativas de salud, dado que es el único control en Nivel 1. Los estudios futuros deberían tener como objetivo ampliar el alcance de la evaluación a múltiples procesos al igual que mantener un contacto con la empresa para obtener un nivel de detalle más profundo. Asimismo, podría alojarse la herramienta del modelo en una aplicación para mayor comodidad y portabilidad.

Por otra parte, los resultados del formulario de evaluación se pueden observar en la siguiente tabla.

Tabla 23 - Resultados de formulario

Métrica	**Puntaje**
Suficiencia	5
Relevancia	4.5
Precisión	4.6
Alcance	4
Comprensión	5
Facilidad de uso	4.6
Practicidad	5

En base a esos resultados puede afirmar la validez del modelo, debido a que recibió un puntaje promedio de 4,6. Esto significa que el modelo brinda valor. Se resalta que las observaciones brindadas por la clínica indican una preferencia por normativas orientadas al contexto peruano, siendo la sugerencia de dicha clínica la de incluir más controles centrados en normativas peruanas a la categoría de salud.

5.4 Plan de continuidad

Se desarrolló un plan de continuidad para asegurar en el tiempo la relevancia del modelo de madurez en ciberseguridad para empresas de servicio en el sector salud mediante actualizaciones al contenido, considerando de los avances en ciberseguridad, privacidad y normativa de salud.

El plan permite garantizar lo siguiente:

- Asegurar la relevancia del modelo mediante la actualización de su contenido
- Mantener a la solución competitiva contra otros modelos de madurez
- Mantener la integración de ciberseguridad, privacidad y salud correcta para así mantener la ventaja competitiva del modelo

El plan de continuidad utiliza los roles definidos en ITIL, los cuales se identifican de la siguiente manera

- Solicitante del cambio

Rol asignado a la persona que solicita el cambio al modelo de madurez. Estos pueden ser cambios a controles ya existentes o la agregación de nuevos controles a las subcategorías existentes

- Gestor de cambios

Controla los cambios, asegurando que causen la menor disrupción posible al uso de la herramienta. Puede permitir cambios pequeños al modelo como la clarificación de algún concepto de los controles existentes

En el caso los cambios requieran la agregación de controles, modificación o eliminación de un control existente o la creación de nuevas categorías o subcategorías, este requerirá el permito del comité de cambios.

- Comité de cambios

Equipo que analiza las solicitudes de cambio de alto impacto y determina la aprobación o desaprobación de estas. Debe estar conformado de expertos que representen cada área principal de la empresa.

- Comité de cambios de emergencia

Comité que realiza las funciones del comité de cambios en el evento que estos se encuentren no disponibles para la toma de decisiones.

- Implementador del cambio

Expertos encargados en implementar el cambio aprobado por el comité de cambio

Asimismo, los procesos definidos en este plan de continuidad son los siguientes

1. Emisión de solicitud de cambio

El Solicitador de cambio emite una solicitud a la gestión de cambio, especificando obligatoriamente los componentes del modelo afectados, la urgencia y el cambio a ser aplicado al modelo. La solicitud de cambio es recibida por el gestor de cambio que evalúa si es un cambio de baja magnitud que él pueda aprobar/desaprobar o si requiere del comité de cambios.

2. Evaluación de solicitudes de cambio

El comité de cambio, evaluara el cambio según el impacto de este, el tiempo que costara implementarlo y la relevancia de dicho cambio. En el caso el comité de cambio no se encuentre disponible, el comité de cambios de emergencia será quien evalué dicha solicitud.

3. Aprobación de solicitud

El comité que realizo la evaluación finalmente decide si la solicitud será aprobada y ejecutada o rechazada debido a alguna carencia en los criterios de evaluación

4. Programación de cambio

El cambio es programado para ser implementado dentro de una fecha específica por el implementador de cambios y el gestor de cambios.

5. Implementación de cambio

El implementador de cambio con la ayuda del gestor de cambios, implementan el cambio solicitado y actualizando la versión del modelo de madurez.

6. Revisión de cambio implementado

El solicitador de cambio evalúa que el cambio solicitado se halla implementado correctamente y el gestor de cambio evalúa por un periodo de tiempo el impacto causado por el cambio en caso se necesite realizar un retroceso del cambio.

Finalmente, los indicadores desarrollados para medir el éxito de los cambios son los siguientes.

- Porcentaje de cambios implementados con éxito.

$$X = \frac{N^o\ de\ cambios\ implementados\ con\ éxito}{N^o\ de\ cambios\ solicitados}$$

- Porcentaje de cambios no autorizados.

$$z = \frac{N^o\ de\ cambios\ no\ autorizados}{N^o\ de\ cambios\ solicitados}$$

- Tiempo promedio para implementar un cambio.

$$Tiempo\ promedio\ para\ implementar\ un\ cambio = (\sum_{t=1}^{N} X_t)/N$$

- Porcentaje de cambios de emergencia

$$z = \frac{N^o\ de\ cambios\ de\ emergencia}{N^o\ de\ cambios\ solicitados}$$

- Porcentaje de cambios incorrectos implementados

$$z = \frac{N^o\ de\ cambios\ incorrectos}{N^o\ de\ cambios\ autorizados}$$

Se recomienda revisar y actualizar los controles del modelo según la versión más reciente de NIST CSF, NIST Privacy Framework y Ley HIPAA. Esto garantizará su relevancia y mantendrá eficiencia.

CAPÍTULO 6 - GESTIÓN DEL PROYECTO

En este capítulo se explica detenidamente la gestión realizada a lo largo del proyecto con el fin de culminar correctamente.

