**UNIVERSIDAD TECNICA FEDERICO SANTA MARIA**

**Repositorio Digital USM** **https://repositorio.usm.cl**

Tesis USM TESIS de Pregrado de acceso ABIERTO

2021-03

# PLATAFORMA PARA LA EVALUACIÓN DE LA CALIDAD EN SEGURIDAD DE LOS REGISTROS CLÍNICOS ELECTRÓNICOS EN CHILE

HERNÁNDEZ ROBLES, RODRIGO JAVIER

https://hdl.handle.net/11673/50445

*Repositorio Digital USM, UNIVERSIDAD TECNICA FEDERICO SANTA MARIA*

UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA
DEPARTAMENTO DE INFORMÁTICA
VALPARAÍSO - CHILE

# “PLATAFORMA PARA LA EVALUACIÓN DE LA CALIDAD EN SEGURIDAD DE LOS REGISTROS CLÍNICOS ELECTRÓNICOS EN CHILE”

RODRIGO JAVIER HERNÁNDEZ ROBLES

MEMORIA PARA OPTAR AL TÍTULO DE
INGENIERO CIVIL EN INFORMÁTICA

Profesor Guía: Hernán Astudillo
Profesor Correferente: Gastón Márquez

Marzo - 2021

## DEDICATORIA

Para todas las personas que de alguna forma, fueron parte de mi vida durante este hermoso proceso. En especial, a mi familia.

# RESUMEN

**Resumen—** El Registro Clínico Electrónico (RCE) es un documento digital que almacena información relacionada con servicios, los cuales son prestados a pacientes en todos los ámbitos del sistema de salud. Es por ello que, es primordial mantener un seguimiento de los distintos aspectos de seguridad que puedan afectar negativamente a estos sistemas. Actualmente en Chile no existe suficiente información sobre una herramienta que pueda evaluar a través de métricas, los distintos aspectos de seguridad que deben ser considerados en los RCEs. En el presente documento se detalla el desarrollo de una plataforma que, mediante una evaluación de métricas, permitirá evaluar la calidad en seguridad de los RCEs de las distintas Instituciones de Salud del país.

**Palabras Clave—** Registro Clínico Electrónico; Seguridad; Métricas; Plataforma; Evaluación.

# ABSTRACT

***Abstract—*** The Electronic Health Record (EHR) is a digital document that stores information related to services, which are provided to patients in all areas of the healthcare system. For this reason, it is essential to keep track of the different security aspects that may negatively affect these systems. Currently in Chile there is not enough information on a tool that can evaluate, through metrics, the different safety aspects that should be considered in EHRs. This document details the development of a platform that, by means of an evaluation of metrics, will make it possible to evaluate the safety quality of the EHRs of the different health institutions in the country.

***Keywords—*** Electronic Health Record; Security; Metrics; Platform; Evaluation.

# GLOSARIO

API: Application Programming Interface.

BD: Base de Datos.

CENS: Centro Nacional en Sistemas de Información en Salud.

CSS: Cascading Style Sheets.

EHR: Electronic Health Record.

HdU: Historia(s) de Usuario.

HTTP: Hypertext Transfer Protocol.

MINSAL: Ministerio de Salud de Chile.

MVC: Model-View-Controller (Modelo-Vista-Controlador).

NoSQL: non-Structured Query Language.

PDF: Portable Document Format.

RCE(s): Registro(s) Clínico(s) Electrónico(s).

REST: Representational State Transfer.

RDBMS: Relational Database Management System.

SQL: Structured Query Language.

UI: User Interface.

UML: Unified Modeling Language.

XP: eXtreme Programming.

# ÍNDICE DE CONTENIDOS


**RESUMEN** . . . . . III

**ABSTRACT** . . . . . III

**GLOSARIO** . . . . . IV

**ÍNDICE DE FIGURAS** . . . . . VII

**ÍNDICE DE TABLAS** . . . . . VIII

**INTRODUCCIÓN** . . . . . 1

**CAPÍTULO 1: PROBLEMA ESPECÍFICO** . . . . . 3
- 1.1 OBJETIVOS . . . . . 4
  - 1.1.1 OBJETIVO GENERAL . . . . . 4
  - 1.1.2 OBJETIVOS ESPECÍFICOS . . . . . 5

**CAPÍTULO 2: TRABAJO PREVIO** . . . . . 6
- 2.1 GESTIÓN DE LA SEGURIDAD - PRIVACIDAD . . . . . 6
- 2.2 INTEGRIDAD . . . . . 7
- 2.3 CONFIDENCIALIDAD . . . . . 8
- 2.4 SEGURIDAD EN ESPACIO DE TRABAJO . . . . . 8
- 2.5 DISPONIBILIDAD . . . . . 9
- 2.6 REGISTRO CLÍNICO ELECTRÓNICO . . . . . 9
- 2.7 MÉTRICAS PARA EVALUAR LA SEGURIDAD DE LOS RCEs . . . . . 10
  - 2.7.1 MÉTODO DE EVALUACIÓN . . . . . 11

**CAPÍTULO 3: PROPUESTA** . . . . . 13
- 3.1 DOMINIO DEL PROBLEMA . . . . . 13
  - 3.1.1 MODELO DE DOMINIO . . . . . 13
- 3.2 METODOLOGÍA DE DESARROLLO . . . . . 14
  - 3.2.1 HISTORIAS DE USUARIO . . . . . 15
- 3.3 ARQUITECTURA Y DISEÑO DE LA PLATAFORMA . . . . . 17
  - 3.3.1 DIAGRAMA DE CLASES . . . . . 18
  - 3.3.2 MODELO DE DATOS . . . . . 20

**CAPÍTULO 4: IMPLEMENTACIÓN** . . . . . 22
- 4.1 TECNOLOGÍAS UTILIZADAS . . . . . 22
  - 4.1.1 MYSQL . . . . . 22
  - 4.1.2 LARAVEL . . . . . 22
  - 4.1.3 VUE.JS . . . . . 23
  - 4.1.4 TAILWINDCSS . . . . . 23

4.2 PROCESO DE DESARROLLO . . . . . 23
4.3 DESARROLLO DE SPRINTS . . . . . 24
4.3.1 PRIMER SPRINT . . . . . 25
4.3.2 SEGUNDO SPRINT . . . . . 28
4.3.3 TERCER SPRINT . . . . . 30

**CAPÍTULO 5: VERIFICACIÓN** . . . . . 32
5.1 VERIFICACIÓN DE SPRINTS . . . . . 32
5.1.1 PRIMER SPRINT . . . . . 33
5.1.2 SEGUNDO SPRINT . . . . . 37
5.1.3 TERCER SPRINT . . . . . 40

**CAPÍTULO 6: CONCLUSIONES** . . . . . 46

**ANEXOS** . . . . . 47
6.1 ANEXO A: REQUISITOS FUNCIONALES . . . . . 47
6.2 ANEXO B: REQUISITOS NO FUNCIONALES . . . . . 49

**REFERENCIAS BIBLIOGRÁFICAS** . . . . . 50

# ÍNDICE DE FIGURAS


1 Árbol del problema . . . . . 4

2 Representación del instrumento propuesto en [Márquez *et al.*, 2020] . . . . . 11

3 Modelo de dominio . . . . . 14

4 Flujo de trabajo del de la metodología de desarrollo ágil . . . . . 15

5 Model-View-Controller . . . . . 18

6 Diagrama de clases propuesto . . . . . 19

7 Modelo de datos propuesto . . . . . 21

8 Representación de un Sprint en Scrum . . . . . 24

9 Diagrama de flujo de evaluación propuesto . . . . . 25

10 Vista de login. Con logo y colores institucionales del CENS. . . . . 33

11 Vista de lista de evaluaciones asignadas al Evaluador . . . . . 34

12 Vista de lista de evaluaciones asignadas a una Institución de Salud . . . . . 34

13 Vista de estado general de evaluación. Además se muestra el campo de texto para ingresar el feedback general. . . . . 35

14 Vista de detalle de área, con campo de texto para ingresar el feedback específico. . . . . 36

15 Vista de evaluación de métrica con opciones relacionadas a la escala de Likert y sus respectivos criterios de evaluación. . . . . 36

16 Vista de formulario de creación/edición de usuarios. . . . . 37

17 Vista de perfil de Usuario (Institución de Salud). . . . . 38

18 Vista de listado de las evaluaciones asignadas (según perfil) con resumen general relacionado al estado de estas. . . . . 38

19 Vista del principio del documento donde se exporta toda la información de la evaluación en formato PDF. . . . . 39

20 Vista de última página del documento donde se puede ver el resultado final de la evaluación. . . . . 40

21 Vista de tabla de Usuarios con pestañas asociadas a cada Rol, la opción de ver el perfil de cada Usuario y la opción de “eliminarlo”. . . . . 41

22 Vista de modal de confirmación para “eliminar” Usuario. . . . . 41

23 Vista de formulario para creación de evaluación, donde se debe seleccionar Evaluador, fecha, Institución de Salud y áreas a evaluar. Cabe destacar que es posible seleccionar entre 2 y 5 áreas. . . . . 42

24 Vista de modal de confirmación para eliminar evaluación, aparece luego de pulsar el botón “Eliminar” que aparece en la fig. 18 . . . . . 43

25 Vista de detalle de evaluación cuando está completa. . . . . 44

26 Vista de resultado de búsqueda de Institución de Salud, luego de pulsar el botón de búsqueda en la barra de navegación. . . . . 45

27 Vista opciones de evaluación de métrica, con opción “No Aplica” incluida y su respectivo campo de texto para ingresar la justificación en caso de seleccionarla. 45

# ÍNDICE DE TABLAS

1 Rango de valores para cada opción de la escala de Likert . . . . . 11

2 Rango de valores para selección se resultado final . . . . . 12

3 Endpoints desarrollados en Sprint 1 . . . . . 27

4 Endpoints desarrollados en Sprint 2 . . . . . 29

5 Endpoints desarrollados en Sprint 3 . . . . . 30

6 Resultado de evaluación de RCE para el Hospital Digital de Chile en área Confidencialidad . . . . . 32

# INTRODUCCIÓN

Hoy en día, la calidad de la atención a los pacientes es de gran relevancia dentro de la atención hospitalaria [Shaw *et al.*, 2014]. Las exigencias de satisfacción van aumentando junto con las necesidades, eso incluye conceptos importantes relacionados con la seguridad, como la privacidad y la confidencialidad. Es por ello que, la confianza de los pacientes hacia las Instituciones de Salud, debe garantizarse mediante distintos tipos de acreditación institucional, los cuales permitan medir y evaluar la calidad de los servicios que se ofrecen.

Bajo el contexto de la seguridad, la digitalización de la información en el área de la salud permite abrir nuevas oportunidades de innovación y nuevos retos como lo es la seguridad de la información del paciente. Por ejemplo, en 2018 se filtró la información clínica de aproximadamente 2 millones de pacientes en México [1], esto luego de que un investigador descubriera una base de datos *MongoDB* de acceso público en Internet.

Es por lo anterior, que el Registro Clínico Electrónico (RCE) debe cumplir con estándares y normativas de seguridad para resguardar los derechos de confidencialidad de cada paciente, además, cumpliendo con protocolos de transparencia para así generar confianza en su implementación y esta pueda ser efectiva. Por ejemplo, el uso de la criptografía garantiza la seguridad de la información de los pacientes en los sistemas de registros clínicos electrónicos y el cifrado mejora la seguridad e interoperabilidad de los RCEs durante el intercambio de información entre el médico y los pacientes [Renardi *et al.*, 2018].

Varios países han realizado grandes esfuerzos para salvaguardar la privacidad y los datos de los pacientes en los RCEs. Existen leyes como la Health Insurance Portability and Accountability Act (HIPPA) [2], que entrega un conjunto de reglas de seguridad junto con estándares a seguir, como por ejemplo una lista de planes de contingencia para ciberataques [3], entre otras cosas. Esto con el objetivo principal de mantener la seguridad y confidencialidad de los registros de los pacientes.

Actualmente en Chile, el MINSAL promueve activamente la implementación de políticas de seguridad de la Información [4], que da la posibilidad de disminuir en forma significativa el impacto de los riesgos a los que están sometidos los activos de información. No obstante, no es posible saber si estas políticas de seguridad se están cumpliendo en su mayoría, en los sistemas de información que manejan las Instituciones de Salud.

Sumado a lo anterior, es importante mencionar que no hay una evidencia clara sobre la existencia de una herramienta que permita evaluar los distintos apartados de seguridad, los cuales puedan estar (o no) cubriendo los RCEs de las distintas Instituciones de Salud. Esto

[1] https://www.totalsec.com.mx/blog/blog.php?P=mexico%3A-datos-personales-de-mas-de-2-millones-de-pacientes-expuestos-en-internet
[2] https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
[3] https://www.hhs.gov/sites/default/files/cyber-attack-checklist-06-2017.pdf
[4] https://redsalud.ssmso.cl/sistema-de-seguridad-de-la-informacion/

es un problema, ya que no es posible dimensionar la cantidad de plataformas que pueden tener vulnerabilidades de seguridad, sin embargo, esto también es una oportunidad para investigar y generar una herramienta que facilite ese trabajo.

El objetivo de este documento, es exponer el proceso de desarrollo de una plataforma que permita evaluar la calidad de la seguridad de un RCE, esto mediante un instrumento de calidad construido a partir de un estudio realizado por el CENS.

En el primer capítulo se expone el contexto bajo el cual se desarrollará la plataforma, este se compone principalmente de los conceptos relacionados al RCE y al instrumento de calidad que se implementará.

En el capítulo 2, se describe el problema a abordar relacionado a la situación país. Posteriormente se exponen los objetivos generales y específicos.

Luego, en el capítulo 3, se muestra el trabajo previo relacionado a las distintas áreas que abarca el instrumento de calidad, ya que no existe evidencia clara de un instrumento similar.

En el capítulo 4, se expone la propuesta de la solución planteada junto con los antecedentes relacionados al dominio del problema, además se explica la metodología de desarrollo y elementos relacionados al diseño de la solución.

Posteriormente, en el capítulo 5, se expone el proceso de implementación junto con una breve descripción de las tecnologías utilizadas, además se detalla el paso a paso del proceso de desarrollo involucrado y una propuesta de despliegue para la plataforma.

Finalmente, el capítulo 6 se muestra el proceso de validación, el cual comienza con un caso de aplicación básico de la evaluación basada en el instrumento de calidad. Luego se detalla la validación realizada durante el proceso de desarrollo con las capturas de la plataforma desarrollada; y luego presentar las conclusiones en el capítulo 7.

# CAPÍTULO 1
# PROBLEMA ESPECÍFICO

En estos momentos, nuestro país se encuentra en las primeras fases de acreditación de todos sus procesos clínicos, esto para que los prestadores clínicos institucionales puedan garantizar una atención de acuerdo a estándares de calidad y seguridad en hospitales de mediana y baja complejidad. Bajo este escenario, el Centro Nacional de Sistemas de Información en Salud (CENS) busca desarrollar estrategias y actividades que permitan alcanzar un sistema de salud más conectado, innovar a través de las tecnologías de información en salud, cerrar las brechas en conocimiento y aplicación de sistemas de información en salud, y crear criterios para asegurar la calidad de dichos sistemas [5].

Respecto a la calidad de estas plataformas, un aspecto importante a considerar a la hora de evaluar estándares, es la seguridad. Esto debido al constante avance tecnológico al que se enfrenta no solo el país, si no que también el mundo. Junto con estos avances, también han surgido variadas formas de vulnerar un sistema, lo cual es importante si se está bajo un contexto relacionado con la salud.

Hoy en día, la mayoría de las Instituciones de Salud utiliza un RCE, el cual cumple la función de ser un documento digital que almacena información confidencial y de utilidad tanto para pacientes como para profesionales clínicos, por lo que es de gran importancia la seguridad de los datos que almacena este registro.

En Chile, el RCE ha tenido avances importantes desde el inicio de su implementación en los establecimientos públicos de salud a través de la estrategia SIDRA (Sistema de Información de la Red Asistencial)[6]. Actualmente el 81,3 % de los centros de atención primaria y el 75,2 % de los hospitales cuenta con algún sistema de RCE [E-HealthReporter, 2018]. En el contexto del proceso de acreditación en salud, la construcción de estos registros debe cumplir con determinados requisitos para que los prestadores institucionales puedan garantizar una atención de acuerdo a estándares de calidad y seguridad.

Es por lo anterior, que es necesaria la existencia de una evaluación que permita medir la calidad un RCE desde el punto de vista del software implementado en un servicio clínico, independiente de qué técnicas, métodos o mecanismos de seguridad tenga incorporado. Esto es crítico, pues algunos estudios describen que debe existir un delicado equilibrio en lo que respecta a seguridad y usabilidad [Ka-Ping Yee, 2004]. Por ejemplo, un RCE no puede tener los tres mecanismos de autenticación [7] ya que compromete seriamente la usabilidad del RCE, especialmente en servicios clínicos críticos como Urgencias.

[5] Sitio web CENS: `https://cens.cl/`

[6] Sitio web e-Salud: `http://www.salud-e.cl/sidra-home/estrategia/`

[7] Breve descripción de 3FA: `https://searchsecurity.techtarget.com/definition/three-factor-authentication-3FA`

La complejidad de medir la seguridad de un RCE que ya está en uso va más allá del software, también hay que (i) considerar al usuario final que utiliza el RCE, (ii) el lugar donde se encuentra desplegado el RCE y (iii) la gestión de seguridad informática que el servicio clínico tiene. Dicho lo anterior, un proveedor de software RCE debe tener en cuenta que la seguridad no es solamente está incluida en el software en sí, sino también en áreas transversales al desarrollo de software.

Lo anterior se puede ver ilustrado en la figura 1.

