DIVISION DE ESTUDIOS DE POSGRADO E INVESTIGACION

SISTEMA PARA LA VALIDACIÓN DE PERFILES DE CONOCIMIENTOS EN EL AREA DE LA SEGURIDAD DE LA INFORMACIÓN

T E S I S

PRESENTADA COMO REQUISITO PARCIAL

PARA OBTENER EL GRADO DE:

MAESTRO EN CIENCIAS DE LA COMPUTACIÓN

JALIL GERARDO ESPINOZA ZEPEDA

DIRECTOR DE TESIS

DR. OSCAR MARIO RODRIGUEZ ELIAS

HERMOSILLO, SONORA, MÉXICO **JUNIO DEL 2021**

SECCIÓN: DIV. EST. POS. E INV.
No. OFICIO: DEPI/159/21
ASUNTO: AUTORIZACIÓN DE IMPRESIÓN DE TESIS.

07 de julio de 2021

C. JALIL GERARDO ESPINOZA ZEPEDA
P R E S E N T E.

Por este conducto, y en virtud de haber concluido la revisión del trabajo de tesis que lleva por nombre **"Sistema para la validación de perfiles de conocimientos en el área de la seguridad de la información"**; que presenta para el examen de grado de la MAESTRÍA EN CIENCIAS DE LA COMPUTACIÓN, y habiéndola encontrado satisfactoria, nos permitimos comunicarle que se autoriza la impresión del mismo a efecto de que proceda el trámite de obtención de grado.

Deseándole éxito en su vida profesional, quedo de usted.

A T E N T A M E N T E

DR. OSCAR MARIO RODRÍGUEZ ELIAS
DIRECTOR

M.C. SONIA REGINA MENESES MENDOZA
SECRETARIO

S.E.P.
INSTITUTO TECNOLÓGICO DE HERMOSILLO
DIVISIÓN DE ESTUDIOS DE POSGRADO

M.C. FRANCISCO GABRIEL IBARRA LEMAS
VOCAL

M.C.O. ROSA IRENE SÁNCHEZ FERMÍN
JEFA DE LA DIVISIÓN DE ESTUDIOS DE POSGRADO E INVESTIGACIÓN

RISF/eme*

CARTA CESIÓN DE DERECHOS

En la ciudad de Hermosillo Sonora a el día 20 de agosto del año 2021 el que suscribe **C. JALIL GERARDO ESPINOZA ZEPEDA**, alumno de la maestría en **CIENCIAS DE LA COMPUTACIÓN** adscrito a la División de Estudios de Posgrado e Investigación, manifiesta que es autor intelectual del presente trabajo de **TESIS TITULADO SISTEMA PARA LA VALIDACIÓN DE PERFILES DE CONOCIMIENTOS EN EL ÁREA DE LA SEGURIDAD DE LA INFORMACIÓN** bajo la dirección del **DR. OSCAR MARIO RODRIGUEZ ELIAS** y ceden los derechos del mismo al Tecnologico Nacional de México/Instituto Tecnologico de Hermosillo, para su difusión, con fines académicos y de investigación.

Los usuarios de la información no deben de reproducir el contenido textual, graficas, tablas o datos contenidos sin el permiso expreso del autor y del director del trabajo. Este puede ser obtenido a la dirección de correo electrónico siguiente: jgez_17@gmail.com y omrodriguez@hermosillo.tecnm.mx. Una vez otorgado el permiso se deberá expresar el agradecimiento correspondiente y citar la fuente del mismo.

A T E N T A M E N T E

Jalil Gerardo E. Z.

Jalil Gerardo Espinoza Zepeda

Agradecimientos

Agradezco el apoyo del CONACYT por la beca que se me otorgó con número 744901. También agradezco a mi director de tesis Oscar Mario Rodríguez Elías quien me guio durante toda la realización de la tesis y a mis revisores Sonia Regina Meneses Mendoza, Francisco Gabriel Ibarra Lemas por su gran apoyo. Así mismo, agradezco todo el apoyo otorgado por la empresa Código Verde, y en particular a su director general, ingeniero David Taboada, por proporcionar los datos para la elaboración de esta tesis, así como para la realización del proyecto que aquí se describe.