6.1 Ciclo de Vida del Proyecto

Tabla 24 - Ciclo de vida del proyecto

Fase	Actividades principales	Criterio de entrada	Criterio de salida
Incepción	Elaboración de Project Charter	Inicio del proyecto	Project Charter presentado y aceptado
Planificación	Elaboracion de Benchmark de soluciones y Documento Integrador de controles	Análisis de soluciones actuales de ciberseguridad, privacidad y normativa de salud	Exposición del cumplimiento de indicadores de éxito 1,2,3,4 ante comite
Implementación	Elaboracion y validación de herramienta Certificacion de entregables realizados	Elaboración de la herramienta del proyecto	Validacion de herramienta del modelo y obtención de certificación IT - Service
Planeamiento de continuidad	Elaboracion del plan de continuidad	Desarrollo del plan de continuidad	Plan de continuidad completo
Aporte adicional	Elaboracion de Taxonomia basada en ACM Cybersecurity 2020 Curricular Framework	Incepción de aporte adicional a proponer	Taxonomía aceptada Presentación final del proyecto aceptada.

6.2 Enfoques de Desarrollo

Tabla 25 - Enfoques de desarrollo

Entregable	Enfoque de desarrollo
Benchmark de soluciones actuales	• Alcance adaptable • Método iterativo de desarrollo
Justificación de selección de soluciones para integrar en el modelo	• Alcance estable • Metodo Iterativo
Documento comparativo de controles integrados	• Alcance estable • Método incremental
Documento de estructura del modelo de madurez	Alcance estable
Escala de madurez	• Alcance estable • Metodo Iterativo
Herramienta de evaluación de madurez	• Alcance estable • Metodo Iterativo
Certificación de IT - Services	Alcance estable
Plan de continuidad	• Alcance estable • Metodo Iterativo
Taxonomía de ciberseguridad basada en ACM Cybersecurity 2020	• Alcance adaptable • Método iterativo de desarrollo

6.3 Cronograma del proyecto

Tabla 26 - Cronograma del proyecto

Hito	Fecha	Documentos a presentar:
Sustentación del proyecto al 25% de completo con el Portfolio Manager	29/04/2019	• Benchmark de soluciones • Justificación de selección de soluciones para integrar en el modelo
Sustentación del proyecto al 25% de completo ante el comité	15/05/2019	• Benchmark de soluciones • Justificación de selección de soluciones para integrar en el modelo

Sustentación del proyecto al 50% de completo ante el Portfolio Manager	28/06/19	• Documento comparativo de controles integrados • Documento de estructura del modelo de madurez
Sustentación del proyecto al 50% de completo ante el comité	01/07/19	• Documento comparativo de controles integrados • Documento de estructura del modelo de madurez
Sustentación del proyecto al 75% de completo ante el Portfolio Manager	24/09/19	• Escala de madurez • Herramienta de evaluación de madurez
Validación de la herramienta del proyecto con el Cliente	02/10/19	• Herramienta de evaluación de madurez
Emisión de certificado de IT - Services	07/10/2019	• Certificación de IT - Services
Sustentación del proyecto al 75% de completo ante el comité	07/10/2019	• Escala de madurez • Herramienta de evaluación de madurez
Sustentación de la taxonomía propuesta al 100% de completo ante el Portfolio manager	04/05/2020	• Taxonomía de ciberseguridad basada en ACM
Sustentación de la taxonomía propuesta al 100% de completo ante el comité	15/05/2020	• Taxonomía de ciberseguridad basada en ACM
Sustentación final del proyecto ante el Portfolio Manager	27/05/2020	• Plan de continuidad
Sustentación final del proyecto ante el comité	03/06/2020	• Plan de continuidad

6.4 Entregables

Tabla 27 - Entregables

Entregable	Método de aprobación
Benchmark de soluciones actuales	• Certificación por parte de la empresa IT Service • Aprobación por parte del Product owner (Acta de aceptación)
Justificación de selección de soluciones para integrar en el modelo	• Certificación por parte de la empresa IT Service • Aprobación por parte del Product owner (Acta de aceptación)
Documento comparativo de controles integrados	• Certificación por parte de la empresa IT Service • Aprobación por parte del Product owner (Acta de aceptación)
Documento de estructura del modelo de madurez	• Certificación por parte de la empresa IT Service • Aprobación por parte del Product owner (Acta de aceptación)
Escala de madurez	• Certificación por parte de la empresa IT Service • Aprobación por parte del Product owner (Acta de aceptación)
Herramienta de evaluación de madurez	• Aprobación por parte del Product owner (Acta de aceptación)
Certificación de IT - Services	• Resultado de la aprobación por parte de la empresa IT Service
Plan de continuidad	• Certificación por parte de la empresa IT Service • Aprobación por parte del Product owner (Acta de aceptación)
Taxonomía de ciberseguridad basada en ACM Cybersecurity 2020	• Certificación por parte de la empresa IT Service • Aprobación por parte del Product owner (Acta de aceptación)