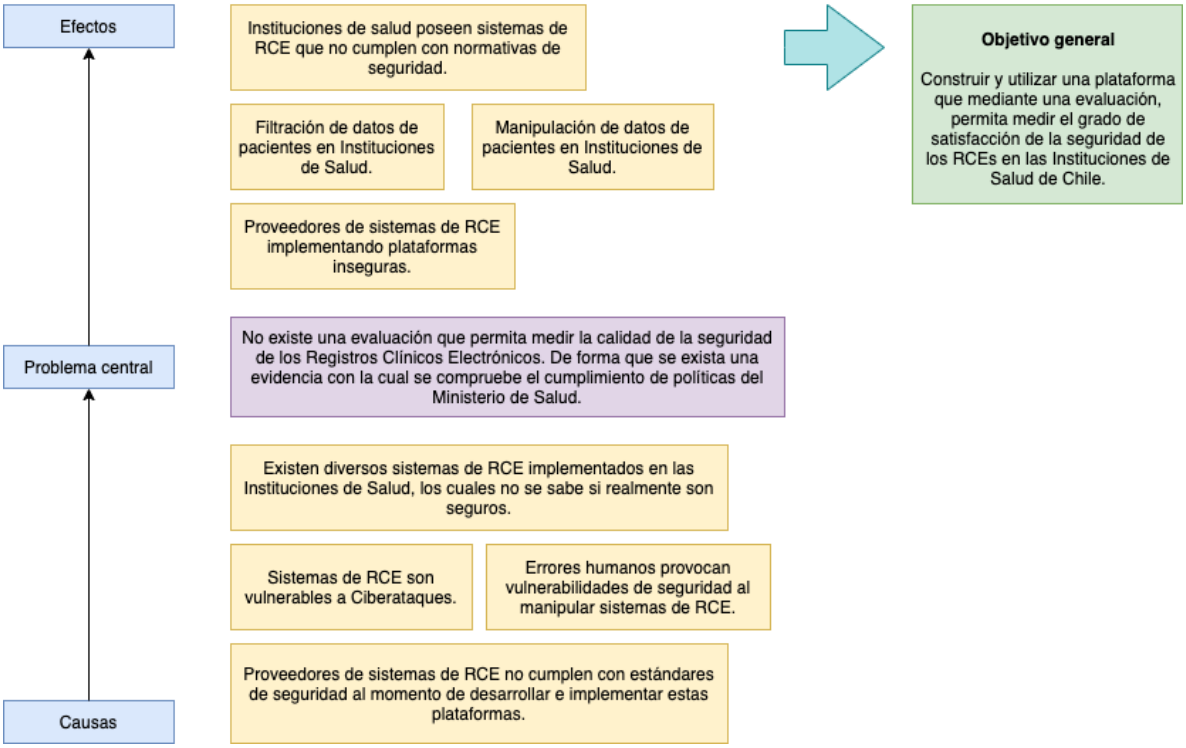


Figura 1: Árbol del problema
Fuente: Elaboración propia.

## 1.1. OBJETIVOS

### 1.1.1. OBJETIVO GENERAL

Construir y utilizar una plataforma que mediante una evaluación, permita medir el grado de satisfacción de la seguridad de los RCEs en las Instituciones de Salud de Chile.

### 1.1.2. OBJETIVOS ESPECÍFICOS

- Desarrollar e implementar una plataforma que permita medir el grado de satisfacción de la seguridad de los RCEs a través de una evaluación según la escala de Likert.
- Construir un modelo que permita al sistema integrar nuevas métricas de calidad multidimensionales en el futuro.
- Ejecutar evaluaciones piloto a Servicios de Salud utilizando la plataforma, con el objetivo de conocer los primeros aspectos en la seguridad de los RCEs.

# CAPÍTULO 2
# TRABAJO PREVIO

A continuación se presenta el trabajo previo relacionado a distintos aspectos que abarca la seguridad en los sistemas de información de salud. Ya sea mediante evaluaciones técnicas o generales.

## 2.1. GESTIÓN DE LA SEGURIDAD - PRIVACIDAD

El reporte creado por la *Organisation for Economic Co-operation and Development (OECD)* [8] discute posibles métricas para medir la seguridad del paciente. En el reporte se describen diferentes prácticas, así como también estrategias de mitigación de potenciales problemas de los pacientes respecto a incidentes de seguridad.

[Wang *et al.*, 2019] discute la preservación de la privacidad de los pacientes en los RCEs en dos diferentes aspectos: en los sistemas de información de los hospitales y nivel de regulación en la gestión de las tecnologías en un hospital. La contribución de los autores es proponer nuevos mecanismos de anonimato y privacidad, los cuales son medidos para evaluar que la eficacia de estos en la protección de los datos.

[Yang *et al.*, 2006] plantea la preocupación sobre la protección de la información de la salud de los pacientes en esta era de la información. El propósito de este estudio es determinar lo que constituye un marco jurídico eficaz para proteger tanto la seguridad como la privacidad de la información sobre la salud, especialmente en los RCE.

Bajo este contexto, el autor junto con un grupo de expertos redactan las ”Directrices de seguridad de la información médica y protección de la privacidad”, las cuales identifican nueve principios y comprenden 12 artículos, esto con la esperanza de que las organizaciones médicas tengan una referencia eficaz sobre cómo gestionar la información médica de manera confidencial y segura, especialmente en las transacciones electrónicas.

[Aldosari, 2017] discute que el mantenimiento preciso de los registros médicos de los pacientes se ha convertido en un problema mundial con el rápido aumento del número de pacientes. Además, menciona que proporcionarles una atención médica adecuada, manteniendo su seguridad a la vista se está convirtiendo en un gran desafío para los médicos, lo que finalmente provoca la creación de los RCEs.

Sin embargo, el autor menciona que en lugar de aumentar la eficiencia de la atención, los RCEs se han convertido en una carga para los médicos ya que, en última instancia, aumentan

[8] Sitio web OECD: `https://www.oecd.org/health/health-systems/Measuring-Patient-Safety-April-2018.pdf`

su tasa de error y reducen la tasa de producción, lo que afecta a la seguridad del paciente. Es por esto que el objetivo del estudio es apoyar a estos sistemas a través de tecnologías informáticas como los sistemas de deciciones de apoyo clínico (CDSS), sistemas computarizados de órdenes médicas (CPOE), intercambio de información sanitaria (HIE), aplicación de documentación móvil y un sistema de alertas de seguridad. Esto, con el objetivo de obtener el máximo beneficio, el cual requiere una formación adecuada de los médicos sobre el uso juicioso de estas características para el RCE. El autor menciona además que, de lo contrario, éstas podrían introducir un número considerable de errores médicos, los que pueden tener resultados fatales para los pacientes.

## 2.2. INTEGRIDAD

[Hulstijn *et al.*, 2011] plantea un modelo de referencia de medidas de seguridad para preservar la integridad de la información que, a diferencia de los enfoques tradicionales que se centran en un enfoque defensivo para preservar la integridad de los datos, presenta medidas ofensivas para estimular la integridad de la información, proporcionando así retroalimentación respecto del uso de estos. Se utiliza como caso de estudio el EPD [9] (Dutch national Electronic Patient Dossier).

[Li *et al.*, 2015] discute sobre la necesidad de crear un sistema de intercambio de información entre los RCE's de los servicios de salud en Taiwan. Esto debido a que hay muchos problemas respecto a la excesiva utilización de recursos médicos y a la poca continuidad de la atención de la salud, por ejemplo, se menciona que hay información sobre resultados de pruebas de laboratorio que se encuentran duplicados, lo que implica que hubo un gasto innecesario de recursos.

En el articulo se exponen principalmente experiencias de hospitales que ofrecen un servicio de intercambio de información de RCE, reflejando así importantes ventajas de esto y evitando los problemas mencionados inicialmente, además se menciona que se facilita mucho el acceso a las personas a sus propios registros médicos.

[Kristianson *et al.*, 2009] menciona que el uso de los datos clínicos de los RCEs para la investigación clínica y para la evaluación de la calidad de la atención requiere de todo un proceso de extracción. Además señala que muchos esfuerzos han fracasado porque los datos extraídos parecían no estar estructurados, incompletos y plagados de errores. El problema clave fue la dificultad para localizar los datos, ya que no se reforzó ninguna forma estándar de introducir los datos en el sistema RCE. Finalmente los datos de laboratorio, la información sobre drogas y los datos de diagnóstico podían utilizarse directamente, mientras que otros datos, como los relativos a los signos vitales, requerían mucho trabajo para localizarlos y resultar útiles.

[9] `https://business.gov.nl/regulation/medical-devices/`

## 2.3. CONFIDENCIALIDAD

[Yu *et al.*, 2010] describe como los incisos de la ley HIPAA se pueden utilizar para proponer mecanismos de seguridad, tales como la firma digital. El objetivo principal de la investigación de los autores es proponer nuevos certificados de firma digital con el fin de proporcionar nuevos mecanismos más robustos para autenticar usuarios a un RCE. A su vez, mencionan a alto nivel posibles métricas para medir el nivel autenticación en RCEs.

[Griffith, 2019] discute cómo abordar la confidencialidad y la seguridad de los datos en los RCEs. En este artículo, el autor menciona la relevancia de las enfermeras en este contexto, lo que sugiere que la seguridad abarca a destinos roles en una institución de salud y también la necesidad de medir la confidencialidad para introducir mejoras al RCE.

[Renardi *et al.*, 2018] menciona algunos indicios de métricas que permiten medir el nivel de seguridad de un RCE en cuanto su tipo de encriptación de datos. Principalmente, los autores tienen como objetivo aplicar el proceso de criptografía, el cual que perturba y dificulta la velocidad de transmisión de datos.

El resultado demostró que los datos transmitidos podían ser seguros y que el proceso de cifrado no obstaculizaba el intercambio de datos.

[Kahn y Sheshadri, 2008] describe que la atención sanitaria de calidad significa cada vez más abordar la seguridad, la privacidad y la confidencialidad de los registros clínicos tanto en entornos alámbricos como inalámbricos. Este artículo intenta abordar estas preocupaciones presentando una comparación de los patrones de flujo de datos, esto en un entorno de atención médica electrónica junto con los de los consultorios médicos tradicionales, demostrando formas rentables en que los consultores de TI pueden ayudar a los proveedores de atención médica que trabajan en los RCE, manteniendo y administrando sus propias políticas de privacidad y seguridad.

## 2.4. SEGURIDAD EN ESPACIO DE TRABAJO

[Yeo *et al.*, 2012] discute que el estudio de los requisitos de seguridad para un sistema de RCE móvil se divide en consideraciones legales e investigaciones de seguridad seccionales. En el artículo se examinaron las consideraciones jurídicas relativas a los servicios médicos a distancia, la información personal de los pacientes y el RCE, los dispositivos médicos, el establecimiento de sistemas móviles y las aplicaciones móviles. Para las cuatro investigaciones de seguridad seccionales se utilizó el nivel de seguridad móvil SL-3 de las Normas de Seguridad para Teléfonos Inteligentes del Servicio Nacional de Inteligencia (NIS).

[Mcmullen *et al.*, 2014] menciona que los registros clínicos electrónicos (RCE/EMR) y los registros de salud electrónicos (EHR) se han convertido en sistemas esenciales, mediante los cuales las enfermeras profesionales (EP) comunican información vital sobre los pacientes a

otros miembros del equipo de atención de la salud, así como a los mismos pacientes. En este artículo se examinan las importantes distinciones entre los RCE/EMR y los EHR; se examina la génesis de estos tipos de registros; se resumen las disposiciones aplicables de la Ley de transferibilidad y responsabilidad de los seguros médicos de un reciente caso jurídico, centrado en la utilización por los profesionales de la enfermería de los RCE/EMR y los EHR; se aborda el acceso abierto de los pacientes a la información médica; y se examinan las amenazas a la seguridad.

## 2.5. DISPONIBILIDAD

[Edinger *et al.*, 2012] analiza la variación en la adopción de las funcionalidades de los RCEs y sus patrones de uso, las barreras para su adopción y los beneficios percibidos por la cantidad de médicos en ejercicio de un lugar determinado. Esto lo realizan mediante una encuesta por correo a una muestra aleatoria y representativa a nivel nacional de médicos en ejercicio, identificados en el *Physician Masterfile* de la Asociación Médica Americana.

El estudio comprueba que los médicos que ejercen en establecimientos pequeños tienen niveles bajos de adopción al RCE y que estos son menos propensos a usar estos sistemas.

[Williams y Boren, 2008] menciona que el registro clínico electrónico (RCE) no solo es bienvenido por los proveedores de servicios de salud como una forma de mejorar la calidad de la atención, sino que también sirve como un catalizador para el desarrollo. El propósito de este estudio es examinar los beneficios del RCE y su contribución final al desarrollo de la prestación de servicios de salud. Respecto a los resultados, estos indican la importancia de un sistema de RCE en los países en desarrollo para facilitar la recolección de datos, la introducción de datos, la recuperación de información y la generación de informes de manera eficaz y eficiente, así como la investigación. Sin embargo, los países desarrollados no están haciendo lo suficiente para ayudar a los países en vías de desarrollo a aplicar la tecnología moderna necesaria para facilitar la calidad de la atención.

## 2.6. REGISTRO CLÍNICO ELECTRÓNICO

El registro clínico electrónico (RCE) es un documento de carácter institucional correspondiente a todos los registros de la atención de los pacientes efectuados por el equipo de salud y que deben mantenerse en la ficha clínica. En general, este documento digital reúne información de relevancia de diferentes ámbitos del paciente, incluyendo referencias clínicas, administrativas, demográficas, de historial clínica, alergias, medicación, resultados de estudios y cuenta del paciente [Papoutsi *et al.*, 2015].

El RCE permite incluir toda la información contenida en un registro de salud tradicional, el perfil de salud, comportamiento e información ambiental del paciente. Además del conte-

nido, también incluye la dimensión del tiempo, que permite la inclusión de información a través de múltiples episodios y proveedores, que en última instancia, se desarrollarán en un registro de por vida.

En la literatura, existen dos conceptos muy similares al RCE, estos son:

- *Electronic Medical Record* (EMR): Es un registro electrónico relacionado con la salud de un paciente que puede ser creado, recopilado y mantenido, al que pueden acceder los médicos y otro personal autorizado dentro de una Institución de Salud [Tsai *et al.*, 2019]. Los EMR's están generalmente estrictamente asociados con médicos, hospitales o proveedores debido a las preocupaciones sobre la privacidad y la divulgación de información a terceros. El hecho de que los EMR's estén vinculados a médicos específicos, significa que estos no son capaces de intercambiar información de manera interoperable. Además, los EHR's mejoran el proceso general de atención de la salud pero no utiliza datos interoperables basados en estándares, por lo que no tiene un "uso significativo".
- *Patient Health Record* (PHR): Se trata de un registro electrónico relacionado con la salud de un paciente, que cumple con las normas de interoperabilidad y que puede ser extraído de múltiples fuentes mientras es administrado, compartido y controlado por el paciente [Daglish y Archer, 2009]. La información contenida en un PHR puede diferir un poco de la de un EHR porque los individuos pueden añadir datos por sí mismos, por ejemplo, información dietética o medicamentos sin receta.

A pesar de que estos registro difieren un poco en sus objetivos, ambos apuntan hacia el registro de datos médicos y personales de un paciente. Por lo que en este trabajo, se considera al PHR y EMR cuando se menciona y se estudia al RCE.

## 2.7. MÉTRICAS PARA EVALUAR LA SEGURIDAD DE LOS RCEs

Un estudio reciente apoyado por el CENS [Márquez *et al.*, 2020], propone un instrumento que, mediante métricas de seguridad transversales, permite medir la grado de satisfacción en la seguridad en los RCEs con el objetivo de que estos cumplan estándares de calidad y seguridad en software de RCE que ya se encuentren en uso en las Instituciones de Salud que lo hayan implementado. El instrumento está compuesto por cinco enfoques (o áreas) y diecinueve métricas de seguridad, estas fueron recogidas y caracterizadas a través del estudio de la literatura académica y gris relacionada al tema (ver figura 2)

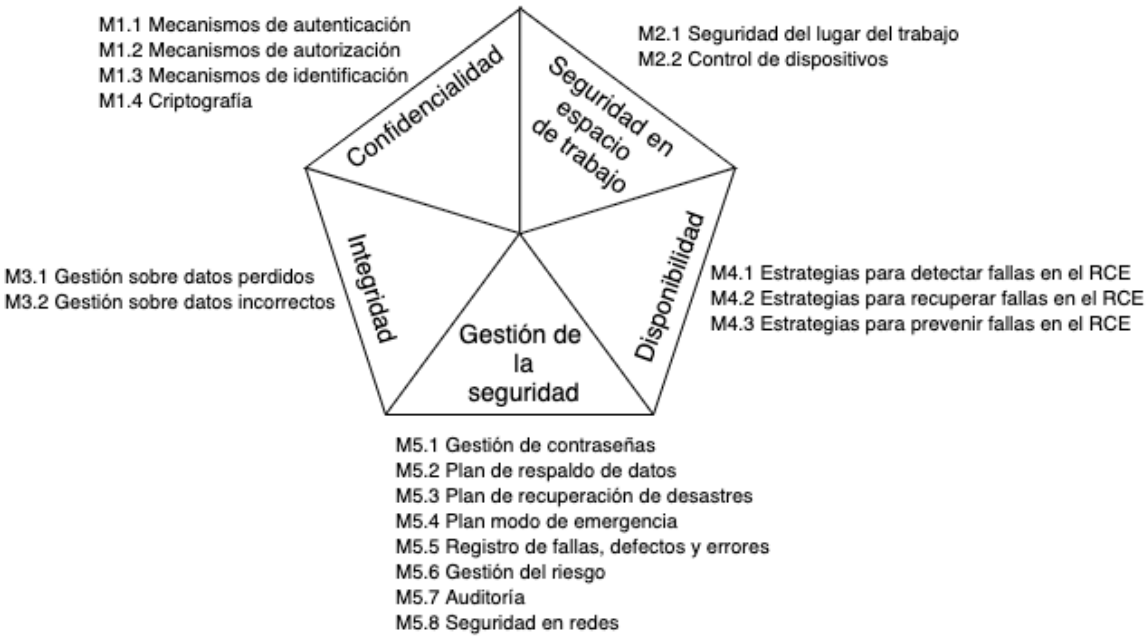


Figura 2: Representación del instrumento propuesto en [Márquez *et al.*, 2020]
Fuente: Elaboración propia.