Resumen

Actualmente, determinar los conocimientos que posee un individuo, conlleva grandes desafíos, no solo para la comunidad educativa, sino también en las organizaciones que necesitan tener personal capacitado que se ocupe de mantener segura la información, al igual que los equipos tecnológicos que pueden ser alterados con una intención dañina. La presente investigación tubo el objetivo de diseñar un sistema que identifique los conocimiento y habilidades necesarias en las que debe capacitarse una persona, basado en el perfil del puesto de trabajo que desempeña un individuo e interés a futuro del mismo, de tal manera que se pueda concluir cursos de capacitación adecuadas en el área de la ciberseguridad. Posterior al diseño se continuó con el desarrollo del sistema. Este sistema debe reportar una ruta de aprendizaje a seguir considerando las diferentes certificaciones que se ofrecen en las áreas de la ciberseguridad. Para el desarrollo de la solución se utiliza el concepto de perfil de conocimiento, así como las técnicas de mapeo de perfiles de conocimiento. Estas técnicas permiten comparar el perfil de conocimiento de un individuo contra el definido para un puesto de trabajo, identificando qué aspectos del perfil del puesto se cumplen, y cuáles no, de esta forma se busca identificar las áreas de conocimiento y habilidades en las que debe ser capacitada una persona. El sistema diseñado utiliza como material de apoyo el marco de referencia NICE el cual define áreas de especialidad, puestos de trabajo, además de los conocimientos y habilidades en ciberseguridad que debe poseer un individuo.

Palabras claves: Seguridad Informática, Ciberseguridad, Capacitación, Riesgos de Seguridad, Perfil de Conocimiento, Roles de Trabajo.

Abstract

Currently, determining the knowledge that an individual possesses, entails great challenges, not only for the educational community, but also in organizations that need to have trained personnel who are in charge of keeping information secure, as well as technological equipment that can be altered with harmful intent. The present research has the objective of designing a system that identifies the necessary knowledge and skills that a person must be trained on, based on the profile of the job that an individual performs and future interest in it, in such a way that he/she can complete appropriate training courses in the area of cybersecurity. After the design, the creation of the system was done. This system must inform a learning path to continue considering the different certifications offered in the areas of cybersecurity. For the development of the solution, the concept of knowledge profile is used, as well as knowledge profile mapping techniques. These techniques allow comparing the knowledge profile of an individual against that defined for a job, identifying which aspects of the job profile are met or not, in this way it seeks to identify the areas of knowledge and skills in which a person should be trained on. The system designed uses, as support material, the NICE frame of reference which defines areas of specialty, jobs, as well as the knowledge and skills in cybersecurity that an individual must possess.

Keywords: Computer Security, Cybersecurity, Training, Security Risks, Knowledge Profile, Work Roles.

Contenido

Índice de Ilustraciones

Índice de Diagramas

Índice de Tablas

1 Introducción

El conocimiento se puede entender como la facultad del ser humano para comprender, por medio de la razón, la naturaleza y cualidades de las cosas; es un concepto invaluable e intangible de información que se obtiene por medio de las experiencias propias o de otros entes y de los estudios realizados durante su vida [43]. La capacidad de la mente humana para abstraer y entender los datos es única de cada individuo, este la representa como información útil y valida dependiendo de la comprensión de cada una de las variables teóricas y prácticas de la realidad.

De lo dicho anteriormente se entiende que la obtención del conocimiento tiene limitaciones de tiempo, dedicación, experiencia, capacidad de comprensión y abstracción de los datos, que confiera valor para resolver una situación concreta, de aquí radica la importancia de estar capacitándose constantemente, ya sea para consolidar o para aprender algo nuevo.