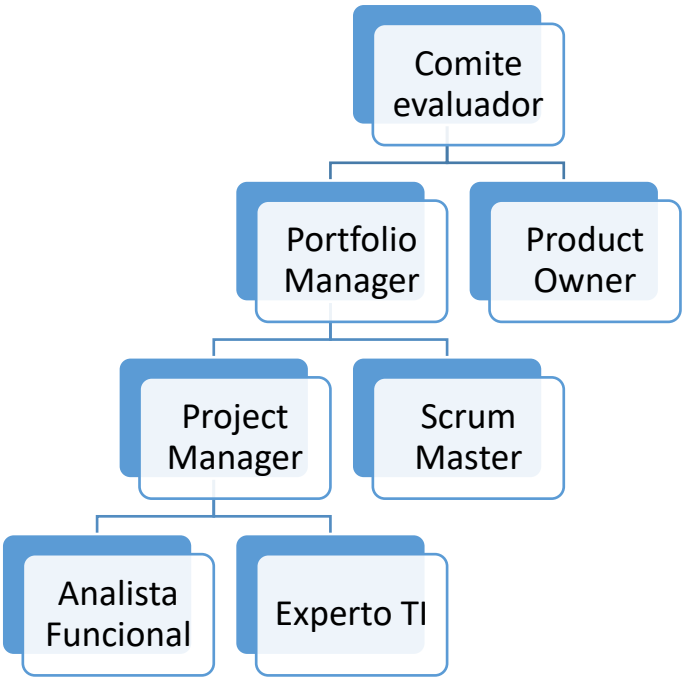
6.5 Gestión de recursos humanos

Tabla 28 - Miembros del Equipo y Estimaciones

Rol	Cantidad	Nivel de pericia
1. Project manager	1	• Conocimientos en gestión de proyecto basado en buenas prácticas. • Capacidad de gestionar y controlar el progreso de un proyecto
2. Scrum Master	1	• Conocimientos en metodología Scrum y sus múltiples componentes. • Capacidad de organización de personal y recursos
3. Portfolio Manager	1	• Conocimiento en gestión de proyectos • 5+ años de experiencia • Capacidad de garantizar calidad en las presentaciones del proyecto
4. Product Owner	1	• Conocimiento en Ciberseguridad y modelos de madurez • 5+ años de experiencia • Conocimiento de nuevas tendencias con respecto a ciberseguridad y modelos de madurez
5. Analista funcional	42	• Comprensión lectora • Capacidad de análisis de literatura académica
6. Experto TI	4	• Capacidad de asegurar la calidad de entregables relacionados a modelos de madurez.

6.6 Organigrama del Proyecto

Figura 6 - Organigrama Del Proyecto



6.7 Roles y Responsabilidades

Figura 7 - Roles y responsabilidades

Rol	Responsabilidad	Autoridad
1. Analista funcional	• Elaboración de resúmenes de literatura académica	• Documentos elaborados deben ser aprobados por Project Manager
2. Experto TI	• Certificación de entregables brindados por el Project Manager	• Certificación de entregables • Aprueba/Desaprueba entregables brindados
3. Portfolio Manager	• Orientar al equipo del proyecto con respecto a los aspectos de gestión de proyecto	• Aprueba/Desaprueba exposición ante comité • Aprueba/Desaprueba documentación del proyecto
4. Product Owner	• Orientar al equipo del proyecto con respecto a los aspectos de Ciberseguridad y Modelos de madurez cubiertos en el proyecto	• Aprueba/Desaprueba entregables del proyecto • Aprueba/Desaprueba objetivos específicos del proyecto

6.8 Gestión de Riesgos

Se optó por dos tipos principales de categorización: Riesgo interno y Riesgo externo.

- Riesgo Interno: Proveniente del equipo de proyecto o recursos adquiridos para la elaboración del proyecto.
- Riesgo Externo: Proveniente de factores externos al equipo del proyecto como los grupos de interés, entorno político, económico y social del proyecto.

6.9 Frecuencia y Tiempo

Los riesgos del proyecto serán verificados al inicio de cada Sprint (duración 3 semanas), realizando los cambios necesarios a los riesgos ya identificados y agregando nuevos riesgos en caso sea necesario.

6.10 Seguimiento de Riesgos

Los riesgos encontrados al igual que las contingencias preparadas serán registrados en un archivo Excel que permitirá conservar un listado y control de versiones de los riesgos relacionados al proyecto. Estos riesgos serán verificados con el Portfolio manager durante una de las dos sesiones semanales ya programadas.

6.11 Gestión de comunicaciones

Stakeholder	Información	Método	Frecuencia	Remitente
Portfolio Manager	Se comunican los documentos de gestión del	Las sesiones con el portfolio manager son	Dos sesiones por semana los días Lunes y	Henry Bryan Perez Navarro

	proyecto, los avances semanales del proyecto, la realización de las actividades del sprint Toda esta información es transmitida de forma formal, detallando lo realizado en cada sesión con el portfolio manager y los resultados de lo avanzado fuera de las sesiones Se presentan además las presentaciones de los proyectos para recibir el permiso de	realizadas mediante la plataforma Blackboard Collaborate y los reportes de actividades realizadas y documentos de gestión son enviados mediante formularios brindados por el portfolio manager	Miercoles entre las 4:00 pm y 7:00 pm	y Humberto Luis Salcedo Jara

	exponer ante el comité			
Product Owner	Se comunican los avances realizados con respecto al producto y los entregables principales del proyecto. Se utiliza lenguaje formal para comunicar dichos entregables.	Las sesiones con el portfolio manager son realizadas mediante la plataforma Blackboard Collaborate donde los resultados son presentados y las observaciones recibidas	1 sesión por semana dependiendo de la disponibilidad del Product Owner	Henry Bryan Perez Navarro y Humberto Luis Salcedo Jara
Comité Evaluador	Se presentan los resultados del proyecto al 25%, 50%, 75% y 100% del proyecto	Los resultados son presentados mediante presentaciones y un DVD con todos los entregables y materiales elaborados durante el	4 exposiciones en intervalos de 3 meses decididos por el comité evaluador	Henry Bryan Perez Navarro y Humberto Luis Salcedo Jara

		proyecto en la presentación del 100%		

6.12 Gestión de Adquisiciones

Tabla 29 - Fecha de Adquisiciones

Fecha	Actividad
Domingo de cada semana del proyecto	Adquisición de recursos analíticos para la elaboración de resúmenes de artículos seleccionados.
11/08/2019	Adquisición de experto TI para la certificación del Benchmark del proyecto
01/09/2019	Adquisición de experto TI para la certificación del Documento comparativo de controles
22/09/2019	Adquisición de experto TI para la certificación de la Escala de Madurez
03/05/2020	Adquisición de experto TI para la certificación de la Taxonomia ACM Cybersecurity 2020 Curricular Framework

Tabla 30 - Supuestos y restricciones de adquisiciones

Categoria	Supuestos y restricciones
Adquisición de recursos	• Se asume que el recurso tiene las habilidades necesarias para cumplir la labor solicitada • Se asume que la disponibilidad del recurso es suficiente para cumplir las 20 horas semanales requeridas • Se asume que el recurso comunicara al Project Manager cualquier impedimento con respecto al cumplimiento de la labor asignada • El recurso no trabajara más de 20 horas hombre cada semana • El recurso asignado al proyecto al inicio de cada semana depende de la decisión de la empresa IT - Service
Compra de licencias	• Siempre se adquirirá la versión más reciente del producto en cuestión • A menos que sea explícitamente indicado, se utilizara la versión Open – Source del producto

La adquisición de analistas y IT Expert será realizada a través de la empresa “IT – Service”

6.13 Gestión de costo

El costo de los recursos humanos del proyecto será medido según horas hombre.