### 2.7.1. MÉTODO DE EVALUACIÓN

Cada métrica es medida utilizando una escala de Likert. Según [Márquez *et al.*, 2020], esta escala corresponde un método de medición utilizado por investigadores con el objetivo de evaluar la opinión y actitudes de las personas. Dado que que el instrumento evalúa la seguridad de un RCE ya implementado en una Institución de Salud, la escala de Likert sirve para realizar mediciones y conocer sobre el grado de conformidad de una persona o encuestado hacia determinada oración afirmativa o negativa.

El puntaje final de la métrica se basa en el promedio de los valores de la escala por cada área, los cuales corresponden a los siguientes:

El puntaje de cada métrica, se basa en el valor asociado a cada opción de la escala de Likert, los cuales corresponden a los siguientes:

| **Escala de Likert** | **Valor** |
|---|---|
| Muy satisfecho | 5 |
| Satisfecho | 4 |
| Neutral | 3 |
| Insatisfecho | 2 |
| Totalmente Insatisfecho | 1 |

Tabla 1: Rango de valores para cada opción de la escala de Likert

Luego, en evaluación final, se promedian los valores seleccionados para cada métrica, obteniendo un puntaje por área, estos puntajes se deben promediar nuevamente para asignar el resultado final, el cual se describe a continuación:

| **Rango de valores** | **Resultado** |
|---|---|
| [5 - 4] | Muy suficiente |
| [3.9 - 3] | Suficiente |
| [2.9 - 2] | Insuficiente |
| [1.9 - 1] | Muy Insuficiente |

Tabla 2: Rango de valores para selección se resultado final

Donde el valor asociado al rango de valores, corresponde al puntaje promedio entre todas las áreas.

# CAPÍTULO 3
# PROPUESTA

Como se mencionó anteriormente, el objetivo es desarrollar una plataforma que evaluar la calidad de la seguridad de un RCE según el instrumento propuesto por [Márquez *et al.*, 2020], lo involucra la existencia de métricas de calidad, las cuales se dividen en áreas que las contienen. Esto debe ser medido mediante un método de evaluación que permita medir de forma discreta el grado de cumplimiento de cada métrica.

El método de evaluación propuesto consiste en la elaboración de una escala de Likert para calificar cada una de las métricas, las cuales al estar asociadas a un área, entregan un resultado promedio a partir de estas. Finalmente se calcula nuevamente un promedio. pero en este caso, del puntaje de las áreas que apliquen en la evaluación, lo que se traduce en un resultado en base a este puntaje final.

## 3.1. DOMINIO DEL PROBLEMA

La poca evidencia de la existencia de un instrumento de evaluación para los aspectos de seguridad de los RCEs, puede convertirse en un grave problema a mediano y largo plazo, si bien aún existen instituciones de salud que aún no poseen un RCE implementado, existe una gran cantidad que si lo tiene, por lo que es necesario implementar un instrumento que permita evaluar distintos aspectos de la característica más importante que se requiere para este tipo de sistemas, que es la seguridad. Lo anterior podría abordarse ya sea mediante una evaluaciones técnicas o a través de un instrumento de calidad que permita realizar un diagnostico general.

### 3.1.1. MODELO DE DOMINIO

A continuación (Fig, 3) se presenta el modelo de dominio. Este diagrama UML presentado por [Fowler *et al.*, 2002] tiene como objetivo ser un modelo conceptual de todo lo relacionado con el dominio del problema que se desea abordar a través de una propuesta de solución. En este diagrama se describen las entidades y atributos mas importantes, además de sus respectivas relaciones.

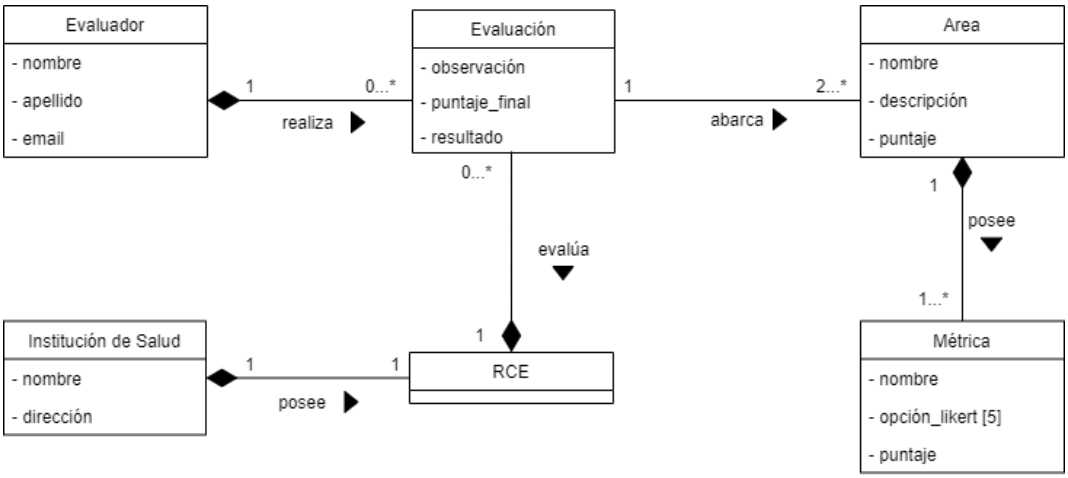


Figura 3: Modelo de dominio
Fuente: Elaboración propia.

El modelo de dominio explica la problemática a través de las entidades, atributos y relaciones expuestas. En principio, se tiene que el evaluador aplica una evaluación a un RCE, la cual también está relacionada a una Institución de Salud, además se puede apreciar que estas últimas cuatro entidades están fuertemente relacionadas, por lo que existe una dependencia entre ellas.
Por otro lado, se tiene que la evaluación abarca áreas que, a su vez, contienen las métricas que finalmente evalúan los distintos aspectos asociados a la seguridad, esto mediante una escala de Likert.

## 3.2. METODOLOGÍA DE DESARROLLO

Para el desarrollo de la plataforma, se propone utilizar prácticas asociadas a la metodología de desarrollo ágil (Agile Software Development)[10]. El flujo de trabajo de esta metodología (fig. 4) consiste en desarrollar funcionalidades de forma iterativa, con tal que se realice un proceso de feedback y mejora continua en cada ciclo. El objetivo finalmente es llegar a una plataforma cercana a lo que se busca, además de minimizar riesgos y cambios a gran escala que pudiesen generar, por ejemplo, una deuda técnica de gran volumen [Holvitie *et al.*, 2018].

[10] `https://www.agilealliance.org/agile101/`

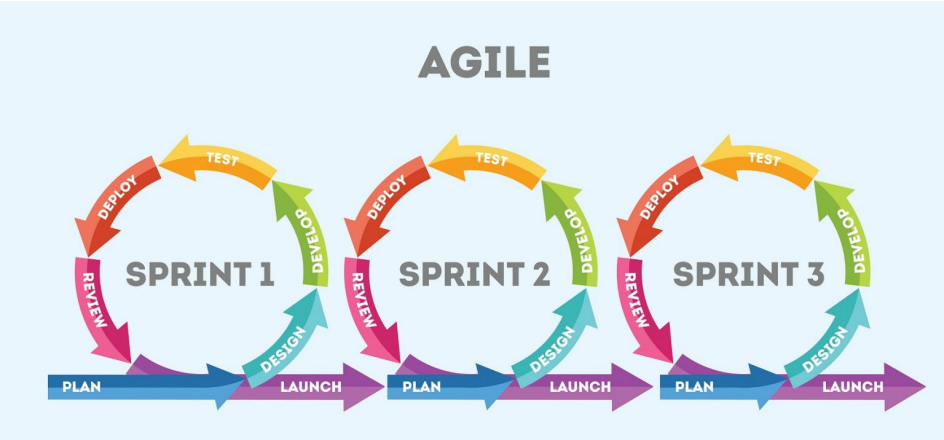


Figura 4: Flujo de trabajo del de la metodología de desarrollo ágil
Fuente: SolDevelo[11]

### 3.2.1. HISTORIAS DE USUARIO

Las historias de usuario[12] son una representación con enfoque ágil de los requisitos (ver en Anexos 6.1 y 6.2), ya que se trata una forma de conversar sobre estos, por lo que en este caso es una herramienta esencial para desarrollar las distintas funcionalidades de la plataforma propuesta.

Antes de definir las historias de usuario como tal, es importante establecer los roles principales para los usuarios de la plataforma. Estos se definen a continuación:

- **Administrador**: Encargado de gestionar usuarios, esto implica crear, eliminar y modificar usuarios. Además se encarga de gestionar las evaluaciones, esto significa que debe crear, asignar y eliminar evaluaciones, sin embargo, este no puede interferir en el proceso de aplicación de estas,
- **Evaluador**: Encargado de realizar las evaluaciones a las Instituciones de Salud.
- **Institución de Salud**: Entidad que posee un RCE a evaluar.

Cabe mencionar que el rol **"Usuario"** corresponde a una generalización de los mencionados anteriormente.

A continuación se presentan las historias de usuario propuestas y acordadas junto con CENS. La estructura de presentación utilizada es la siguiente:

- **(ID)** - Descripción HdU

[12] `https://www.agilealliance.org/glossary/user-stories/`

Primero se describen las HdU correspondiente al acceso de los Usuarios al sistema:

- **(Hdu-1)** - Como **Usuario**, quiero acceder a la plataforma con mis credenciales para que los datos asociados a mi perfil estén seguros.
- **(HdU-2)** - Como **Usuario**, quiero generar un documento a partir una evaluación completa para acreditar el resultado de esta.

Luego se describen las HdU asociadas al rol "**Administrador**":

- **(HdU-3)** - Como **Administrador**, quiero crear **Usuarios** para que puedan acceder al sistema.
- **(HdU-4)** - Como **Administrador**, quiero visualizar el perfil de los **Usuarios** para extraer información específica de cada uno.
- **(HdU-5)** - Como **Administrador**, quiero editar la información de los **Usuarios** para mantener sus datos actualizados.
- **(HdU-6)** - Como **Administrador**, quiero eliminar **Usuarios** para restringir el acceso de estos a la plataforma.
- (**HdU-7)** - Como **Administrador**, quiero crear evaluaciones para que los **Evaluadores** puedan aplicarlas a una **Institución de Salud**.
- (**HdU-8)** - Como **Administrador**, quiero eliminar evaluaciones para invalidarlas en caso de que sea necesario.
- (**HdU-9)** - Como **Administrador**, quiero ver el detalle de las evaluaciones para saber el progreso de estas.
- **(HdU-10)** - Como **Administrador**, quiero buscar **Instituciones de Salud** para poder encontrarlas de forma rápida.
- **(HdU-11)** - Como **Administrador**, quiero visualizar un resumen general de los estados de las evaluaciones existentes para tomar una decisión al respecto.

Postriormente se describen las HdU asociadas al rol "**Evaluador**":

- **(HdU-12)** - Como **Evaluador**, quiero visualizar un resumen general de los estados de las evaluaciones asignadas para poder tener información respecto al avance de estas.
- **(HdU-13)** - Como **Evaluador**, quiero visualizar la lista de evaluaciones asignadas para acceder a cada una.

- **(HdU-14)** - Como **Evaluador**, quiero acceder a las evaluaciones asignadas para poder aplicarlas a la **Institución de Salud** correspondiente.
- **(HdU-15)** - Como **Evaluador** quiero agregar un comentario a la evaluación para poder entregar un feedback general.
- **(HdU-16)** - Como **Evaluador**, quiero agregar un comentario asociado a la evaluación de cada área para poder entregar un feedback específico.
- **(HdU-17)** - Como **Evaluador**, quiero calificar una métrica asociada a una área mediante un puntaje en escala de Likert para establecer un grado de satisfacción.
- **(HdU-18)** - Como **Evaluador**, quiero calificar una métrica asociada con una opción excluyente para poder descartarla en casos particulares.
- **(HdU-19)** - Como **Evaluador**, quiero buscar **Instituciones de Salud** para poder encontrarlas de forma rápida.

Finalmente se describen las HdU relacionadas con el rol "**Institución de Salud**"

- **(HdU-20)** - Como **Institución de Salud**, quiero visualizar la lista de evaluaciones para acceder a cada una.
- **(HdU-21)** - Como **Institución de Salud**, quiero leer el detalle de las evaluaciones completadas para conocer el resultado y el feedback que pueda existir.

## 3.3. ARQUITECTURA Y DISEÑO DE LA PLATAFORMA

Para el diseño de la arquitectura de la plataforma, es importante tener en cuenta algunos puntos relevantes a la hora de seleccionar patrones de diseño o arquitectura como tal. Estos tienen que ver con el contexto en el que se desarrollará este sistema y en la metodología que se utilizará para ello.

Existen muchos patrones que ayudan principalmente a la reutilización y mantenibilidad del código, así como también a la escalabilidad de la solución que se esté desarrollando. [Fowler *et al.*, 2002], por ejemplo, nos ofrece un abanico de patrones de diseño y arquitectura utilizados de forma muy frecuente en la industria. uno de ellos es Modelo-Vista-Controlador (Model-View-Controller) o en su defecto, MVC.

Este patrón de arquitectura permite separar la capa de datos y la lógica del negocio (modelo) con la representación de esta (vista), esto mediante un módulo intermedio que es el controlador, quien se encarga de gestionar los datos que van a una determinada vista según la regla de negocio establecida. En la fig. se puede apreciar una representación del flujo con el que trabaja MVC.

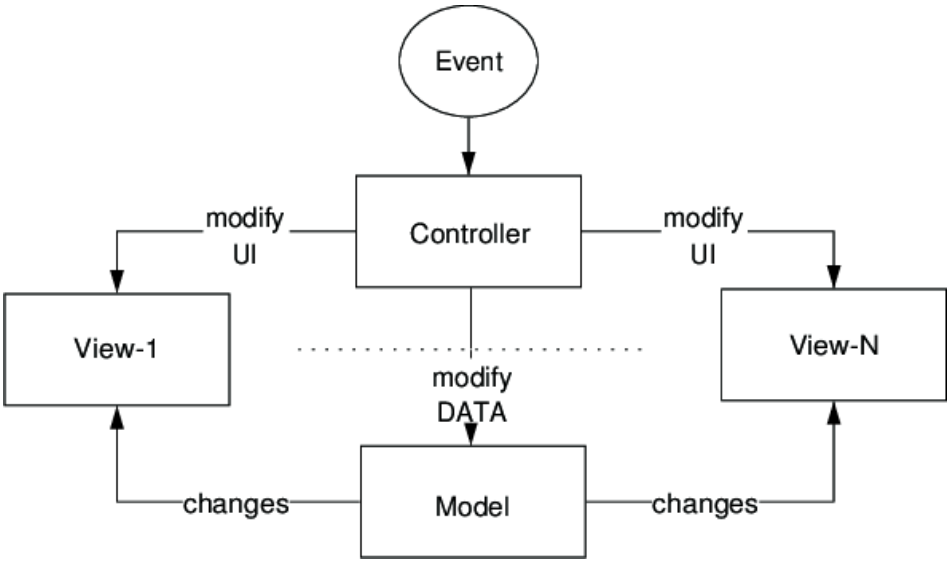


Figura 5: Model-View-Controller
Fuente: [Wielemaker, 2021].

Una de las ventajas mas importantes de este patrón de arquitectura es la modularidad que entrega a cada uno de los elementos que lo componen, esto al mismo tiempo facilita el mantenimiento de cada elemento y la escalabilidad del sistema. Además, esto facilita el desarrollo ágil, ya que permite generar o modificar componentes de forma iterativa e incremental según sea el caso.

### 3.3.1. DIAGRAMA DE CLASES

A continuación (fig. 6) se presenta el diagrama de clases propuesto para la plataforma. Este diagrama tiene como objetivo describir la estructura del sistema a través de las distintas clases y componentes que estarán presentes en el desarrollo. Para este caso se presenta un diagrama simplificado, el cual contiene solamente los atributos y componentes más importantes, sin embargo, las clases no contienen métodos, ya que estos serán definidos en la etapa de implementación.

En el diagrama se puede apreciar la dependencia que existe entre la mayoría de las clases, además de los componentes asociados al patrón MVC (vistas y controladores), los cuales se encuentran asociados cada uno a su modelo correspondiente.