En relación al presente proyecto, se considera el procedimiento de aprendizaje, además de la planificación correcta para la capacitación de los miembros de una organización, con el objetivo de aumentar sus conocimientos, habilidades, y actitudes, de la mejor manera posible, con lo que se espera obtener un aumento en la efectividad laboral por el uso de buenas prácticas en ciberseguridad, respetando los estándares de control de calidad nacional e internacional, garantizando la seguridad de la información para la toma de decisiones.

El enseñar y aprender el manejo de las nuevas tecnologías de la información y comunicación, debe ser parte del proceso de adaptación organizacional para cumplir con las necesidades y exigencias de la nueva industria 4.0. En este documento en especial, se hace referencia a la ciberseguridad. Tomando en cuenta que los avances acelerados en las telecomunicaciones hacen necesario conocer el funcionamiento de las mismas para hacer una buena transición e integración de los cambios, además de hacerlas seguras.

El presidente Barack Obama, expresidente 44 de los Estados Unidos, declaró que la infraestructura digital de américa es “un activo estratégico nacional” por lo que realizó estrategias para defender a su país de las diversas amenazas que conlleva el uso de tecnología, como ejemplo creó el Cybercom y nombró director al general Keith Alexander, director de la Agencia Nacional de Seguridad (NSA) con un mandato claro “conducir las operaciones de amplio espectro para defender las redes militares de Estados Unidos” [30].

La utilización ilícita de las TIC puede tener repercusiones indeseables en la infraestructura, la seguridad nacional y el desarrollo económico de cualquier país [31]. Por lo que existen organizaciones que regulan y facilitan la cooperatividad entre los organizamos gubernamentales y las organizaciones privadas, como ejemplo la unión internacional de telecomunicaciones (UIT).

Las nuevas necesidades relacionadas con la ciberseguridad, considerando el IoT y la digitalización del mundo físico [32], ponen una especial presión en el tema de la formación de recursos humanos, pues la demanda de especialistas altamente calificados en las diversas áreas de la misma se encuentra en crecimiento, y no se prevé que disminuya pronto [33].

Evaluar las habilidades y conocimientos de un individuo en el área de la ciberseguridad es un proceso especializado que lleva tiempo y planeación para ser lo más asertivos posibles. Para ello se deben considerar los intereses personales, conocimientos técnicos, estudios profesionales, experiencia laboral, capacitaciones adquiridas y las responsabilidades laborales. Cualquier profesional o técnico que se desempeña en el manejo y manipulación de información requiere constante actualización en forma periódica, porque de lo contrario llegará un momento en que se desfasará y lejos de aportar a la organización harán que esta pierda defensas ante ataques cibernéticos, además de reducir su competitividad y productividad.

Mantener una buena comunicación y reducir la necesidad de supervisión a los empleados de una empresa son otros motivos a tomar en cuenta al momento de contratar u ofrecer un mejor

puesto de trabajo. El manejo y manipulación de la información es delicado, esto hace que sea necesario un nivel de conocimiento y habilidades técnicas en varias áreas, y la ciberseguridad es una de ellas, con más relevancia en organizaciones grandes, por el gran flujo de datos que se manejan.

La evaluación de la seguridad de la información en las empresas no solo se puede determinar por los sistemas que se utilizan, sino que hay que tomar en cuenta a las personas que laboran en ellas.

En el presente documento se planteó la elaboración de un sistema que sea capaz de apoyar en la toma de decisión en la determinación de las necesidades de capacitación de un individuo en el área de la ciberseguridad, la cual facilite establecer una ruta de capacitación adecuada de acuerdo al rol de trabajo al que va dirigido. Este trabajo se ha desarrollado para la empresa código verde, respetando su misión:

"Elevar el nivel de la seguridad informática de nuestros clientes y reducir significativamente su exposición al riesgo e impacto de posibles ataques" [5].

El presente proyecto se divide en siete capítulos principales, estos son: introducción (primer capítulo), marco teórico (segundo capítulo), análisis del sistema (tercer capítulo), arquitectura del software (cuarto capítulo), desarrollo del prototipo (quinto capítulo), validación del sistema (sexto capítulo), conclusión (séptimo capítulo).