El costo de las licencias adquiridas será un monto único equivalente al costo de dichas licencias.

La medición del rendimiento del proyecto con respecto a costos se realizará mediante la herramienta “Microsoft Project”. Los costos se encuentran asignados a nivel de tarea y son calculados mediante la aplicación del costo por hora hombre de cada recurso asignado y el total de horas estimado de cada tarea.

Se requiere del total de costo del proyecto y el umbral de control a nivel de tareas. Ambos serán utilizados en los reportes emitidos al Portfolio Manager y Product Owner para ayudar con la orientación del proyecto al igual que la gestión de recursos. Además, será utilizado en las presentaciones del proyecto para justificar la viabilidad de la propuesta.

Se podrá obtener presupuesto adicional mediante la venta de la licencia de la herramienta propuesta.

Asimismo, se podrá ofrecer capacitaciones con respecto a la aplicación de la herramienta y comprensión de resultados obtenidos.

6.14 Gestión de Calidad

Con respecto a la elaboración del producto, se han investigado e incorporado controles de fuentes de confianza como NIST e HIPAA al igual que realizado búsquedas de estudios pasados utilizando el buscador académico “Scopus” para garantizar la calidad de las referencias utilizadas. Asimismo, en el caso de la taxonomía se utilizó la versión 2020 de ACM Cybersecurity Curricular Framework como base, asegurando que la información utilizada sea de confianza por asociación.

Con respecto a la elaboración del proyecto, se han incorporado conceptos de PMBOK con respecto a la gestión de proyectos para la elaboración de la documentación del proyecto al igual que el cronograma de este.

El plan de continuidad está basado en la gestión de cambio de ITIL lo cual garantiza que se

Entregables	Procesos
• Benchmark de soluciones de Ciberseguridad, Privacidad y salud • Documento de integración de controles • Escala de madurez • Plan de continuidad • Taxonomia basada en ACM Cybersecurity Curricular Framework 2020	• Proceso de elaboración de benchmark • Proceso de elaboración de Documento de Integracion de controles • Proceso de elaboración de escala de madurez • Proceso de elaboración de taxonomía basada en ACM Cybersecurity Curricular Framework 2020

utilizaran las mejores prácticas en su desarrollo y, por ende, este será de calidad.

Tabla 31 - Métricas de Plan de Continuidad

Especificación o Métrica	Medida
1. Aseguramiento de calidad en el Benchmarking de soluciones	1. Aceptación por parte del Product Owner
2. Aseguramiento de calidad en la integración de controles de las soluciones seleccionadas	2. Aceptación por parte del Product Owner
3. Aseguramiento de calidad en la herramienta propuesta por el proyecto	3. Aceptación por parte del Product Owner
4. Aseguramiento de calidad en el plan de continuidad del proyecto	4. Aceptación por parte del Product Owner
5. Validación de calidad de los entregables del proyecto, por Experto TI	5. Obtención de certificación por parte de IT Services
6. Validación de calidad de la taxonomía elaborada, por Experto TI	6. Obtención de certificación por parte de IT Services

Tabla 32 - Entregables Plan de Continuidad

En el caso de la validación de calidad mediante Product Owner, se realizarán reuniones semanales sobre las cuales se evalúa el progreso de los entregables en cuestión. Una vez terminados, el Product Owner brindara su firma, dando por concluido el entregable y asegurando su calidad.

En el caso de la validación por IT Service, el entregable es entregado la semana previa al periodo de certificación. Este periodo tiene un tiempo de duración de 3 semanas que, al

concluirse resultara en la recepción de observaciones y la certificación después del levantamiento de estas. Se realizarán 4 actividades de certificación en el proyecto

6.15 Gestión de Requerimientos

Los requerimientos del Proyecto fueron obtenidos mediante dos técnicas principales: Observación y entrevistas. Se observaron estudios previos y noticias sobre los incidentes de ciberseguridad relacionados con el área de salud para determinar los requerimientos del proyecto. Además, se realizarán entrevistas a expertos en el tema como el Product Owner para delimitar las necesidades actuales con respecto a modelos de madurez en ciberseguridad.

Todo requerimiento obtenido se analiza bajo los siguientes conceptos:

- Origen: Es un requerimiento proveniente del Portfolio Manager, Product owner, Comité o inferido por investigación

- Prioridad: Indica cuan vital sería el agregado/cumplimiento de dicho requerimiento para lograr satisfacer la problemática encontrada en la propuesta de proyecto. En orden de menor prioridad, los niveles son Mandatorio, Debería, Podría, Deseable.

- Impacto: Indica la complejidad que implicaría el cumplimiento de dicho requerimiento. Se consideran las horas estimadas para el cumplimiento del requerimiento y los recursos involucrados. Los posibles impactos son: Alto, Medio, Bajo

Las categorías asignadas a los requerimientos son las siguientes:

- De gestión: Requerimientos obtenidos por el Portfolio Manager con respecto a la elaboración del proyecto

- De producto: Requerimientos obtenidos por el Product Owner con respecto a la elaboración del producto del proyecto

- De Observación: Requerimientos obtenidos mediante la investigación y evaluación del contexto del sector salud con respecto a ciberseguridad y privacidad

6.15.1 Reporte

- Se realizan 2 sesiones semanales con el Portfolio Manager para medir el progreso del proyecto y las labores relacionadas a la elaboración de dicho proyecto.