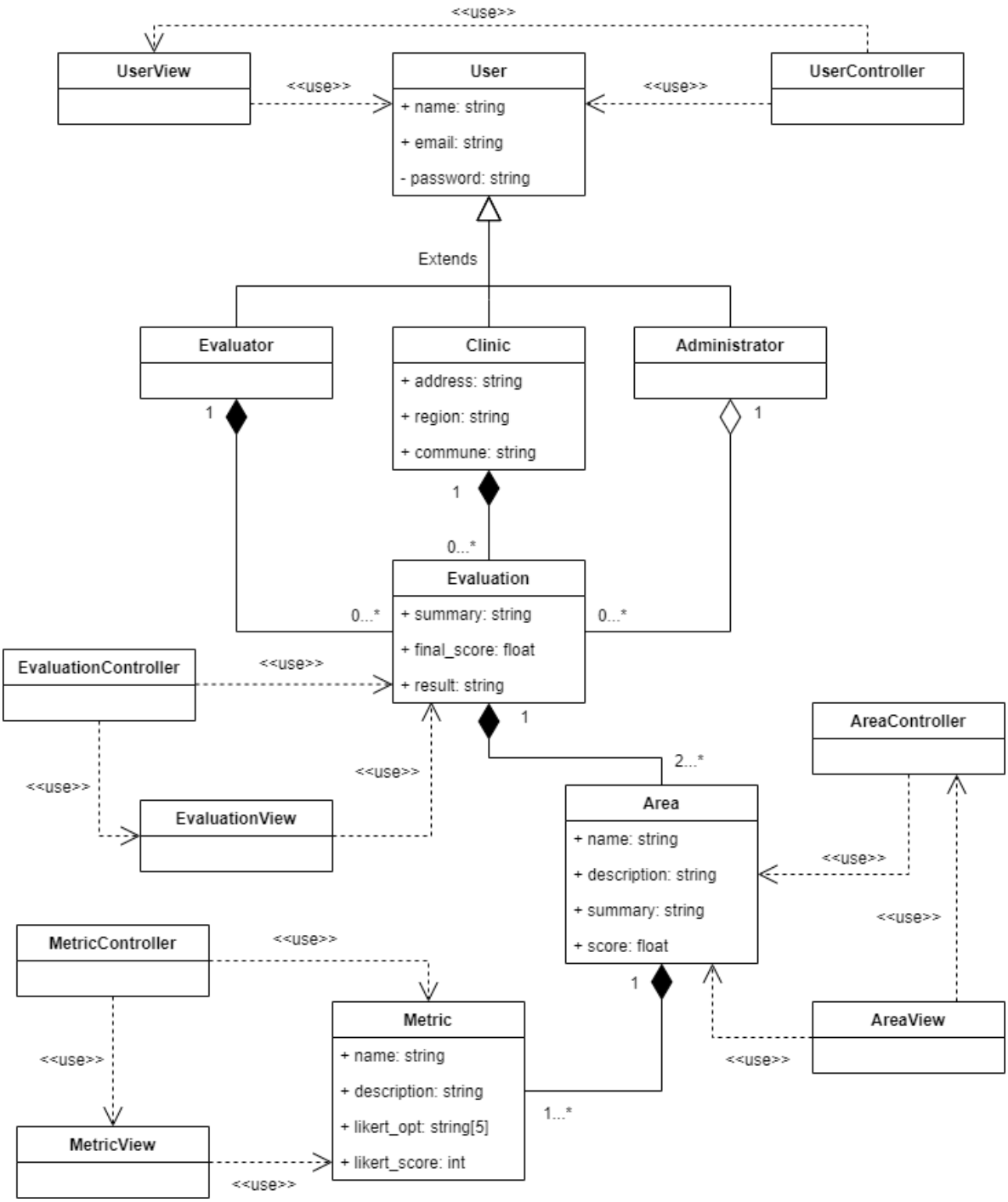


Figura 6: Diagrama de clases propuesto
Fuente: Elaboración propia.

### 3.3.2. MODELO DE DATOS

El modelo de datos propuesto (fig, 7) está basado en una base de datos relacional (SQL). Una de las razones por la cual se decide proponer este tipo de BD es por la gran capacidad de lectura que poseen al manejar tablas relacionadas, lo que sería ventaja, por ejemplo, al momento de generar estadísticas asociadas a los puntajes de las métricas y evaluaciones aplicadas.

Otro punto importante es que bajo el contexto de la plataforma, no es necesario almacenar grandes volúmenes de datos y estructurarlos de forma compleja. En este caso, los datos están fuertemente relacionados y estructurados, por lo que se descartaría por ahora un eventual uso de una base de datos NoSQL.

[Cattell, 2010] realiza una comparación entre los gestores de bases de datos mencionados, donde se mencionan, entre otros, los puntos expuestos anteriormente.

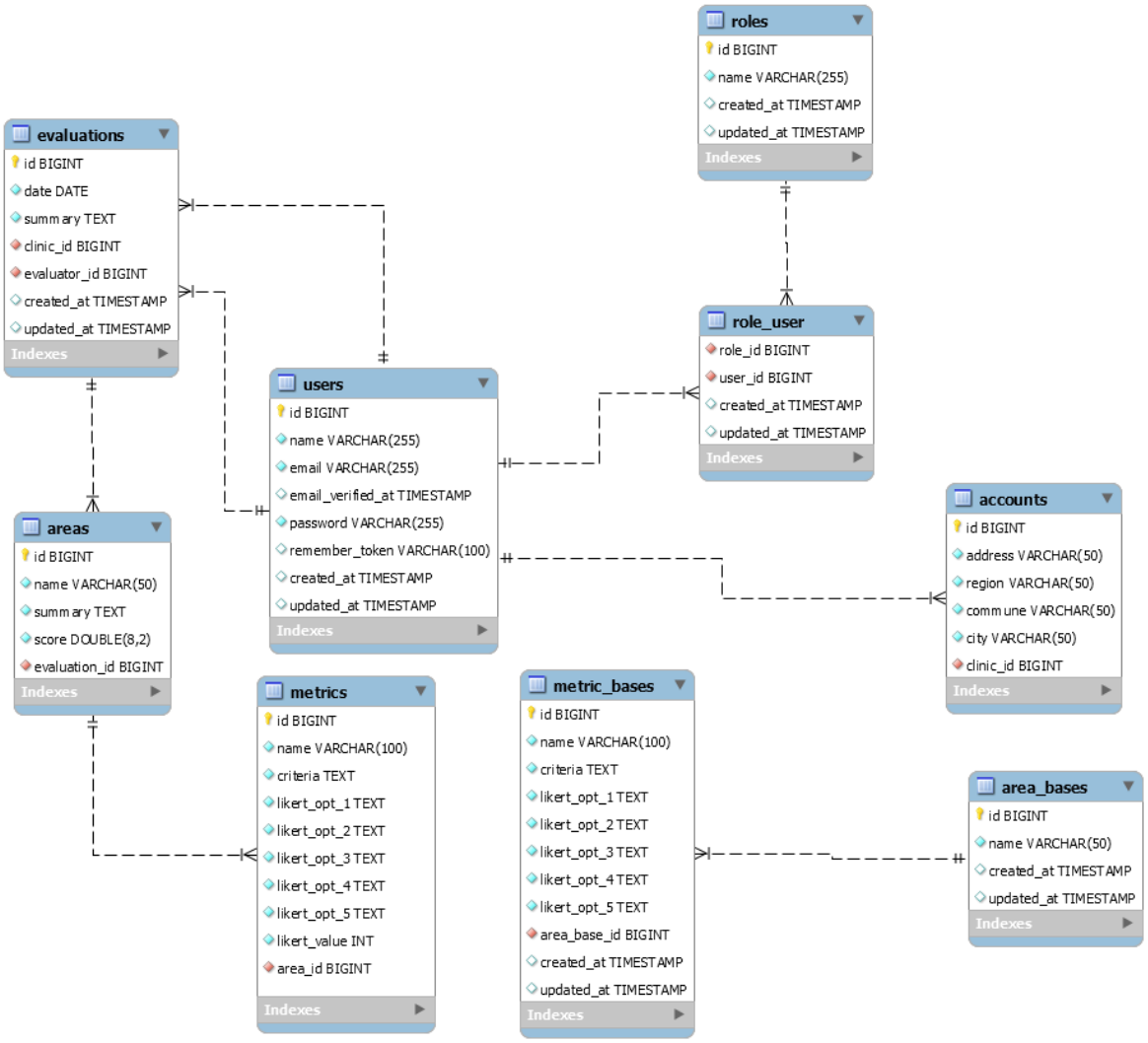


Figura 7: Modelo de datos propuesto
Fuente: Elaboración propia.

Algunos puntos importantes sobre el modelo de datos propuesto:

- Las tablas *metric_bases* y *area_bases* corresponden a los modelos que se cargarán a las tablas *metrics* y *areas* respectivamente cuando se cree una evaluación. Esto permite poder cargar nuevos modelos de evaluación en las tablas *bases* que incluyan, por ejemplo, mas áreas y/o mas métricas, por lo que se podría a futuro seleccionar un modelo de evaluación entre varios cargados para inicializar las evaluaciones.
- La relación M:N entre la tabla *users* y la tabla *roles*, es una decisión pensada para escalabilidad de la plataforma, ya que el manejo de roles se hace mas dinámico y permitiría en el futuro manejar usuarios con múltiples roles, sin embargo, por ahora solo se limitarán a tener un rol asociado.

# CAPÍTULO 4
# IMPLEMENTACIÓN

## 4.1. TECNOLOGÍAS UTILIZADAS

Las tecnologías utilizadas para desarrollo de la plataforma fueron seleccionadas principalmente en base a la metodología de trabajo, la arquitectura propuesta y la escalabilidad a nivel de código, este último punto es muy importante, ya que la plataforma desarrollada corresponde a una primera versión, por lo que es de esperar que a futuro se sigan implementando nuevas funcionalidades en base al código desarrollado.

### 4.1.1. MYSQL

El gestor de bases de datos relacional MySQL[13] es considerado uno de los mas populares en general. Entre sus grandes características se encuentra la seguridad de datos que brinda, el soporte que posee para procesos transaccionales y la gran velocidad de lectura de datos. También es importante destacar que este RDBMS permite realizar roll-backs, por lo que brinda una capacidad de recuperación frente a accidentes que puedan ocurrir.

Bajo el contexto de la plataforma a desarrollar, este RDBMS permitirá, por ejemplo, mantener a largo plazo un gran volumen de datos de forma segura y de rápido acceso. Por lo que será muy útil a la hora de realizar estudios basados en analítica a partir de un modelo de evaluación.

### 4.1.2. LARAVEL

Laravel[14] es un framework web escrito en PHP que se ha hecho bastante popular estos últimos años debido a la arquitectura modular que posee, lo que permite un desarrollo rápido y organizado. Además, la modularidad permite implementar funcionalidades de forma fácil y que, sumado a la gran documentación que posee, permite generar una gran compatibilidad con la metodología de desarrollo ágil.

Otra de las grandes características de este framework es que permite implementar de forma casi nativa el patrón MVC, esto a través de modelos que, al estar integrados con el ORM Eloquent, permite manejar los datos a través de clases y métodos, esto gracias uso del patrón Active Record [Fowler *et al.*, 2002]. También permite crear controladores que habitualmente utilizan uno o mas modelos para enviar datos a las vistas, las cuales son representadas

[13] `https://www.mysql.com/`
[14] `https://laravel.com/`

a través de un motor de plantillas llamado Blade. Este motor permite modularizar y reutilizar código en las vistas, además facilita el manejo de los datos a través de variables PHP y funciones embebidas que generan código HTML de forma dinámica.

### 4.1.3. VUE.JS

Este framework[15] de front end escrito en JavaScript permite implementar interfaces de usuario dinámicas y de forma modular, también permite agregar funcionalidades dinámicas a las plantillas Blade, esto a través de componentes y/o paquetes externos. Cabe destacar que esta herramienta viene integrada a Laravel en sus últimas versiones, por lo que es un stack de tecnologías bastante popular.

### 4.1.4. TAILWINDCSS

TailwindCSS[16] es un framework de CSS que permite aplicar estilos a las vistas de forma rápida y dinámica. La forma en la que opera es mediante clases de HTML que generan automáticamente el código CSS, lo que permite crear componentes de UI de forma rápida y sencilla.

## 4.2. PROCESO DE DESARROLLO

A lo largo del proceso de desarrollo, se utilizaron distintas prácticas y elementos de metodologías ágiles, las cuales se detallan a continuación:

- **Desarrollo iterativo-incremental**: Consiste en repetir un proceso de trabajo similar en iteraciones, en el cual se debe ir evolucionando el producto a desarrollar, por lo que es importante ir mejorando y agregando funcionalidades en cada iteración. Esta práctica es utilizada en metodologías ágiles como Scrum[17] y XP[18].
- **Product y Sprint Backlog**: Consiste en ser una lista de caracterísicas priorizadas, donde cada una se relata de forma breve (HdU), posteriormente y a medida que van pasando los Sprints, se van seleccionando las características según su prioridad, para ser trasladadas al Sprint Backlog correspondiente. Esta herramienta es utilizada en Scrum.
- **Scrum board**: Herramienta para organizar el Product Backlog. Consiste en agrupar las características que se van desarrollando en columnas estilo Kanban[19]. Para este caso

[15] https://vuejs.org/
[16] https://tailwindcss.com/
[17] https://www.scrum.org/
[18] http://www.extremeprogramming.org/start.html
[19] https://kanboard.org/

se utilizó la plataforma Trello[20] como herramienta.

- **Scrum Sprint**: Corresponde a ser un periodo de tiempo fijo (en lo posible) y repetible, en el cual se debe desarrollar el producto a partir de las características definidas en el Product Backlog.

Un punto importante a destacar es que muchos de los elementos aplicados en el desarrollo de la plataforma fueron extraídos de Scrum. Esta metodología se compone de variadas prácticas para gestionar un proceso de desarrollo ágil, sin embargo, para la mayoría es necesario conformar un equipo de desarrollo con múltiples roles para llevarlas a cabo. En la fig. 8 se puede apreciar la interacción de algunas de las actividades asociadas a un Sprint.

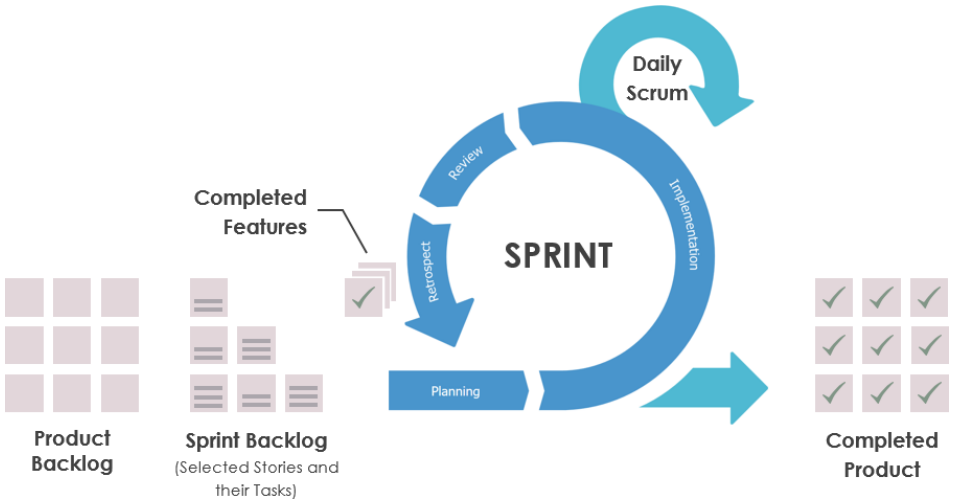


Figura 8: Representación de un Sprint en Scrum
Fuente: Visual-Paradigm[21].

## 4.3. DESARROLLO DE SPRINTS

Descripción de lo desarrollado en cada Sprint según historias de usuario definidas.

El desarrollo de la plataforma se divide en 3 Sprints, cada uno de aproximadamente 4 semanas. A continuación se detalla cada uno con su objetivo y las Historias de Usuario asignadas a cada iteración.

[20] https://trello.com/

### 4.3.1. PRIMER SPRINT

Este Sprint tiene como objetivo desarrollar principalmente el flujo de la evaluación 9 y luego, el acceso a usuarios mediante un login.

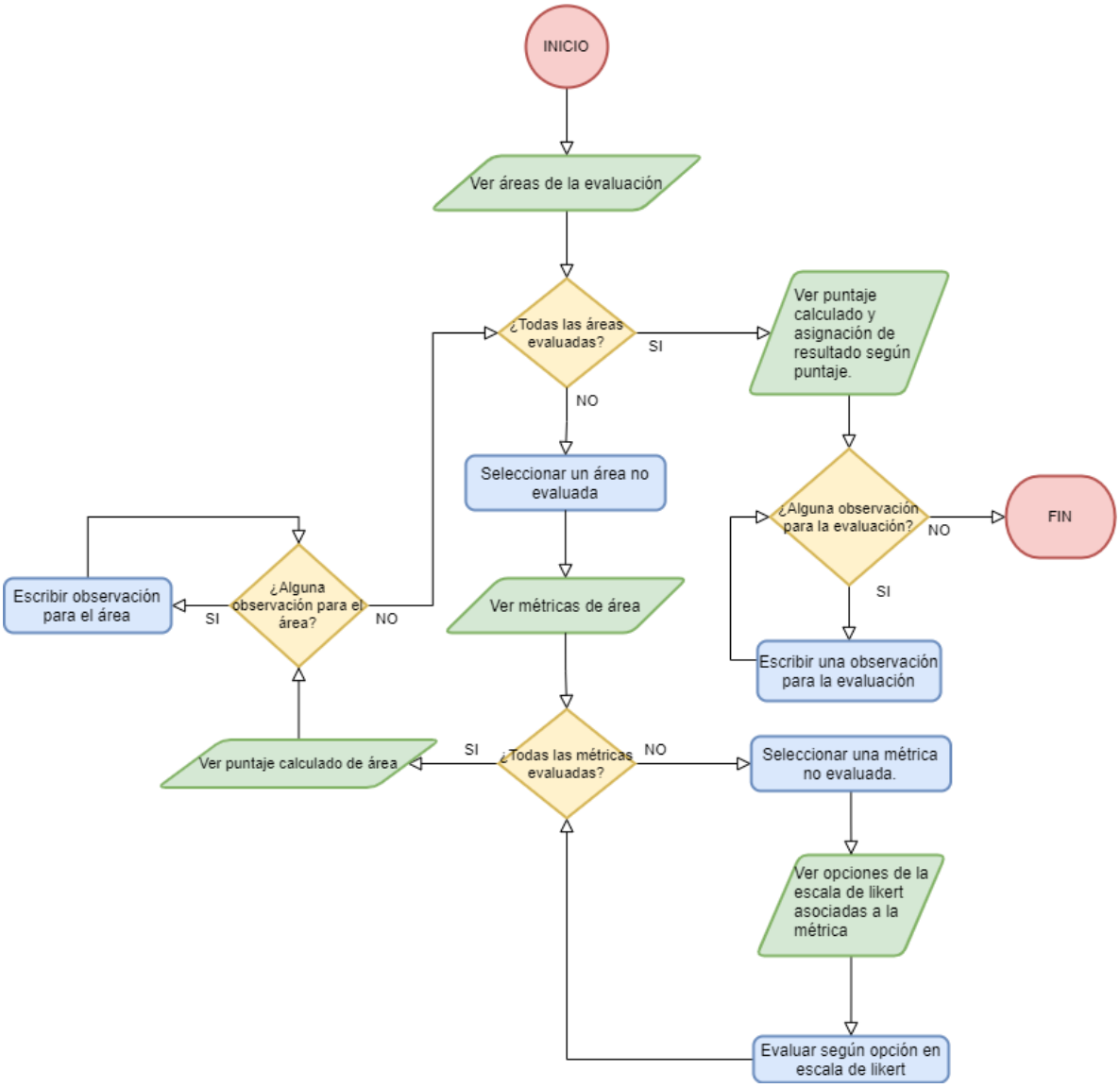


Figura 9: Diagrama de flujo de evaluación propuesto
Fuente: Elaboración propia.