1.1 Antecedentes

En el Tecnológico de Hermosillo se ha desarrollado un modelo de definición de perfiles de conocimiento, y herramientas para el análisis de perfiles en candidatos y puestos de trabajo. Se aprovecho este trabajo previo para adaptarlo al escenario de la seguridad informática. Estos documentos son:

- Construcción de un modelo para el diseño de perfiles de conocimiento realizado por la M.S.I. María de Jesús Velázquez Mendoza [52].
- Construcción de un modelo de lógica difusa para validación de perfiles de conocimiento de personal, desarrollado por Jorge Armando Rosas Daniel [23].

Los conocimientos y los procesos proporcionados en los documentos mencionados anteriormente, se utilizaron en este proyecto y con opción a implementarse en la empresa código verde, como una metodología de evaluación de perfiles de conocimiento en el área de la ciberseguridad. Para dar una idea del rubro de la empresa (especializada en seguridad informática) y los perfiles de los expertos (evaluadores de conocimiento) que en ella trabajan, se explica los servicios que ofrece:

- Pruebas de Penetración.
- Programa de Desarrollo e Implementación de Aplicaciones Seguras.
- Prevención contra Ataques de Ingeniería Social.
- Mapa de Ruta de capacitación en el área de la ciberseguridad.
- Sistema de Gestión de la Seguridad Informática.
- Atención y Solución a Incidentes de Seguridad Informática.
- Protección contra Ataques a la Disponibilidad.

Además de ofrecer consultoría e impartir una gran cantidad de cursos en América Latina acreditados por los organismos certificadores internacionales líderes para entregar en español sus cursos oficiales, algunos de ellos son COMPTIA, EC-COUNCIL, ISC, por último, ISACA [5].

Los servicios de consultoría en seguridad informática se realizan de manera presencial y evaluando la situación de forma manual, esta es indagada por los consultores expertos, que además son instructores de los cursos de certificación. Los expertos analizan los datos proporcionados por los colaboradores (individuos o participantes que desean capacitarse en el área de la ciberseguridad), para definir una ruta de capacitación adecuada a su perfil. El proceso utilizado para la determinación de rutas de capacitación ha resultado efectivo en baja escala, pero no es escalable para analizar cientos de individuos.

La empresa Código Verde desarrolla sus cursos tomando en cuenta estos puntos: el proceso de selección, cursos que se imparten, criterios a tomar en cuenta para recomendación de cursos, criterios basados en la experiencia, responsabilidad actuales y visión de los colaboradores.

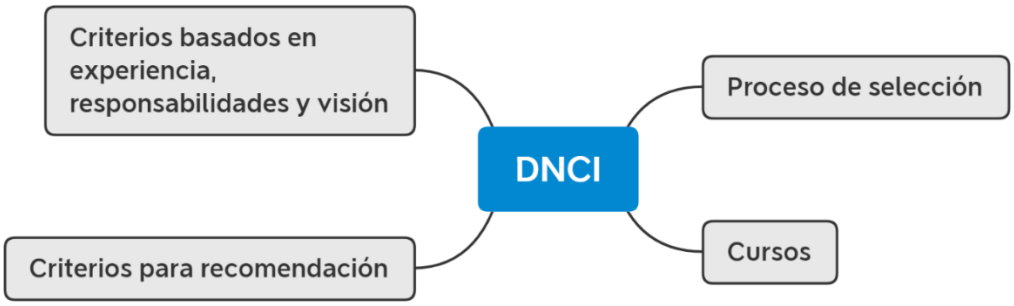

Diagrama 1. Criterios para el proceso de certificación del DNCSI (Diagnóstico de las Necesidades de Capacitación en Seguridad de la Información) [5].