- Se realiza 1 sesión semanal con el Product Owner para verificar el progreso de los entregables del proyecto y asegurar que este sigue una visión precisa.

6.15.2 Validación de Requerimientos

- IT Service: Empresa que nos brindara expertos en TI que certificaran los entregables del proyecto asociados con los requerimientos planteados

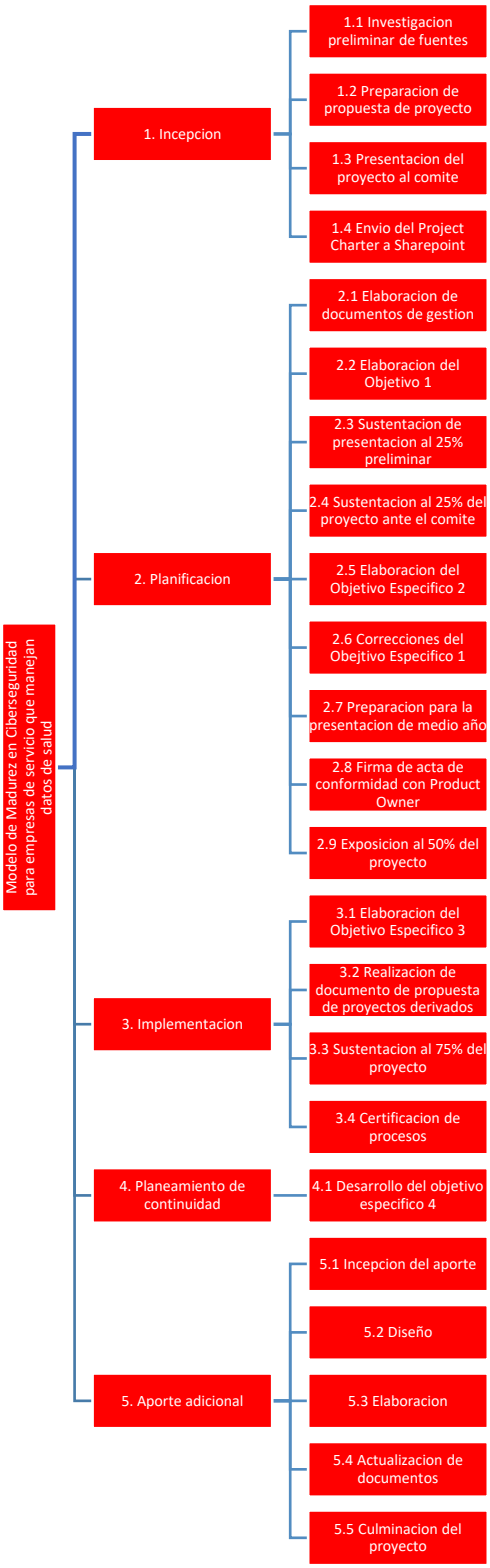
- Portfolio Manager: Brinda su aprobación con respecto al cumplimiento de requerimientos asociados con la elaboración del proyecto.

- Product Owner: Brinda su aprobación con respecto a los requerimientos asociados con el producto del proyecto. Esta se manifiesta en la forma de la "Acta de aceptación" la cual firma al concluir un Objetivo Especifico

6.16 Gestión del Alcance

6.16.1 EDT

Figura 8 - EDT


Modelo de Madurez en Ciberseguridad para empresas de servicio que manejan datos de salud
1. Incepcion
1.1 Investigacion preliminar de fuentes
1.2 Preparacion de propuesta de proyecto
1.3 Presentacion del proyecto al comite
1.4 Envio del Project Charter a Sharepoint
2. Planificacion
2.1 Elaboracion de documentos de gestion
2.2 Elaboracion del Objetivo 1
2.3 Sustentacion de presentacion al 25% preliminar
2.4 Sustentacion al 25% del proyecto ante el comite
2.5 Elaboracion del Objetivo Especifico 2
2.6 Correcciones del Obejtivo Especifico 1
2.7 Preparacion para la presentacion de medio año
2.8 Firma de acta de conformidad con Product Owner
2.9 Exposicion al 50% del proyecto
3. Implementacion
3.1 Elaboracion del Objetivo Especifico 3
3.2 Realizacion de documento de propuesta de proyectos derivados
3.3 Sustentacion al 75% del proyecto
3.4 Certificacion de procesos
4. Planeamiento de continuidad
4.1 Desarrollo del objetivo especifico 4
5. Aporte adicional
5.1 Incepcion del aporte
5.2 Diseño
5.3 Elaboracion
5.4 Actualizacion de documentos
5.5 Culminacion del proyecto

6.16.2 Aceptación de Entregables

Entregable	Método de aprobación
Benchmark de soluciones actuales	• Certificación por parte de la empresa IT Service • Aprobación por parte del Product owner (Acta de aceptación)
Justificación de selección de soluciones para integrar en el modelo	• Certificación por parte de la empresa IT Service • Aprobación por parte del Product owner (Acta de aceptación)
Documento comparativo de controles integrados	• Certificación por parte de la empresa IT Service • Aprobación por parte del Product owner (Acta de aceptación)
Documento de estructura del modelo de madurez	• Certificación por parte de la empresa IT Service • Aprobación por parte del Product owner (Acta de aceptación)
Escala de madurez	• Certificación por parte de la empresa IT Service • Aprobación por parte del Product owner (Acta de aceptación)
Herramienta de evaluación de madurez	• Aprobación por parte del Product owner (Acta de aceptación)
Certificación de IT - Services	• Resultado de la aprobación por parte de la empresa IT Service
Plan de continuidad	• Certificación por parte de la empresa IT Service • Aprobación por parte del Product owner (Acta de aceptación)
Taxonomía de ciberseguridad basada en ACM Cybersecurity 2020	• Certificación por parte de la empresa IT Service • Aprobación por parte del Product owner (Acta de aceptación)