Inicialmente se implementó el modelo de datos presentado en el capitulo anterior, esto a través de las migraciones de Laravel, las cuales permiten crear las tablas y sus respectivos atributos, que posteriormente, podrán asociarse a un modelo gracias a Eloquent. Luego, se crearon los modelos asociados a cada una de las tablas junto sus respectivos controladores

y vistas.

Por otro lado, también se crearon los endpoints (API REST)[22] utilizados para cada petición HTTP, estos están asociados a cada uno de los métodos de un controlador específico y permiten acceder a los distintos recursos que disponen las vistas. Los endpoints desarrollados se detallan en la tabla 3.

Cabe destacar que los 2 últimos endpoints fueron creados, en principio, para que el evaluador pueda crear sus evaluaciones, sin embargo, para el tercer Sprint, esta regla de negocio fue modificada para que el Administrador sea quien cree y asigne las evaluaciones.

También es importante mencionar que los endpoints que poseen restricciones respecto a sus roles, fueron protegidos mediante un middleware[23] tanto para la autenticación, como para los roles de cada Usuario.

[22] `https://restfulapi.net/`
[23] `https://laravel.com/docs/6.x/middleware`

| **API Endpoint** | **Descripción** | **Roles permitidos** |
|---|---|---|
| *GET /login* | Retorna la vista de login para Usuarios, la cual corresponde a la vista de bienvenida la plataforma. | Todos |
| *POST /login* | Recibe credenciales de Usuario y redirecciona a vista correspondiente según rol. | Todos |
| *GET /evaluation* | Retorna todas las evaluaciones asociadas al Usuario. | Usuarios |
| *GET /evaluation/{ev_id}* | Retorna la información de la evaluación con identificador {ev_id}, junto con todos los datos asociados a esta (áreas, métricas, etc.) | Usuarios |
| *GET /evaluation/{ev_id}/areas/{area_id}* | Retorna la información del área {area_id}, asociada a la evaluación {ev_id}, relativa a la evaluación realizada. | Usuarios |
| *GET /evaluation/{ev_id}/areas/{area_id}/metric/{metric_id}* | Retorna la información de la métrica {metric_id}, asociada al área {area_id} y a la evaluación {ev_id}, relativa a la evaluación realizada. | Usuarios |
| *PUT /evaluation/{ev_id}* | Recibe información de la evaluación (observación general) para ser actualizada. | Evaluador |
| *POST /evaluation/{ev_id}/areas/{area_id}* | Recibe información del área evaluada (observación específica) para ser almacenada. | Evaluador |
| *POST /evaluation/{ev_id}/areas/{area_id}/metric/{metric_id}* | Recibe información de la métrica evaluada (opción seleccionada y puntaje de escala de Likert) para ser almacenada. | Evaluador |
| *GET /evaluation/create* | Retorna información necesaria para crear una evaluación (Instituciones de Salud) | Evaluador* |
| *POST /evaluation* | Recibe información de la evaluación, para ser creada y almacenada. | Evaluador* |

Tabla 3: Endpoints desarrollados en Sprint 1

Finalmente, en este primer Sprint se desarrollaron las siguientes Historias de Usuario:

- **(HdU-1)** - Como **Usuario**, quiero acceder a la plataforma con mis credenciales para que los datos asociados a mi perfil estén seguros.
- **(HdU-13)** - Como **Evaluador**, quiero visualizar la lista de evaluaciones asignadas para acceder a cada una

- **(HdU-14)** - Como **Evaluador**, quiero acceder a las evaluaciones asignadas para poder aplicarlas a la Institución de Salud correspondiente.
- **HdU-15)** - Como **Evaluador**, quiero agregar un comentario a la evaluación para poder entregar un feedback general.
- **(HdU-16)** - Como **Evaluador**, quiero agregar un comentario asociado a la evaluación de cada área para poder entregar un feedback específico.
- **(HdU-17)** - Como **Evaluador**, quiero calificar una métrica asociada a una área mediante un puntaje en escala de Likert para establecer un grado de satisfacción.
- **(HdU-20)** - Como **Institución de Salud**, quiero visualizar la lista de evaluaciones para acceder a cada una.
- **(HdU-21)** - Como **Institución de Salud**, quiero leer el detalle de las evaluaciones completadas para conocer el resultado y el feedback que pueda existir.

### 4.3.2. SEGUNDO SPRINT

El segundo Sprint tiene como objetivo ser el punto de desarrollo inicial para todo lo relacionado a la gestión de la plataforma, por lo que se priorizó implementar los componentes relacionados a la creación, visualización y edición de Usuarios por parte del Administrador.

Por otro lado, también se implementaron elementos relacionados a las evaluaciones, como la exportación del documento PDF que acredita la evaluación, en el cual se detallan todos los elementos asociados a la evaluación cuando está completada (puntajes, observaciones y resultado).
Otro elemento importante es el resumen general de los estados de evaluaciones, el cual servirá para que el Usuario tenga una idea de cuantas evaluaciones aún están pendientes y cuantas se han completado. Cabe destacar que esta última funcionalidad mencionada, utiliza el endpoint *GET /evaluation* realizado en el primer Sprint, pero con la información de los estados de las evaluaciones, se generó un gráfico con TailwindCSS para mostrar el resumen.

A continuación se describen los endpoints desarrollados en este Sprint:

| API Endpoint | Descripción | Roles permitidos |
|---|---|---|
| *GET /user* | Retorna todos los Usuarios existentes en el sistema. | Administrador |
| *GET /user/{user_id}* | Retorna la información del Usuario {user_id} | Usuario |
| *GET /user/create* | Retorna la información necesaria para poder crear un Usuario (roles, comunas y regiones) | Administrador |
| *POST /user* | Recibe la información necesaria para poder crear un Usuario y almacenarlo. | Administrador |
| *GET /user/{user_id}/edit* | Retorna la información necesaria para poder editar un Usuario {user_id}. | Administrador |
| *PUT /user/{user_id}* | Recibe la información necesaria para poder editar un Usuario {user_id}. | Administrador |
| *GET /evaluation/{ev_id}/pdf* | Retorna la información de una evaluación completada {ev_id} en un documento PDF. | Usuario |

Tabla 4: Endpoints desarrollados en Sprint 2

Finalmente, en este segundo Sprint se desarrollaron las siguientes Historias de Usuario:

- **(HdU-2)** - Como **Usuario**, quiero generar un documento a partir una evaluación completa para acreditar el resultado de esta.
- **(HdU-3)** - Como **Administrador**, quiero crear Usuarios para que puedan acceder al sistema
- **(HdU-4)** - Como **Administrador**, quiero visualizar el perfil de los **Usuarios** para extraer información específica de cada uno.
- **(HdU-5)** - Como **Administrador**, quiero editar la información de los **Usuarios** para mantener sus datos actualizados
- **(HdU-11)** - Como **Administrador**, quiero visualizar un resumen general de los estados de las evaluaciones existentes para tomar una decisión al respecto.
- **(HdU-12)** - Como **Evaluador**, quiero visualizar un resumen general de los estados de las evaluaciones asignadas para poder tener información respecto al avance de estas.

### 4.3.3. TERCER SPRINT

En este último Sprint se prioriza el desarrollo de la gestión de la plataforma respecto a las evaluaciones, ya que para este Sprint se cambia una regla de negocio importante respecto a la creación de evaluaciones. En el primer Sprint, el evaluador era el encargado de crear sus propias evaluaciones, sin embargo, esto cambia para este Sprint, ya que será el Administrador quien tendrá esa responsabilidad. Además se implementa la opción de poder eliminar una evaluación, esto en caso de que se haya creado una por accidente o para dejar sin efecto alguna evaluación aplicada.

Respecto a la evaluación como tal, también se implementa la opción "No Aplica" para la selección de puntaje de las métricas, de forma que estas puedan excluirse dado algún contexto en particular del RCE y/o de la Institución de Salud.

Por otro lado, y para completar la gestión de usuarios, se desarrolla la opción de "eliminar", sin embargo en realidad los usuarios quedan desactivados, de forma que los datos relacionados que sean de relevancia, no sean eliminados.

Como último punto, también se desarrolla un buscador de instituciones salud, con el objetivo de poder encontrarlas rápidamente.

Los endpoints desarrollados en este Sprint son los siguientes:

| **API Endpoint** | **Descripción** | **Roles permitidos** |
|---|---|---|
| *DELETE /user/{user_id}* | Elimina (desactiva) al usuario {user_id} | Administrador |
| *GET /evaluation/create* | Retorna información necesaria para crear una evaluación (Evaluadores e Instiuciones de Salud) | Administrador |
| *POST /evaluation* | Recibe información de la evaluación, para ser creada y almacenada. | Administrador |
| *DELETE /evaluation/{ev_id}* | Elimina la evaluación {ev_id} | Administrador |

Tabla 5: Endpoints desarrollados en Sprint 3

Finalmente, en este último Sprint, se desarrollaron las siguientes Historias de Usuario:

- **(HdU-6)** - Como **Administrador**, quiero eliminar **Usuarios** para restringir el acceso de estos a la plataforma.
- **(HdU-7)** - Como **Administrador**, quiero crear evaluaciones para que los **Evaluadores** puedan aplicarlas a una **Institución de Salud**.
- **(HdU-8)** - Como **Administrador**, quiero eliminar evaluaciones para invalidarlas en caso de que sea necesario.

- **(HdU-9)** - Como **Administrador**, quiero ver el detalle de las evaluaciones para saber el progreso de estas.
- **(HdU-10)** - Como **Administrador**, quiero buscar **Instituciones de Salud** para poder encontrarlas de forma rápida.
- **(HdU-18)** - Como **Evaluador**, quiero calificar una métrica asociada con una opción excluyente para poder descartarla en casos particulares.
- **(HdU-19)** - Como **Evaluador**, quiero buscar **Instituciones de Salud** para poder encontrarlas de forma rápida.

Notas:

- Para la **HdU-9**, se utilizó el endpoint *GET /evaluación/{ev_id}*, junto con las mismas vistas implementadas en el Sprint 1.
- Para la **HdU-18**, se modificó el método que realiza el cálculo de los puntajes para cada área en el modelo correspondiente.

# CAPÍTULO 5
# VERIFICACIÓN

Previo al desarrollo de la plataforma, se realizó una prueba de concepto para CENS, la cual consistió en realizar la evaluación del área de Confidencialidad al Registro Clínico Electrónico del Hospital Digital de Chile[24]. Este RCE para ese entonces aún estaba en desarrollo, por lo que la aplicación de la evaluación se realizó sobre las especificaciones técnicas que se requirieron en la licitación [25], por lo que la prueba de concepto fue aplicada bajo esos criterios técnicos.

A continuación se muestran los resultados de la evaluación realizada para las métricas del área Confidencialidad:

| **Métrica** | **Puntaje** |
|---|---|
| Mecanismos de autenticación | 5 |
| Mecanismos de autorización | 4 |
| Mecanismos de identificación | 4 |
| Criptografía | 3 |
| **Total** | **4** |
| **Resultado** | **Muy suficiente** |

Tabla 6: Resultado de evaluación de RCE para el Hospital Digital de Chile en área Confidencialidad

Los comentarios del evaluador fueron los siguientes:

- Se sugiere implementar un mecanismos de autorización automáticos para el RCE.
- Se sugiere implementar al menos un mecanismo de identificación adicional para el RCE.
- Se debe especificar el método de criptografía que se utiliza en caso de hacerlo.

## 5.1. VERIFICACIÓN DE SPRINTS

En cada uno de los Sprints, se realizó un demo de la plataforma para verificar las Historias de Usuario implementadas con el CENS, además mediante estas instancias se recibía el feedback de parte de CENS para mejorar algunos aspectos y/o realizar cambios respecto a las reglas de negocio, funcionalidades o estéticos.

[24] `https://www.hospitaldigital.gob.cl/`
[25] Acceso a recursos de licitación

A continuación se mencionan las Historias de Usuario desarrolladas por Sprint y su respectiva captura de la plataforma.

### 5.1.1. PRIMER SPRINT

En este Sprint se presentan funcionalidades relacionadas al acceso de Usuarios y a la interacción de estos con las Evaluaciones en base al Rol.

- Login: HdU-1.

Figura 10: Vista de login. Con logo y colores institucionales del CENS.

- Visualizar evaluaciones asignadas: HdU-13 y HdU-20.

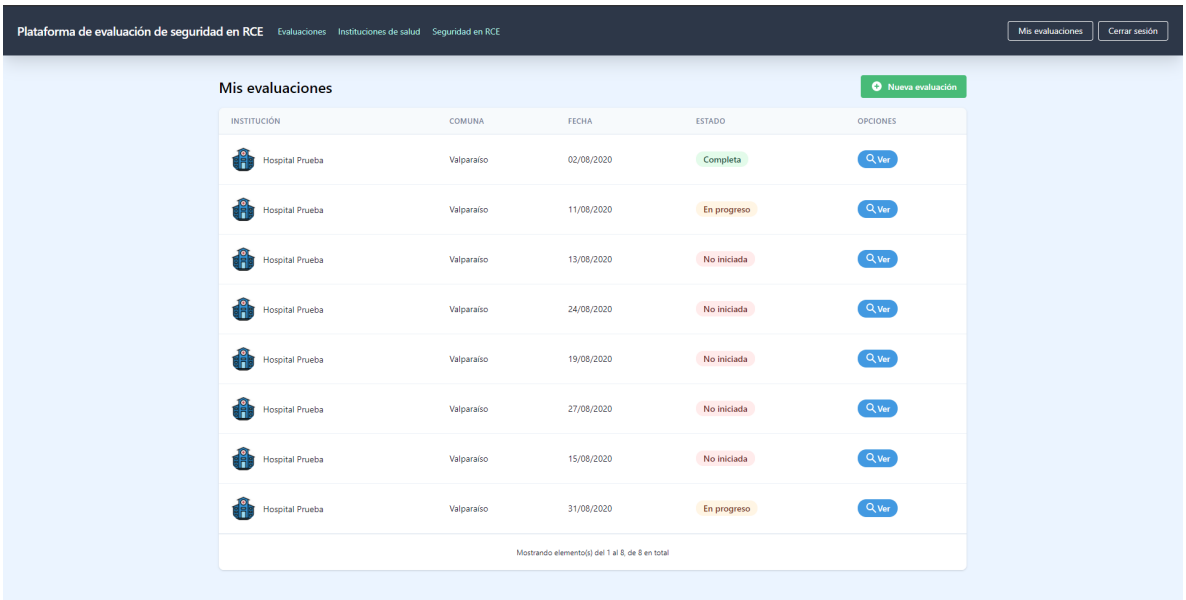


Figura 11: Vista de lista de evaluaciones asignadas al Evaluador

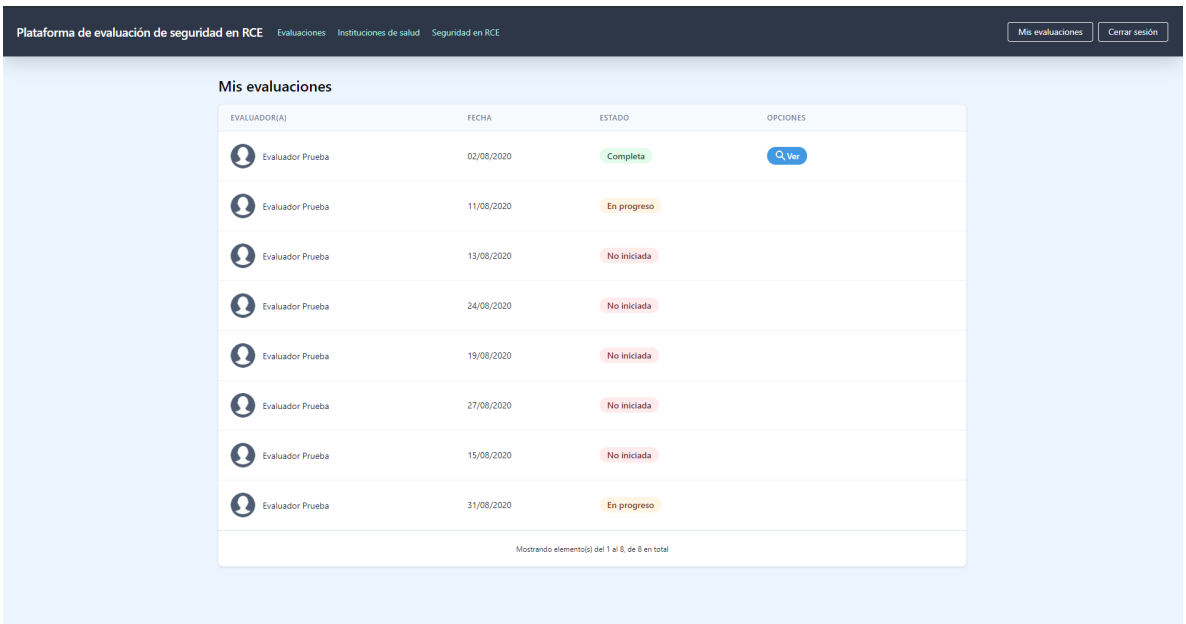


Figura 12: Vista de lista de evaluaciones asignadas a una Institución de Salud

En las tablas, se puede apreciar la columna “Estado”, la cual se compone de 3 estados distintos: Completa, En progreso y No iniciada. El estado de una evaluación se actualiza cada vez que se realiza la evaluación de una métrica.