En el Diagrama 1 se muestran las métricas que se siguen para el proceso de selección de rutas de capacitación en el área de la ciberseguridad. En el Diagrama 2, se muestra enumerado el proceso de selección de rutas de capacitación

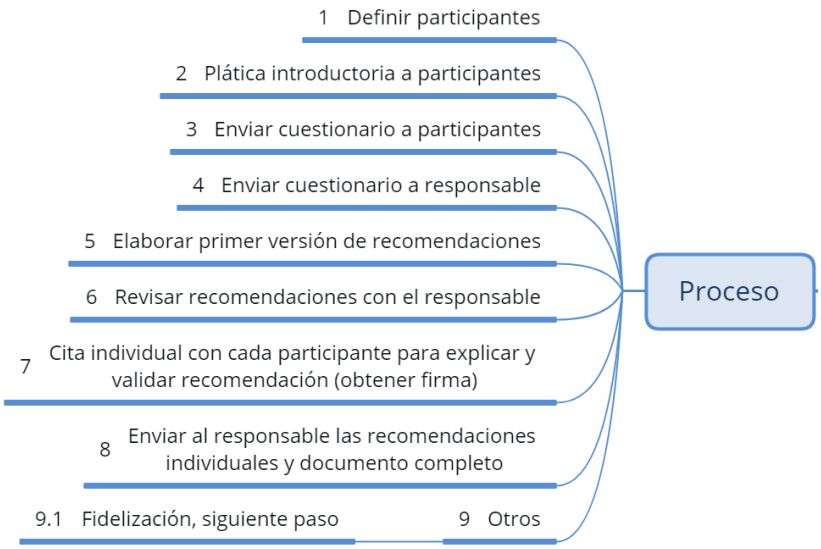

Diagrama 2. Proceso de selección de rutas de capacitación [5]. Véase pág. 44, Diagrama 7.

Los expertos especifican criterios con lo que determinan una ruta de capacitación adecuada para cada colaborador; esos criterios recomendados se muestran en el Diagrama 3.

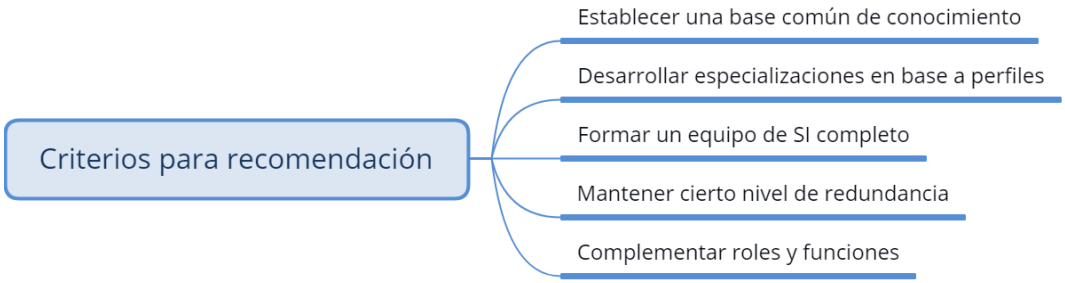

Diagrama 3. Criterios para recomendar rutas de capacitación [5].

Comenzar a mostrar el proceso de elegir una o varias rutas de certificación para cada colaborador, depende del perfil de conocimiento de cada uno, así como el rol que deberá desempeñar como especialista en ciberseguridad en su organización.

A partir de lo mencionado anteriormente, se abordó el siguiente trabajo que ayudan a identificar necesidades o rutas de capacitación para cada colaborador usando un sistema o aplicación. Primeramente, se debe introducir datos a un sistema para que un experto analice el perfil de conocimiento del colaborador en la misma aplicación, cuya retroalimentación se almacene. Continuando con la discusión sobre la posibilidad de aprovechar esa información para trabajar en el mapeo de perfiles de conocimiento realizando de manera autónoma por el sistema y que identifique necesidades de capacitación en seguridad informática, y de ahí partir en la planificación de rutas para la certificación de especialistas, todo esto usando un algoritmo de aprendizaje inteligente.

Importante: en este documento se habla indistintamente de colaboradores, participantes o aspirantes, tratándolos como un individuo que responde o responderá el formulario de detección de necesidades en el área de la ciberseguridad y al cual se le desarrollará una ruta de aprendizaje en el área de la ciberseguridad.