6.16.3 Alcance e integración de requerimientos

Requerimiento	Indicador	Paquete de trabajo

• La solución debe considerar las perspectivas de ciberseguridad, privacidad y normativas de salud	IE1	2.6.2 Firma del indicador de éxito 1
• Los componentes de la solución deben ser justificados	IE2	2.6.3 Firma del indicador de éxito 2
• Se requiere de una evaluación integrada de ciberseguridad, privacidad en el sector de salud	IE3	2.8.1 Firma de indicador de éxito 3
• Se necesita de un método para facilitar la evaluación de empresas que manejan datos de salud	IE4	2.8.2 Firma de indicador de éxito 4
• Los resultados de la herramienta deben de ser precisos	IE5	3.3.2.6 Validación de herramienta del modelo
• La solución propuesta debe mantenerse relevante posterior a la conclusión del proyecto	IE6	5.5.2 Validación del indicador de éxito 6
• Se debe asegurar la calidad de los entregables del proyecto	IE7	3.4.4 Emisión de certificado de IT - Services
• El proyecto debe brindar un valor adicional a la propuesta de modelo de madurez	IE8	5.3.6.2 Taxonomía certificada

CONCLUSIONES

- El modelo es válido, fue probado en una clínica de Lima - Perú, donde el nivel de capacidades fue 2 de 5, lo cual nos permitió identificar brechas importantes y plantear recomendaciones. Mediante un formulario de evaluación se obtuvo un puntaje 4.6 de 5. Esto demuestra que el modelo cumple su propósito en cuanto a brindar valor a las empresas de salud.
- Se logró la elaboración de una taxonomía de investigación para la rápida identificación de temas con niveles bajos de exploración lo cual permitirá enfocar los esfuerzos de investigación en áreas de necesidad.
- A través del análisis de las áreas de ciberseguridad, privacidad y gestión de datos de salud de nuestro modelo se ha logrado identificar la situación actual de la empresa

en un único análisis. Esto permitió establecer recomendaciones en un tiempo menor comparado a un análisis convencional utilizando las tres perspectivas separadas.

- Algunas de las recomendaciones brindadas a la organización fueron la documentación y estandarización de procesos actuales al igual que la inclusión de procesos que atiendan las necesidades de ciberseguridad, privacidad y salud al igual que sus requerimientos legales. Asimismo, se recomendó la estandarización de la gestión de espacio disponible, el proceso de prueba de backup y los planes de respuesta para reducir la incertidumbre y facilitar su automatización.
- Se recibieron observaciones con respecto al uso de normativa peruana dentro del modelo, señalando que sería apropiado incluir más controles orientados a dicha perspectiva.
- Por otra parte, la investigación inicial mediante benchmarking nos permitió identificar las soluciones actuales que mejor se adaptaban a nuestra propuesta. Asimismo, la elaboración de la taxonomía confirmó que existe una necesidad de investigaciones que contemplen aspectos de Ciberseguridad y Privacidad en el Sector Salud.
- El plan de continuidad permite que el modelo se mantenga actualizado, ya que al contener leyes necesita una flexibilidad para adaptar nuevos controles que permitan cumplir nuevas regulaciones que puedan surgir en los siguientes años.

RECOMENDACIONES

- Se recomienda que para proyectos similares se realice un análisis de validación del modelo por parte de un experto en el área y un representante de la organización a aplicar el modelo. Asimismo, se recomienda, para proyectos similares, utilizar una taxonomía para identificar los sectores que necesitan investigación. A partir de ello, realizar un benchmarking de soluciones actuales de esa área y sector para identificar las mejores alternativas.
- En una futura iteración de este proyecto o uno de propuesta similar, se recomienda realizar la etapa de implementación en múltiples empresas. Que el modelo pase por

distintas iteraciones permite que mejoren y se consoliden los flujos y procesos de evaluación y medición.

- Realizar seguimiento de las normativas legales, ya que al ser un modelo que integra leyes necesita constante actualización según vayan apareciendo modificaciones en la ley.
- Automatizar ciertos controles e informes requeridos para hacer seguimiento al cumplimiento de normativas y estándares mediante una plataforma. Las organizaciones pueden identificar y mejorar de una manera más rápida su nivel de madurez al tener este proceso de análisis en gran parte automatizado.

GLOSARIO

BACK UP: Copia de respaldo

SUSALUD: Superintendencia Nacional de Salud

IPRESS: Instituciones Prestadoras de Salud

IAFAS: Administradoras de Fondos de Aseguramiento en Salud

MINSA: Ministerio de Salud

COBIT: Control Objectives for Information and related Technology

HIPAA: Health Insurance Portability and Accountability Act

FRAMEWORK: Marco de trabajo

BIBLIOGRAFÍA

Abdelhamid, M., Kisekka, V., & Samonas, S. (2019). Mitigating e-services avoidance: the role of government cybersecurity preparedness. *Information and Computer Security*, *27*(1), 26–46. https://doi.org/10.1108/ICS-02-2018-0024

AICPA/CICA. (2011). AICPA/CICA Privacy Maturity Model. *Aicpa/Cica*, *March*, 1–42. https://www.kscpa.org/writable/files/AICPADocuments/10-

229_aicpa_cica_privacy_maturity_model_finalebook.pdf

Birnbaum, D., Gretsinger, K., Antonio, M. G., Loewen, E., & Lacroix, P. (2018). Revisiting public health informatics: patient privacy concerns. *International Journal of Health Governance*, *23*(2), 149–159. https://doi.org/10.1108/IJHG-11-2017-0058