Además una Institución de Salud no puede revisar el detalle de la evaluación a menos que esté completada.

- Flujo de aplicación de evaluación: HdU-14. HdU-15, HdU-16, HdU-17 y HdU-21.

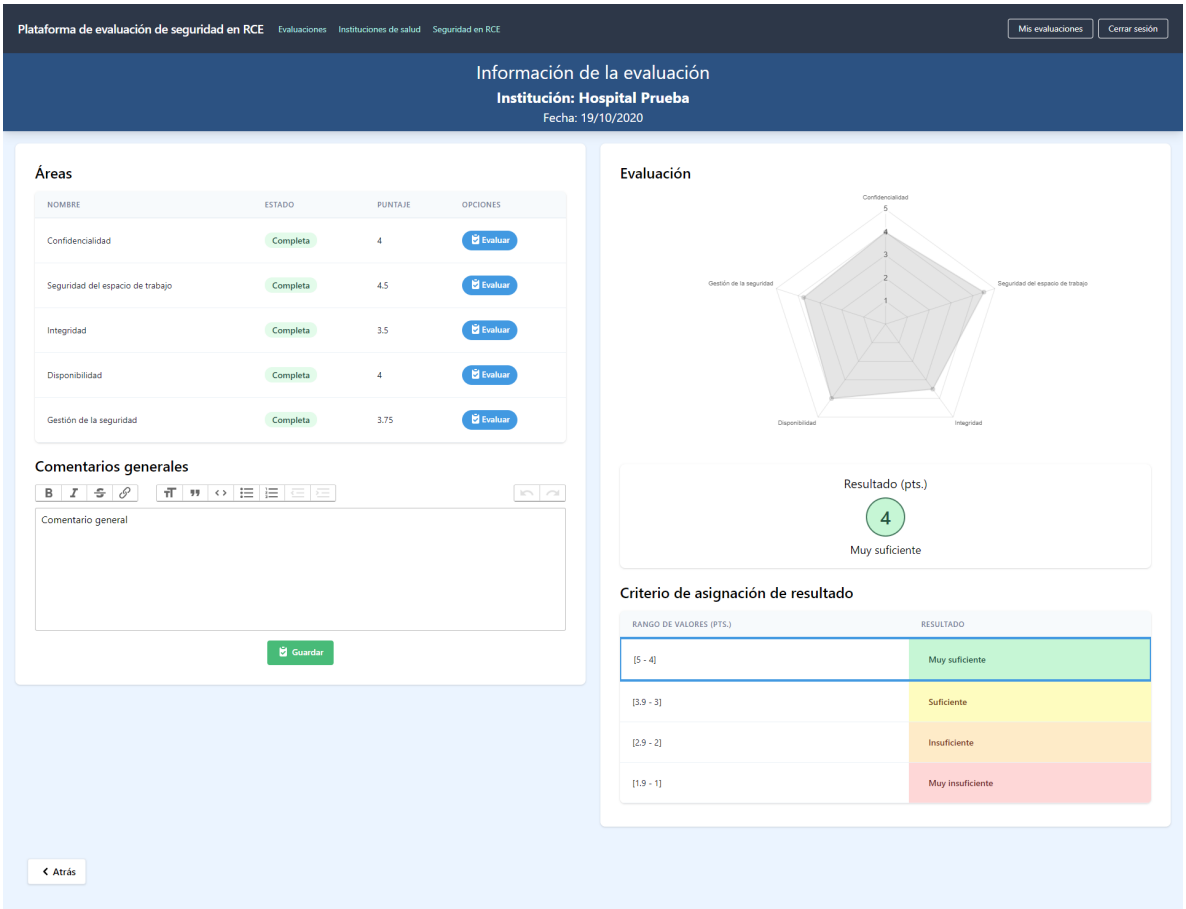


Figura 13: Vista de estado general de evaluación. Además se muestra el campo de texto para ingresar el feedback general.

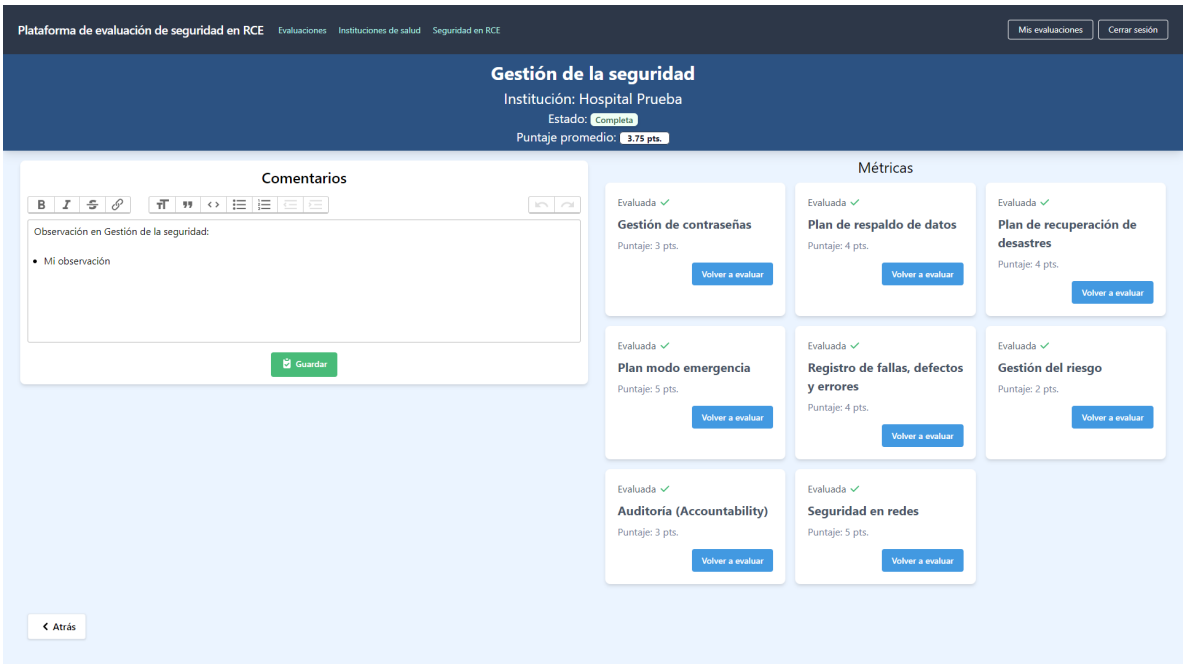


Figura 14: Vista de detalle de área, con campo de texto para ingresar el feedback específico.

Se puede apreciar además, la distribución en tarjetas que poseen las métricas, lo que provoca que el proceso de evaluación sea mas intuitivo.

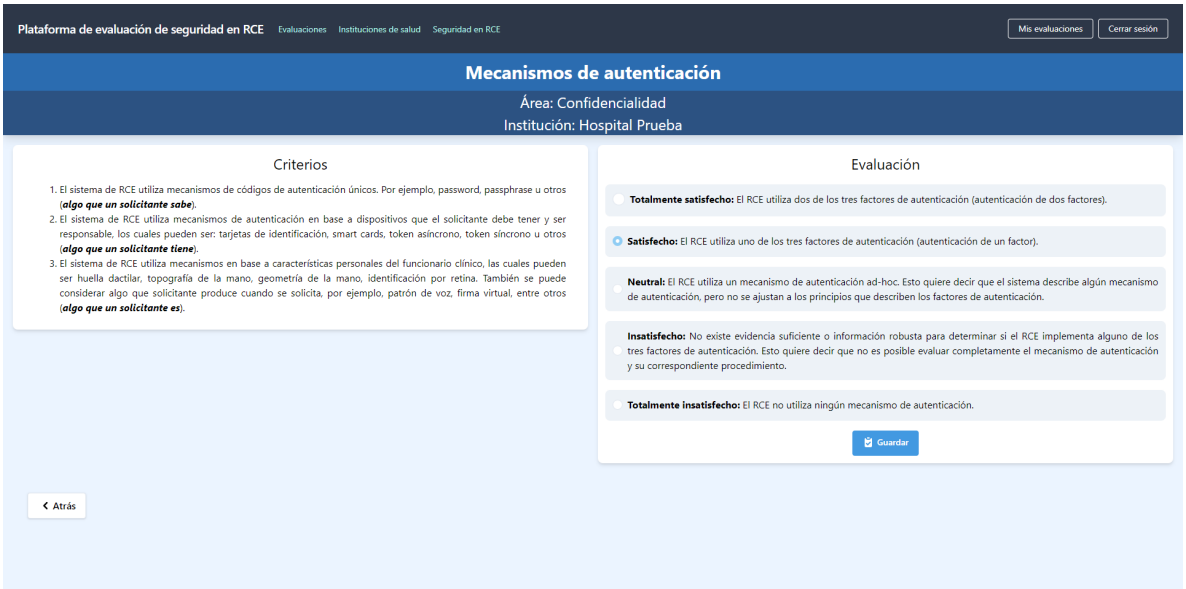


Figura 15: Vista de evaluación de métrica con opciones relacionadas a la escala de Likert y sus respectivos criterios de evaluación.

### 5.1.2. SEGUNDO SPRINT

En este Sprint se presentan funcionalidades relacionadas a la gestión de la plataforma y documento de acreditación de la evaluación.

- Gestión de la plataforma (1/2): HdU-3, HdU-4, HdU-5, HdU-11, hdu-12.

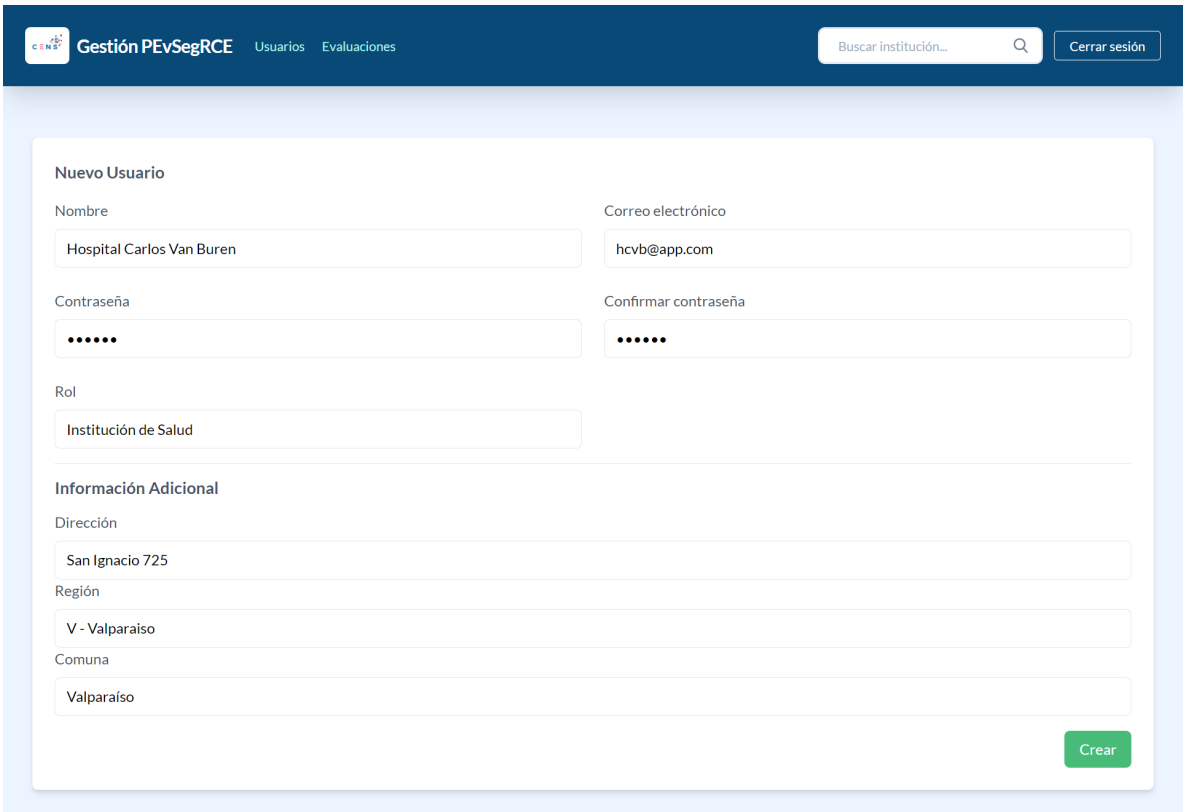


Figura 16: Vista de formulario de creación/edición de usuarios.

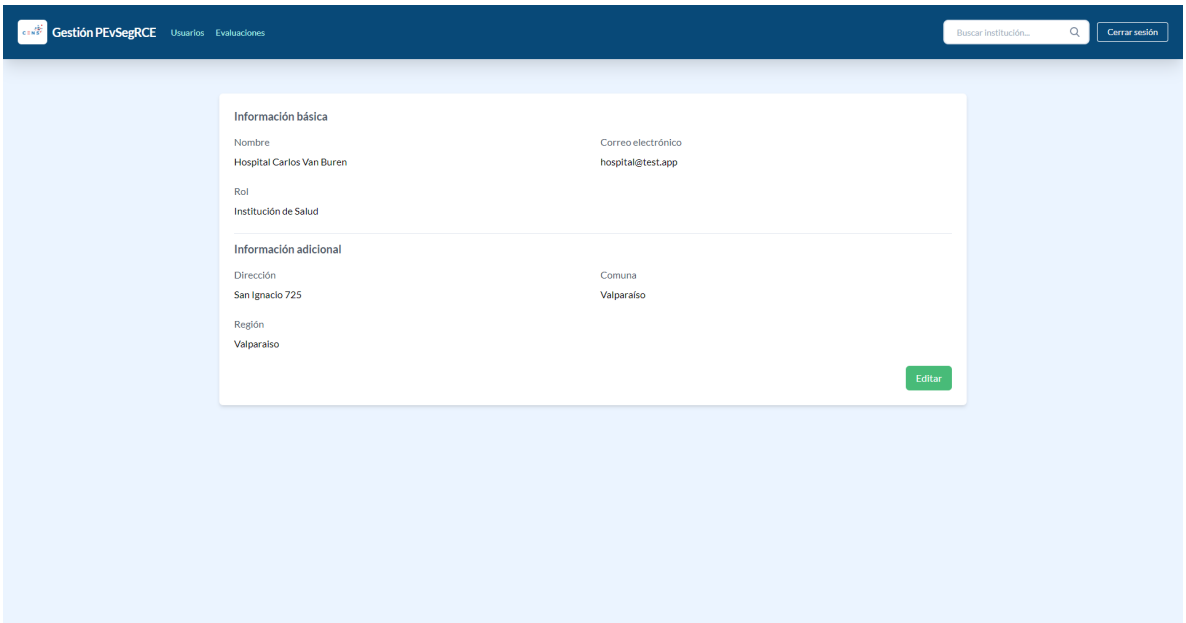


Figura 17: Vista de perfil de Usuario (Institución de Salud).

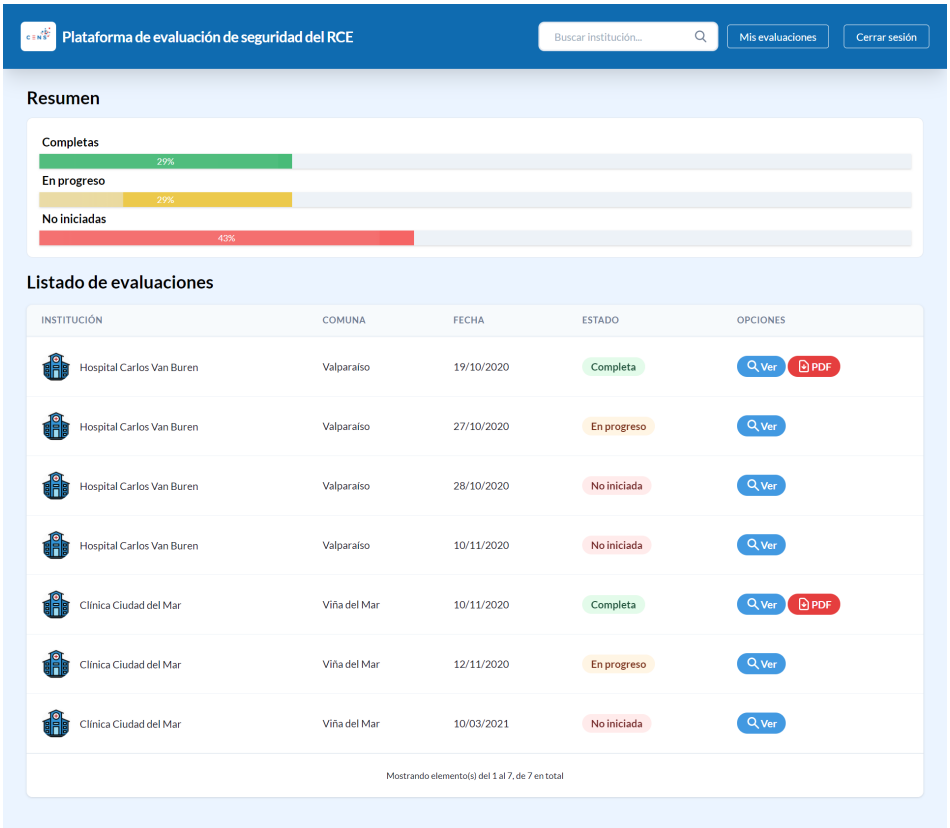


Figura 18: Vista de listado de las evaluaciones asignadas (según perfil) con resumen general relacionado al estado de estas.