1.2 Planteamiento del problema

La empresa Código Verde efectúa exámenes de diagnósticos para identificar perfil de conocimientos y con ello establecer rutas de capacitación en el área de la ciberseguridad, obteniendo la información de los colaboradores (individuos que desean capacitarse en el área). Estos diagnósticos son realizados de manera manual y siendo analizados por expertos que evalúan los conocimientos del individuo, con el fin de determinan una estrategia para la capacitación y posteriormente la certificación.

Realizar el análisis de conocimientos de diferentes individuos es un trabajo arduo, además de ser limitado a una cierta cantidad de exámenes, ya que depende del tiempo disponible de los expertos. La experiencia del evaluador (expertos en ciberseguridad) es otro factor que se debe tomar en cuenta al momento de evaluar.

Considerando lo anterior este trabajo se enfocó en el problema de:

Proponer un sistema que ayude a sistematizar la toma de decisiones para la asignación de rutas de capacitación en ciberseguridad considerando el perfil de conocimiento de los candidatos.

La organización que reciba las capacitaciones obtendrá empleados más capaces, que redunda en datos más seguros. Por parte el trabajador o persona independiente logrará el aprendizaje necesario en ciberseguridad para tener actividades de mayor responsabilidad e igual puestos con perfil definido en el área de la seguridad de datos.

1.3 Preguntas de investigación

La pregunta principal que se planteó para la realización del sistema, fue la siguiente:

¿Cómo desarrollar un sistema que ayude a establecer el perfil de conocimientos en el área seguridad de la información, con el objetivo de especificar uno o varios cursos de capacitación adecuado a las necesidades de una persona u organización en particular?

Las preguntas específicas que se plantearon para la realización del sistema, fueron las siguientes:

1. ¿Cuáles son los conocimientos requeridos para distintos puestos en el área de ciberseguridad?
2. ¿Qué metodología es adecuada para obtener el perfil de conocimiento de candidatos a capacitación en ciberseguridad?
3. ¿Cómo desarrollar un sistema informático que ayude en la captura de los datos de los candidatos?
4. ¿Cómo se puede evaluar la eficiencia del sistema que se proponga?
5. ¿Qué características debe tener el perfil de los candidatos a cursos en seguridad informática, para poder identificar la ruta de capacitación más adecuada para ellos?
6. ¿De qué manera analizar el perfil de los candidatos en el sistema para seleccionar los cursos de capacitación disponibles más adecuados para el desarrollo de una persona en particular?

1.4 Objetivo General:

Diseñar y desarrollar un sistema capaz de almacenar los conocimientos de un individuo en el área de la seguridad de la información, de forma que facilite su evaluación y con ello establecer una ruta de capacitación adecuada, de acuerdo al rol de trabajo que desarrolla o desarrollará.

1.4.1 Objetivos específicos establecidos al iniciar el proyecto

- Estudiar los antecedentes, identificando las principales áreas temáticas que se requiere investigar para el presente proyecto.
- Determinar el alcance y delimitaciones del sistema a realizar.
- Determinar la metodología de investigación para definir la mejor manera de obtener los datos a ser evaluados.
- Determinar los puntos y cuestiones que se evaluarán para definir perfil de conocimientos en el área de la ciberseguridad.
- Determinar los puntos y cuestiones que se evaluarán para definir las rutas de aprendizaje en el área de la ciberseguridad.
- Determinar requerimientos funcionales y no funcionales del sistema.
- Diseñar y desarrollar el sistema de apoyo a la definición de rutas de capacitación en ciberseguridad.
- Verificar y proponer mejoras al sistema desarrollado.

1.5 Justificación

Analizar de manera manual los perfiles de candidatos a cursos de capacitación, en el área de la ciberseguridad, es una tarea tediosa y que consume tiempo, lo que limita la cantidad de personas a evaluar, así como de cursos a ofrecer, por lo que el desarrollo de este sistema que automatiza, al menos en parte este proceso, da la capacidad de procesar una mayor cantidad de candidatos, y de esa forma contribuir al mejoramiento y aumento de especialistas en el área de la seguridad de la información.