Brown, S. M., Aboumatar, H. J., Francis, L., Halamka, J., Rozenblum, R., Rubin, E., Sarnoff Lee, B., Sugarman, J., Turner, K., Vorwaller, M., & Frosch, D. L. (2016). Balancing digital information-sharing and patient privacy when engaging families in the intensive care unit. *Journal of the American Medical Informatics Association*, *23*(5), 995–1000. https://doi.org/10.1093/jamia/ocv182

Busby, J. S., Green, B., & Hutchison, D. (2017). Analysis of Affordance, Time, and Adaptation in the Assessment of Industrial Control System Cybersecurity Risk. *Risk Analysis*, *37*(7), 1298–1314. https://doi.org/10.1111/risa.12681

Carvalho, J. V., Rocha, Á., van de Wetering, R., & Abreu, A. (2019). A Maturity model for hospital information systems. *Journal of Business Research*, *94*(December), 388–399. https://doi.org/10.1016/j.jbusres.2017.12.012

Chong, I., Xiong, A., & Proctor, R. W. (2019). Human Factors in the Privacy and Security of the Internet of Things. *Ergonomics in Design*, *27*(3), 5–10. https://doi.org/10.1177/1064804617750321

Cui, L., Xie, G., Qu, Y., Gao, L., & Yang, Y. (2018). Security and privacy in smart cities: Challenges and opportunities. *IEEE Access*, *6*, 46134–46145. https://doi.org/10.1109/ACCESS.2018.2853985

Cybersecurity Curricular Guidance for Associate-Degree Programs. (2020). https://doi.org/10.1145/3381686

Dankar, F. K., & Badji, R. (2017). A risk-based framework for biomedical data sharing. *Journal of Biomedical Informatics*, *66*, 231–240. https://doi.org/10.1016/j.jbi.2017.01.012

Empresa Peruana de Servicios Editoriales S.A. (2013). Reglamento de la Ley Nº 29733, Ley de Protección de Datos Personales. *Diario Oficial El Peruano*, *35*, 15. www.minjus.gob.pe

Esther Omolara, A., Jantan, A., Abiodun, O. I., Arshad, H., Dada, K. V., & Emmanuel, E. (2020). HoneyDetails: A prototype for ensuring patient's information privacy and thwarting electronic health record threats based on decoys. *Health Informatics Journal*. https://doi.org/10.1177/1460458219894479

Ghobakhloo, M. (2020). Determinants of information and digital technology implementation for smart manufacturing. *International Journal of Production Research*, *58*(8), 2384–2405. https://doi.org/10.1080/00207543.2019.1630775

Gobierno del Peru. (2017). *Aprueban el Reglamento de la Ley N° 30024, Ley que crea el Registro Nacional de Historias Clínicas Electrónicas* (pp. 32–45). https://www.administracion.usmp.edu.pe/institutoconsumo/wp-content/uploads/Reglamento-de-la-Ley-N°-30024-Ley-que-crea-el-Registro-Nacional-de-Historias-Clínicas-Electrónicas.pdf?fbclid=IwAR3hn0LSjlZB7eygWigqjCQ53V1ldG3yQDDA4i2fb5jbiPY-K7xTx3Wxg6M

Gupta, M., Abdelsalam, M., Khorsandroo, S., & Mittal, S. (2020). Security and Privacy in Smart Farming: Challenges and Opportunities. *IEEE Access*, *8*, 34564–34584. https://doi.org/10.1109/ACCESS.2020.2975142

Guttieres, D., Stewart, S., Wolfrum, J., & Springs, S. L. (2019). Cyberbiosecurity in Advanced Manufacturing Models. *Frontiers in Bioengineering and Biotechnology*, *7*. https://doi.org/10.3389/fbioe.2019.00210

ISACA Interactive Glossary & Term Translations | ISACA. (n.d.). Retrieved May 14, 2020, from https://www.isaca.org/resources/glossary

Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in Hospitals: A Systematic, Organizational Perspective. *Journal of Medical Internet Research*, *20*(5), e10059. https://doi.org/10.2196/10059

Khatoun, R., & Zeadally, S. (2017). Cybersecurity and privacy solutions in smart cities. *IEEE Communications Magazine*, *55*(3), 51–59. https://doi.org/10.1109/MCOM.2017.1600297CM

Khou, S., Mailloux, L. O., Pecarina, J. M., & McEvilley, M. (2017). A Customizable Framework for Prioritizing Systems Security Engineering Processes, Activities, and

Tasks. *IEEE Access*, *5*, 12878–12894. https://doi.org/10.1109/ACCESS.2017.2714979

Kour, R., Karim, R., & Thaduri, A. (2019). Cybersecurity for railways – A maturity model. *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit*. https://doi.org/10.1177/0954409719881849

Kuo, K. M., Talley, P. C., & Cheng, T. J. (2019). Deterrence approach on the compliance with electronic medical records privacy policy: The moderating role of computer monitoring. *BMC Medical Informatics and Decision Making*, *19*(1). https://doi.org/10.1186/s12911-019-0957-y

Le, N. T., & Hoang, D. B. (2017). Capability maturity model and metrics framework for cyber cloud security. *Scalable Computing*, *18*(4), 277–290. https://doi.org/10.12694/scpe.v18i4.1329

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: How safe are we? *BMJ (Online)*, *358*. https://doi.org/10.1136/bmj.j3179

Mascetti, S., Metoui, N., Bettini, C., & Lanzi, A. (2018). EPIC: A methodology for evaluating privacy violation risk in cybersecurity systems EPIC: a Methodology for Evaluating Pri-vacy Violation Risk in Cybersecurity Sys-tems. In *TRANSACTIONS ON DATA PRIVACY* (Vol. 11). https://www.researchgate.net/publication/327529035

Nasiri, S., Sadoughi, F., Tadayon, M. H., & Dehnad, A. (2019). Security requirements of internet of things-based healthcare system: A survey study. *Acta Informatica Medica*, *27*(4), 253–258. https://doi.org/10.5455/aim.2019.27.253-258