- Documento de acreditación de la evaluación: HdU-2

# Evaluación de Registro Clínico Electrónico

- Nombre de institución: Hospital Prueba
- Comuna: Valparaíso
- Fecha de evaluación: 2020-10-19
- Evaluador: Evaluador Prueba

## Detalle de evaluación

| Área | Confidencialidad | | | | |
|---|---|---|---|---|---|
| **Métrica** | **Totalmente satisfecho** | **Satisfecho** | **Neutral** | **Insatisfecho** | **Totalmente insatisfecho** |
| Mecanismos de autenticación | | X | | | |
| Mecanismos de autorización | | X | | | |
| Mecanismos de identificación | X | | | | |
| Criptografía | | | X | | |
| **Puntaje** | **4 pts.** | | | | |

Comentarios:

Observación en Confidencialidad:

- Mi observación

| Área | Seguridad del espacio de trabajo | | | | |
|---|---|---|---|---|---|
| **Métrica** | **Totalmente satisfecho** | **Satisfecho** | **Neutral** | **Insatisfecho** | **Totalmente insatisfecho** |
| Seguridad del RCE en el lugar de trabajo | | X | | | |
| Control de dispositivos | X | | | | |

Figura 19: Vista del principio del documento donde se exporta toda la información de la evaluación en formato PDF.

| Área | Gestión de la seguridad | | | | |
|---|---|---|---|---|---|
| **Métrica** | **Totalmente satisfecho** | **Satisfecho** | **Neutral** | **Insatisfecho** | **Totalmente insatisfecho** |
| Gestión de contraseñas | | | X | | |
| Plan de respaldo de datos | | X | | | |
| Plan de recuperación de desastres | | X | | | |
| Plan modo emergencia | X | | | | |
| Registro de fallas, defectos y errores | | X | | | |
| Gestión del riesgo | | | | X | |
| Auditoría (Accountability) | | | X | | |
| Seguridad en redes | X | | | | |
| **Puntaje** | **3.75 pts.** | | | | |

Comentarios:

Observación en Gestión de la seguridad:

- Mi observación

**Evaluación final**

| | |
|---|---|
| **Puntaje** | **4 pts.** |
| **Resultado** | **Muy suficiente** |

Comentarios generales:

Comentario general

Figura 20: Vista de última página del documento donde se puede ver el resultado final de la evaluación.

### 5.1.3. TERCER SPRINT

En este Sprint se presentan funcionalidades relacionadas a la gestión de la plataforma, la incorporación de la opción "No Aplica.ª la evaluación de métricas y el buscador de Instituciones de Salud.

- Gestión de la plataforma (2/2): HdU-6, HdU-7, HdU-8, HdU-9, HdU-10.

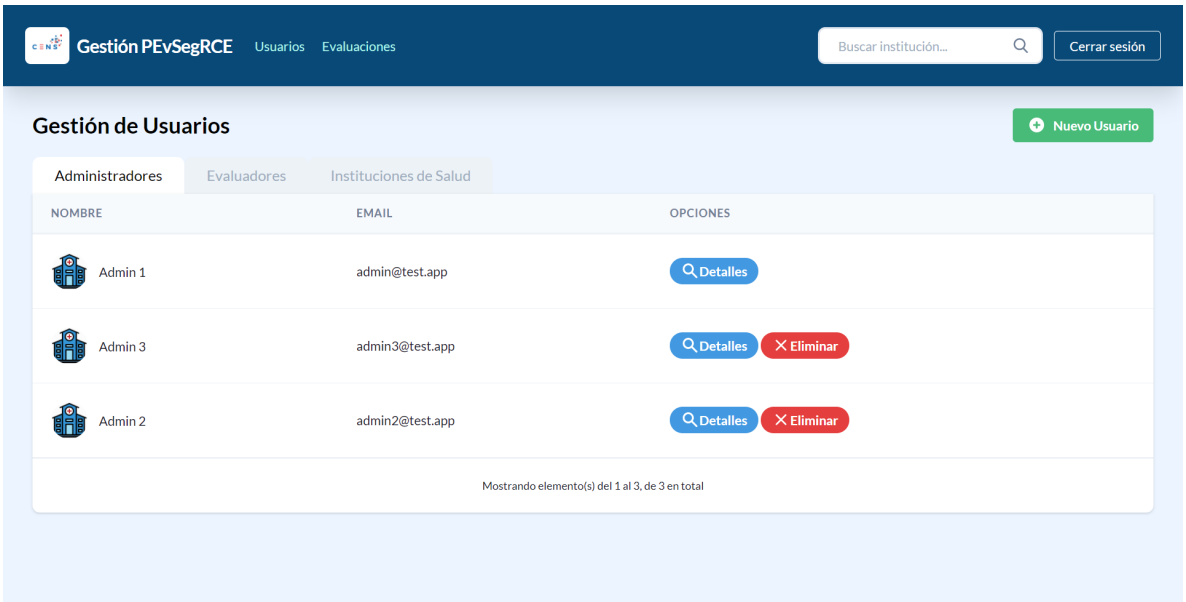


Figura 21: Vista de tabla de Usuarios con pestañas asociadas a cada Rol, la opción de ver el perfil de cada Usuario y la opción de "eliminarlo".

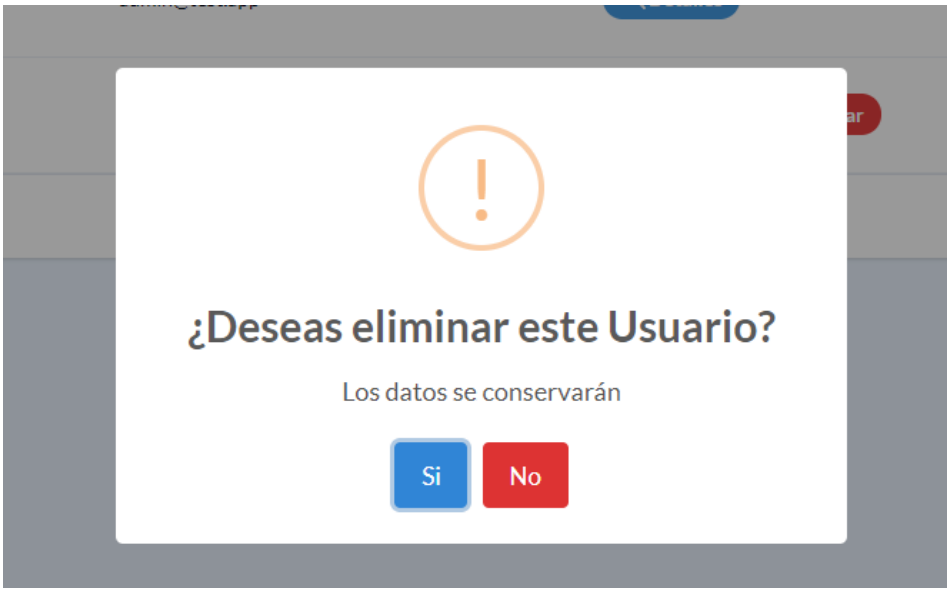


Figura 22: Vista de modal de confirmación para "eliminar" Usuario.

Cabe destacar que este modal fue implementado mediante un componente de Vue.js.

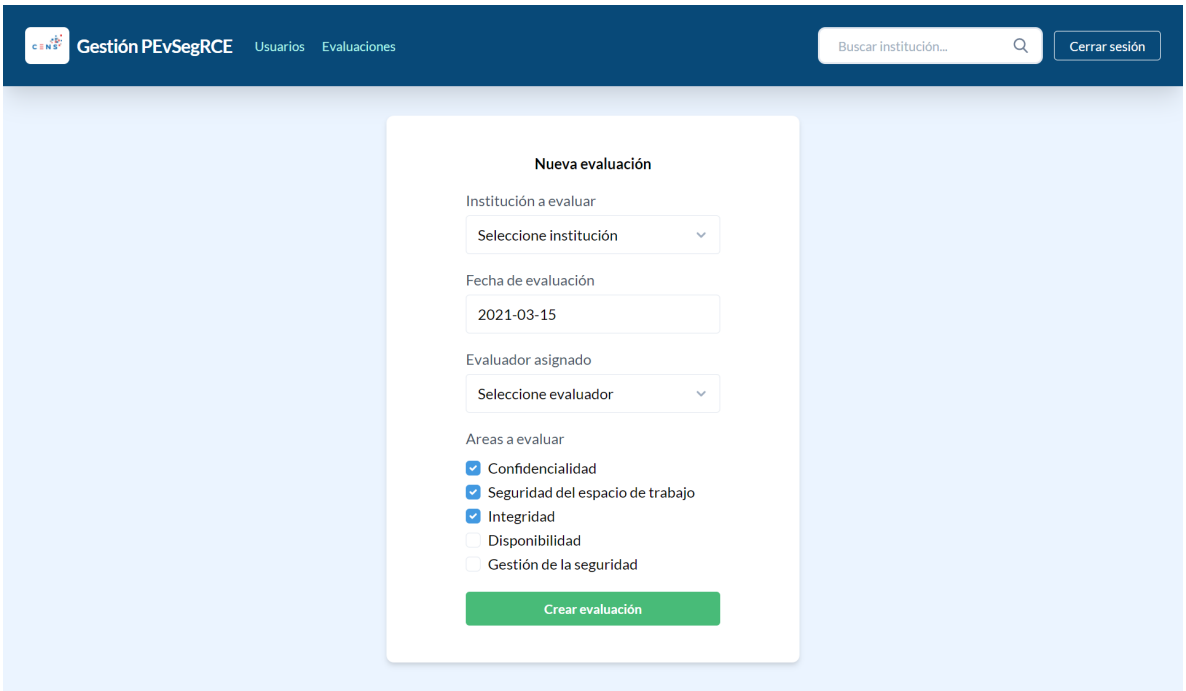


Figura 23: Vista de formulario para creación de evaluación, donde se debe seleccionar Evaluador, fecha, Institución de Salud y áreas a evaluar. Cabe destacar que es posible seleccionar entre 2 y 5 áreas.

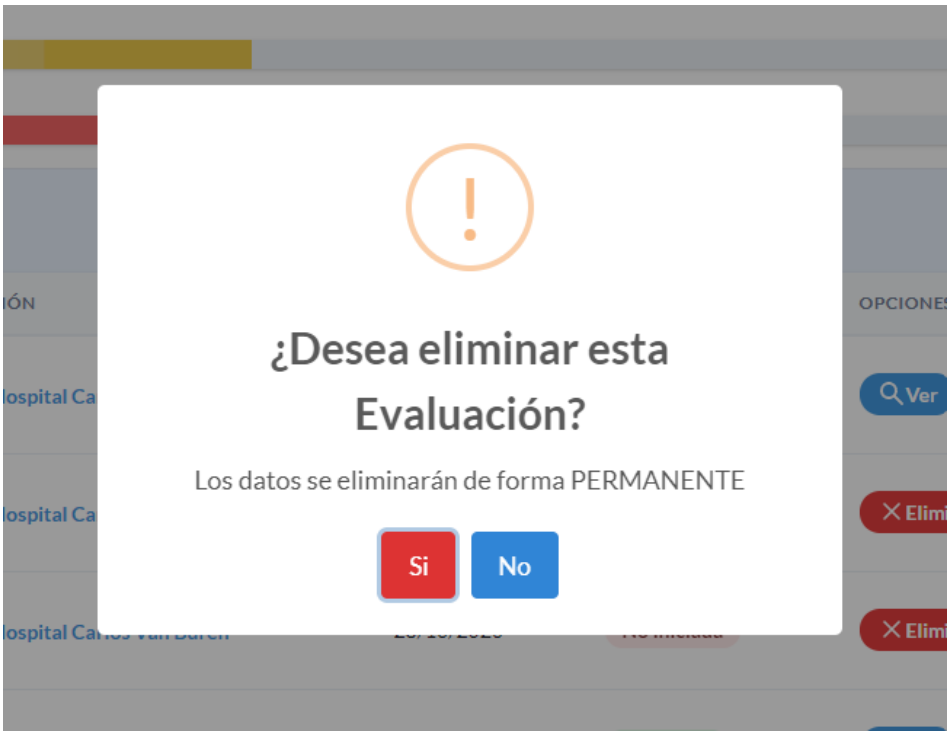


Figura 24: Vista de modal de confirmación para eliminar evaluación, aparece luego de pulsar el botón “Eliminar” que aparece en la fig. 18

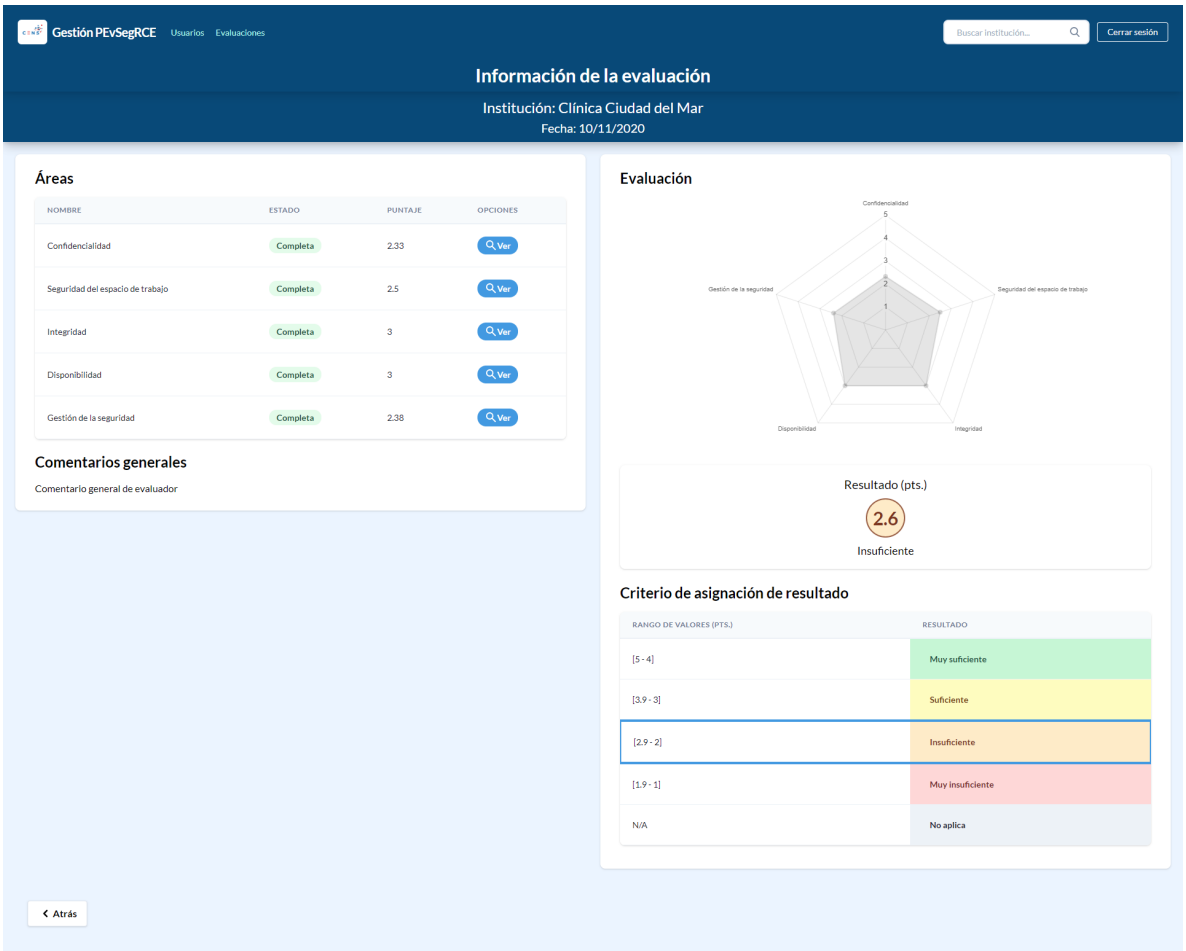


Figura 25: Vista de detalle de evaluación cuando está completa.