National Institute of Standards and Technolgy. (2014). Framework for Improving Critical Infrastructure Cybersecurity. In *Framework for Improving Critical Infrastructure Cybersecurity Note to Readers on the Update* (pp. 29–35). https://doi.org/10.6028/NIST.CSWP.04162018

National Institute of Standards and Technolgy. (2020, January 16). *NIST Privacy Framework*. January 16, 2020. https://doi.org/10.6028/NIST.CSWP.01162020

National Institute of Standards and Technology (NIST). (2014). SP 800-53 Rev.4 - Security and Privacy Controls for Federal Information Systems and Organizations. *National Institute of Standards and Technology (NIST) - Special Publication*, *800–53*, 1–460.

https://doi.org/10.6028/NIST.SP.800-53r4

Natsiavas, P., Rasmussen, J., Voss-Knude, M., Votis, K., Coppolino, L., Campegiani, P., Cano, I., Marí, D., Faiella, G., Clemente, F., Nalin, M., Grivas, E., Stan, O., Gelenbe, E., Dumortier, J., Petersen, J., Tzovaras, D., Romano, L., Komnios, I., & Koutkias, V. (2018). Comprehensive user requirements engineering methodology for secure and interoperable health data exchange 08 Information and Computing Sciences 0806 Information Systems. *BMC Medical Informatics and Decision Making*, *18*(1). https://doi.org/10.1186/s12911-018-0664-0

OMS | El Perú. (n.d.). Retrieved June 30, 2020, from https://www.who.int/workforcealliance/countries/per/es/

Prakash Attili, V. S., Mathew, S. K., & Sugumaran, V. (2018). Understanding information privacy assimilation in it organizations using multi-site case studies. *Communications of the Association for Information Systems*, *42*(1), 66–94. https://doi.org/10.17705/1CAIS.04204

Rose, J. (2013). *Selecting, Using, and Creating Maturity Models: A Tool for Assurance and Consulting Engagements*. *July*, 1–27. https://www.iia.org.uk/media/358857/selecting__using__and_creating_maturity_models_-__a_tool_for_assurance_and_consulting_engagements.pdf

Salah, D., Paige, R., & Cairns, P. (2014). An evaluation template for expert review of maturity models. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 8892). https://doi.org/10.1007/978-3-319-13835-0_31

Security, I. (2019). *Cost of a Data Breach Report 2019*. https://www.ibm.com/downloads/cas/ZBZLY7KL

Shen, N., Sequeira, L., Silver, M. P., Carter-Langford, A., Strauss, J., & Wiljer, D. (2019). Patient privacy perspectives on health information exchange in a mental health context: Qualitative study. *Journal of Medical Internet Research*, *21*(11). https://doi.org/10.2196/13306

Shen, N., Strauss, J., Silver, M., Carter-Langford, A., & Wiljer, D. (2019). The eHealth trust model: A patient privacy research framework. *Studies in Health Technology and*

Informatics, *257*, 382–387. https://doi.org/10.3233/978-1-61499-951-5-382

Shi, M., Jiang, R., Hu, X., & Shang, J. (2019). A privacy protection method for health care big data management based on risk access control. *Health Care Management Science*. https://doi.org/10.1007/s10729-019-09490-4

Stoldt, J. P., Price, M., & Weber, J. (2019). Towards a clinical analytics adoption maturity framework for primary care. *Studies in Health Technology and Informatics*, *257*, 399–403. https://doi.org/10.3233/978-1-61499-951-5-399

Takai-Igarashi, T., Kinoshita, K., Nagasaki, M., Ogishima, S., Nakamura, N., Nagase, S., Nagaie, S., Saito, T., Nagami, F., Minegishi, N., Suzuki, Y., Suzuki, K., Hashizume, H., Kuriyama, S., Hozawa, A., Yaegashi, N., Kure, S., Tamiya, G., Kawaguchi, Y., … Yamamoto, M. (2017). Security controls in an integrated Biobank to protect privacy in data sharing: Rationale and study design. *BMC Medical Informatics and Decision Making*, *17*(1). https://doi.org/10.1186/s12911-017-0494-5

Thorpe, J. H., Gray, E. A., & Cartwright-Smith, L. (2016). Show us the data: The critical role health information plays in health system transformation. *Journal of Law, Medicine and Ethics*, *44*(4), 592–597. https://doi.org/10.1177/1073110516684800

Ti, G., Isaca, Manuel, G., Quintanilla, Y., Erastus Mosha, MINTIC, Arte, E. D. E. L., Muñoz Periñán, I. L., Ulloa Villegas, G., Copy, P., Lanter, D., Isaca, الـ شعـ يـ بي ,ا .م., Ocasio, V. M., Andres, C., Saavedra, S., MINTIC, Neira, A. L., Spohr, J. R., … Weybrecht, G. (2012). COBIT 5 - Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa. In *Guía de inspiración para la implementación de PRME: Segunda Edición: Aprender para Avanzar* (Vol. 147, Issue 17). https://doi.org/10.9774/gleaf.9781783537846_16

U.S. Dept. of Labor Employee Benefits Security Administration. (1996). HIPAA. Health Insurance Portability and Accountability Act of 1996. In *104th Congress: Vol. Public Law*. https://www.govtrack.us/congress/bills/104/hr3103/text

Visión y Misión | SUSALUD. (n.d.). Retrieved June 30, 2020, from http://portal.susalud.gob.pe/nosotros-vision-mision/

Wagire, A. A., Joshi, R., Rathore, A. P. S., & Jain, R. (2020). Development of maturity model for assessing the implementation of Industry 4.0: learning from theory and

practice. *Production Planning and Control*, *0*(0), 1–20. https://doi.org/10.1080/09537287.2020.1744763

Zandona, D. J., & Thompson, J. M. (2017). Going beyond Compliance: A Strategic Framework for Promoting Information Security in Hospitals. *Health Care Manager*, *36*(4), 364–371. https://doi.org/10.1097/HCM.0000000000000189