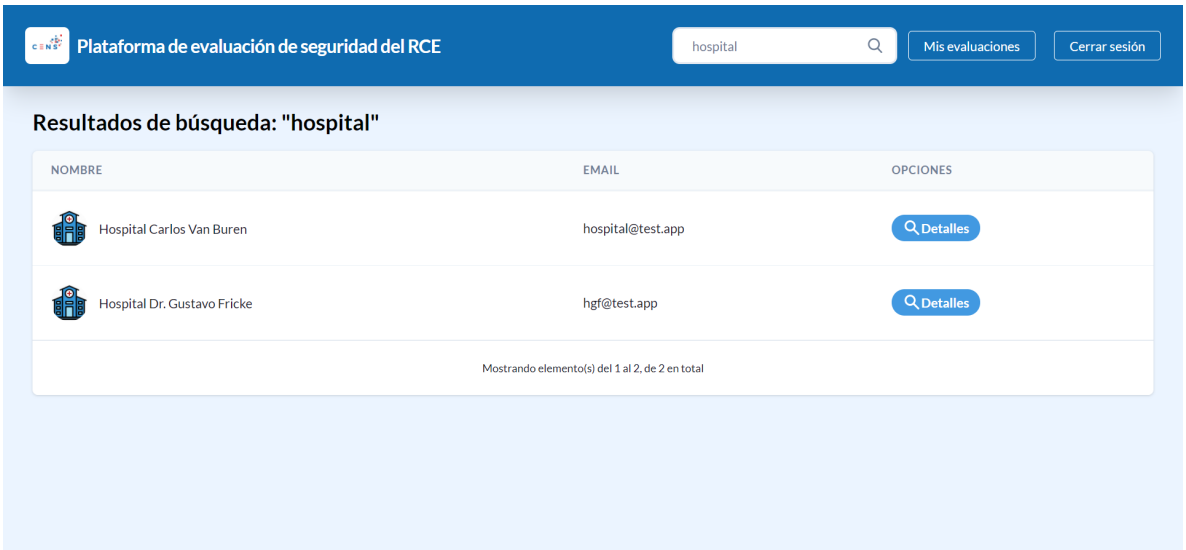


Figura 26: Vista de resultado de búsqueda de Institución de Salud, luego de pulsar el botón de búsqueda en la barra de navegación.

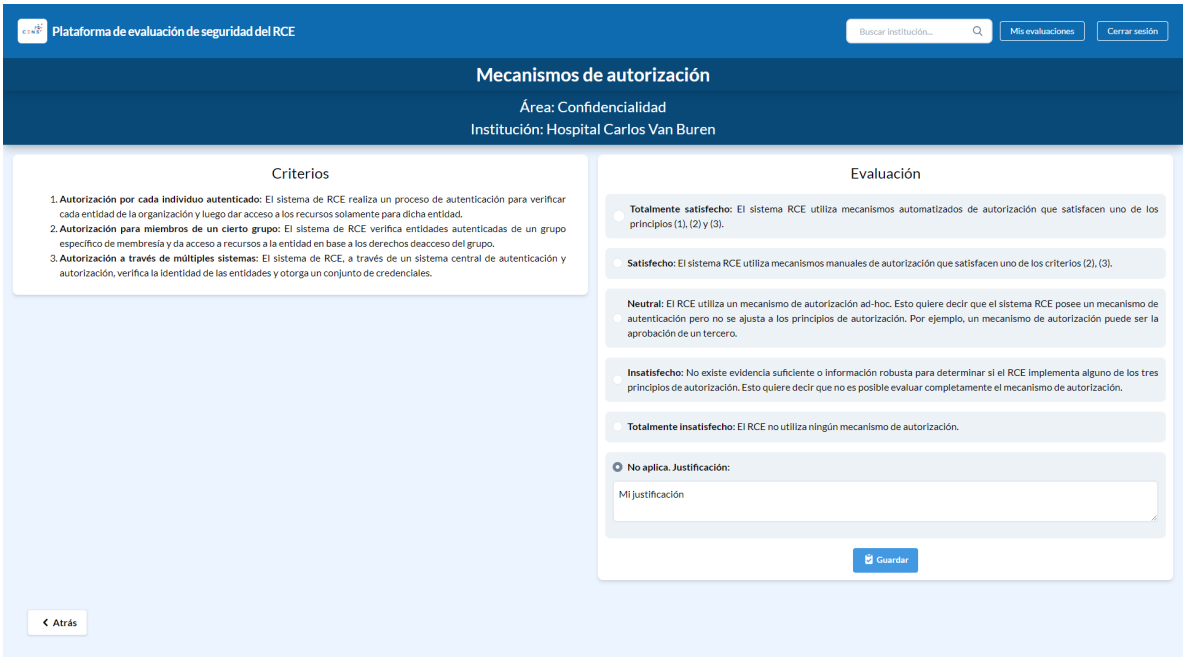


Figura 27: Vista opciones de evaluación de métrica, con opción “No Aplica” incluida y su respectivo campo de texto para ingresar la justificación en caso de seleccionarla.

# CAPÍTULO 6
# CONCLUSIONES

En el trabajo realizado en este documento, fue posible comprobar que la seguridad de los RCEs es algo crítico, debido a la sensibilidad de los datos que manejan estos sistemas y lo que podría provocar una hipotética falla de seguridad. En este caso se debe prevenir este tipo de situaciones mediante herramientas que puedan diagnosticar este tipo de incidencias antes de que ocurran. Por eso, es tan importante que existan plataformas como la desarrollada en este documento y más aun si fue implementada a partir de un instrumento de calidad que fue diseñado a partir de una exhaustiva investigación.

Respecto a los objetivos planteados, estos fueron parcialmente cumplidos, ya que no se logró realizar el despliegue de la plataforma, debido a que este proceso se encuentra en gestiones por parte del CENS en estos momentos. Por otro lado, tampoco se pudo realizar el caso de prueba al RCE de alguna Institución de Salud, dada la situación de emergencia sanitaria en la que se encuentra el país. Sin embargo, se espera desplegar la plataforma para poder realizar las primeras evaluaciones en el corto plazo.

Como trabajo a futuro, se propone desarrollar la gestión del modelo de evaluación y realizar una gran cantidad de evaluaciones a distintos RCEs, de forma que se almacene un gran volumen de datos para así, generar valor mediante un análisis exploratorio de datos que, por ejemplo, podría entregar tendencias o patrones repetitivos entre distintos RCEs. También sería interesante expandir el instrumento de calidad a otras áreas relacionadas con la calidad del software, lo que podría generar a futuro una gran plataforma de evaluación de calidad de software, orientado tanto al RCE, como a otras plataformas utilizadas en el área de la salud.

Desarrollar esta plataforma fue una gran experiencia, ya que pude aprender muchos conceptos relacionados con la seguridad de los datos y de los RCE. Además fue una instancia para aplicar gran cantidad de los conocimientos que adquirí a lo largo de la carrera. A pesar de que no se cumplieron algunos objetivos, me siento conforme con el resultado, ya que la plataforma podrá ser utilizada a futuro o podría ser el puntapié inicial para una herramienta que será un tremendo aporta a la Salud digital en Chile.

# ANEXOS

## 6.1. ANEXO A: REQUISITOS FUNCIONALES

| ID | Nombre | Roles asociados | Descripción |
|---|---|---|---|
| **RF1** | Acceso al sistema | Usuario | El usuario debe ingresar al sistema utilizando sus credenciales (email y contraseña). |
| **RF2** | Gestión de Usuarios | Administrador | El administrador puede crear, leer, actualizar y eliminar usuarios. No puede eliminar su misma cuenta. |
| **RF3** | Gestión de evaluaciones | Administrador | El administrador puede crear y eliminar evaluaciones. |
| **RF4** | Búsqueda de Instituciones de Salud | Administrador, Evaluador | Los Administradores y Evaluadores pueden encontrar Instituciones de Salud mediante un buscador. |
| **RF5** | Creación de evaluación | Administrador | Al momento de crear una evaluación, se debe seleccionar el Evaluador asignado, Institución a evaluar. fecha de evaluación y áreas a evaluar del modelo actual. |
| **RF6** | Creación de Usuarios | Administrador | Al momento de crear un Usuario, se debe proveer un nombre, email, contraseña temporal y rol correspondiente. Para el caso de la creación de una Institución de salud, se debe proveer además dirección. región y comuna. |
| **RF6** | Visualización de Usuarios | Administrador, Evaluador | Al momento de visualizar la información de un Usuario, solo se pueden ver los atributos nombre, email y rol. Para el caso de una Institución de salud, se puede ver también la dirección, región y comuna. |
| **RF7** | Edición de Usuarios | Administrador | Al momento de actualizar la información de un Usuario, solo se pueden editar los atributos nombre, email y rol. Para el caso de una Institución de salud, se puede editar también la dirección, región y comuna. |

| | | | |
|---|---|---|---|
| **RF8** | Eliminación (desactivación) de Usuarios | Administrador | Al momento de .eliminar"(desactivar) un Usuario, se debe mostrar un mensaje o ventana de confirmación. Además los datos asociados al usuario eliminado en el sistema se deben conservar. |
| **RF9** | Restablecer contraseña | Usuario | Los usuarios pueden restablecer su contraseña en caso que deseen cambiarla ya sea por tener una contraseña temporal o por olvido de esta. Este proceso se debe validar vía email. |
| **RF10** | Estado de evaluaciones | Usuario | Las evaluaciones tienen 3 estados asociados, estos son: no iniciada, en progreso y completada. Estos estados pueden ser visualizados por todos los Usuarios según las evaluaciones que les correspondan. |
| **RF11** | Visualización de Evaluaciones | Administrador, Inst. de Salud | Al momento de visualizar la información de una evaluación, se debe mostrar el estado, el resultado, las observaciones y el detalle de los puntajes de cada área y métrica correspondiente. Además, el Administrador o Inst. de Salud solo puede visualizar la información de las evaluaciones completadas. |
| **RF12** | Eliminación de Evaluaciones | Administrador | Al momento de eliminar una evaluación, se debe mostrar un mensaje o ventana de confirmación. Además los datos asociados a la evaluación también se deben eliminar. |
| **RF13** | Visualización de Evaluaciones asignadas | Evaluador | Al momento de visualizar la información de una evaluación asignada, se debe mostrar el estado, el resultado, las observaciones y el detalle de los puntajes de cada área y métrica correspondiente. |
| **RF14** | Aplicación de Evaluación | Evaluador | El Evaluador podrá acceder a todas sus evaluaciones asignadas y evaluar por área cada métrica asociada. Cada métrica debe desplegar sus 5 alternativas asociadas a un valor en la escala de likert y solo se podrá escoger 1. |

| | | | |
|---|---|---|---|
| **RF15** | Alternativa ”No Aplica” | Evaluador | Para cada métrica, se debe mostrar una opción ”No aplica”junto a las opciones de la escala de likert, la cual será seleccionada en casos particulares y no aportará al puntaje total por área. |
| **RF16** | Puntaje por área de la evaluación | Evaluador | En el detalle de la evaluación se debe mostrar un puntaje por área, que corresponde al promedio de los puntajes de las métricas asociadas. |
| **RF17** | Puntaje final de la evaluación | Evaluador | Al momento de finalizar la evaluación de todas las áreas, se debe mostrar un puntaje final que corresponde al promedio de los puntajes de las áreas que apliquen |
| **RF18** | Resultado de la evaluación | Evaluador | Se debe mostrar un resultado asociado al puntaje final de la evaluación, el cual está basado en un criterio de asignación. |
| **RF19** | Exportar evaluación | Usuarios | Cuando una evaluación esté completada, se debe poder exportar a través de un PDF. |
| **RF20** | Estado de evaluaciones | Administrador, Evaluador | Se debe mostrar el estado general de las evaluaciones disponibles según el rol del Usuario. Esto a través de un gráfico que refleje el resumen de lo mencionado. |

## 6.2. ANEXO B: REQUISITOS NO FUNCIONALES

| ID | Nombre | Descripción |
|---|---|---|
| **RNF1** | Despliegue | El sistema debe estar desplegado únicamente en los servidores del CENS. |
| **RNF2** | Interfaz | El sistema debe tener una interfaz clara, intuitiva y moderna. Se debe priorizar el flujo de la aplicación de la evaluación. |

# REFERENCIAS BIBLIOGRÁFICAS

[Aldosari, 2017] Aldosari, B. (2017). Patients' safety in the era of emr/ehr automation. *Informatics in Medicine Unlocked*, 9:230 – 233.

[Cattell, 2010] Cattell, R. (2010). Scalable sql and nosql data stores. *SIGMOD Record*, 39:12–27.

[Daglish y Archer, 2009] Daglish, D. y Archer, N. (2009). Electronic personal health record systems: A brief review of privacy, security, and architectural issues. pp. 110 – 120.

[E-HealthReporter, 2018] E-HealthReporter (2018). Soledad muñoz: "la estrategia digital en salud es un camino a largo plazo que trasciende a los gobiernos; es una visión de estado". `https://ehealthreporter.com/es/noticia/soledad-munoz-la-estrategia-digital-en-salud-es-un-camino-a-largo-plazo-que-trasciende-a-los-gobiernos-es-una-vision-de-estado/`.

[Edinger *et al.*, 2012] Edinger, T., Cohen, A. M., Bedrick, S., Ambert, K. H., y Hersh, W. R. (2012). Barriers to retrieving patient information from electronic health record data: Failure analysis from the trec medical records track. *AMIA ... Annual Symposium proceedings. AMIA Symposium*, 2012:180–8.

[Fowler *et al.*, 2002] Fowler, M., Rice, D., Foemmel, M., Hieatt, E., Mee, R., y Stafford, R. (2002). *Patterns of Enterprise Application Architecture*. Addison-Wesley Professional.

[Griffith, 2019] Griffith, R. (2019). Electronic records, confidentiality and data security: The nurse's responsibility. *British journal of nursing (Mark Allen Publishing)*, 28:313–314.

[Holvitie *et al.*, 2018] Holvitie, J., Licorish, S. A., Spínola, R. O., Hyrynsalmi, S., MacDonell, S. G., Mendes, T. S., Buchan, J., y Leppänen, V. (2018). Technical debt and agile software development practices and processes: An industry practitioner survey. *Information and Software Technology*, 96:141–160.

[Hulstijn *et al.*, 2011] Hulstijn, J., van der Jagt, J., y Heijboer, P. (2011). Integrity of electronic patient records. En Janssen, M., Scholl, H. J., Wimmer, M. A., y Tan, Y.-h., editores, *Electronic Government*, pp. 378–391, Berlin, Heidelberg. Springer Berlin Heidelberg.

[Ka-Ping Yee, 2004] Ka-Ping Yee (2004). Aligning security and usability. *IEEE Security Privacy*, 2(5):48–55.

[Kahn y Sheshadri, 2008] Kahn, S. y Sheshadri, V. (2008). Medical record privacy and security in a digital environment. *IT Professional*, 10(2):46–52.

[Kristianson *et al.*, 2009] Kristianson, K. J., Ljunggren, H., y Gustafsson, L. L. (2009). Data extraction from a semi-structured electronic medical record system for outpatients: A model to facilitate the access and use of data for quality control and research. *Health Informatics Journal*, 15(4):305–319. PMID: 20007655.

[Li *et al.*, 2015] Li, Y.-C., Yen, J.-C., Chiu, W.-T., Jian, W.-S., Shabbir, S. A., y Hsu, M.-H. (2015). Building a national electronic medical record exchange system–experiences in taiwan. *Computer methods and programs in biomedicine*, 121.

[Mcmullen *et al.*, 2014] Mcmullen, P., Howie, W., Philipsen, N., Bryant, V., Setlow, P., Calhoun, M., y Green, Z. (2014). Electronic medical records and electronic health records: Overview for nurse practitioners. *The Journal for Nurse Practitioners*, 10:660–665.

[Márquez *et al.*, 2020] Márquez, G., Taramasco, C., y Astudillo, H. (2020). Defining security metrics to evaluate electronic health records systems: A case study in chile. *2nd International Workshop on Software Engineering for Healthcare (SEH)*.

[Papoutsi *et al.*, 2015] Papoutsi, C., Reed, J., Marston, C., Lewis, R., Majeed, A., y Bell, D. (2015). Patient and public views about the security and privacy of electronic health records (ehrs) in the uk: Results from a mixed methods study healthcare information systems. *BMC Medical Informatics and Decision Making*, 15.

[Renardi *et al.*, 2018] Renardi, M., Kuspriyanto, Cholis, N., y Rakhman, E. (2018). Securing electronic medical record in near field communication using advanced encryption standard (aes). *Technology and Health Care*, 26:1–6.

[Shaw *et al.*, 2014] Shaw, C., Groene, O., Botje, D., Sunol, R., Kutryba, B., Klazinga, N., Bruneau, C., Hammer, A., Wang, A., Arah, O., y Wagner, C. (2014). The effect of certification and accreditation on quality management in 4 clinical services in 73 european hospitals. *International Journal for Quality in Health Care*, 26(Suppl 1):100–107.

[Tsai *et al.*, 2019] Tsai, M.-F., Hung, S.-Y., Yu, W.-J., Chen, C., y Yen, D. (2019). Understanding physicians' adoption of electronic medical records: Healthcare technology self-efficacy, service level and risk perspectives. *Computer Standards & Interfaces*, 66.

[Wang *et al.*, 2019] Wang, Q., Zhu, G., Wang, C., y Cheng, H. (2019). Research on privacy-preserving methods of electronic medical records. *Journal of Physics: Conference Series*, 1176:022029.

[Wielemaker, 2021] Wielemaker, J. (2021). Logic programming for knowledge-intensive interactive applications.

[Williams y Boren, 2008] Williams, F. y Boren, S. A. (2008). The role of electronic medical record in care delivery in developing countries. *International Journal of Information Management*, 28(6):503 – 507.

[Yang *et al.*, 2006] Yang, C.-M., Lin, H.-C., Chang, P., y Jian, W.-S. (2006). Taiwan's perspective on electronic medical records' security and privacy protection: Lessons learned from hipaa. *Computer Methods and Programs in Biomedicine*, 82(3):277 – 282.

[Yeo *et al.*, 2012] Yeo, K., Lee, K., Kim, J.-M., Kim, T.-H., Choi, Y.-H., Jeong, W.-J., Hwang, H., Baek, R.-M., y Yoo, S. (2012). Pitfalls and security measures for the mobile emr system in medical facilities. *Healthcare informatics research*, 18:125–35.

[Yu *et al.*, 2010] Yu, Y.-C., Huang, T.-Y., y Wei, H. (2010). Forward secure digital signature for electronic medical records. *Journal of medical systems*, 36:399–406.