La implementación de este sistema auxilia en el proceso de selección, asiste en el establecimiento de un plan de capacitación para una persona u organización, ofreciendo una o varias recomendaciones. Es en parte, un instrumento facilitador, que permite la operatividad y efectividad en la toma de decisión de la empresa. Más específicamente se buscó reducir los tiempos de evaluación de los exámenes de diagnóstico y en proporción contraria un aumento de la cantidad de exámenes que se puedan realizar en un tiempo determinado.

El sistema favorece en la reducción de tiempo y esfuerzo en la realización de las actividades mencionadas anteriormente. Las personas beneficiadas son los expertos en ciberseguridad, que en sí son los que toman la decisión del plan de capacitación. Se considera que la etapa de selección es una parte crítica para definir las acciones a seguir en la capacitación, así que se obtiene un beneficio altamente cuantificable en tiempo-esfuerzo y mayores oportunidades de negocio.

1.6 Alcances y delimitaciones

Alcances

- Este sistema se desarrolló con el objetivo de ser aplicado en toda Latinoamérica, siendo utilizado por usuarios expertos e inexpertos en el área de las TI, por lo que se estableció un software ligero, fácil de usar e implementar en cualquier parte del país.
- Identificación de las certificaciones a realizar tomando en cuenta los puntos cuantificables, como los estudios obtenidos en el área de las TI, experiencias en ciertas áreas, exámenes de certificación realizados, responsabilidades y preguntas específicas sobre sus intereses personales.
- Detecta en cierta medida las principales debilidades y fortalezas de conocimientos en el área de la ciberseguridad de un individuo, considerando para ello, cierta cantidad de preguntas específicas a contestar.

Delimitaciones

- Los resultados del sistema están delimitados a las experiencias y necesidades de la empresa Código Verde, siendo estos los que realicen la valoración final, calificando la exactitud del sistema.
- Las certificaciones, roles de trabajo y en general los conocimientos en ciberseguridad son temas extensos, además de cambiantes en su temario, por la rápida evolución de la tecnología.
- La Información inconsistente de cada persona a evaluar tomando en cuenta los criterios basados en la experiencias, responsabilidades y visión de cada uno. El conocimiento tácito es un punto complicado de evaluar, cuando se trata de una variedad de individuos.

- No se conoce las necesidades y problemáticas propias de la organización u individuo a evaluar.
- La distancia entre el desarrollador del proyecto y la empresa código verde fue una limitante fuerte, ya que no se observaron los procesos de trabajo y el producto final del mismo, directamente en la organización. Esto limita los comentarios e ideas expuestas por los expertos en seguridad de la empresa.

1.7 Metodología de trabajo

La metodología de trabajo utilizada en este proyecto está basada en el ciclo de vida del desarrollo de software (SDLC); la estructura de la Ilustración 1 contiene los procesos, actividades y tareas relacionadas con el desarrollo y validación de un producto de software, abarcando la vida completa del sistema, desde la definición de los requisitos hasta la implementación.

Ilustración 1. Proceso Metodológico del proyecto.

El desarrollo del proyecto fue un proceso interactivo de investigación, definiciones e identificación de conceptos, con constantes cambios en la planificación del proyecto, avanzando en cada iteración en el proceso de análisis, la arquitectura y las validaciones del sistema. De la metodología utilizada se dejó fuera el capítulo 7, conclusiones de la tesis, ya que el proyecto se encuentra en su fase de prototipado.

1.8 Estructura del documento

La elaboración del proyecto se divide en seis fases generales, las cuales se desglosan en puntos específicos en un organigrama, estableciendo fechas de entrega:

En el primer capítulo se define la problemática a solucionar, los objetivos del proyecto, justificación, alcances y delimitaciones, así como la estructura del documento.

En el segundo capítulo se desarrolla el marco teórico, especificando conceptos básicos, así, como el informe de proyectos realizado por investigadores en relación al tema de la propia tesis.

En el tercer capítulo se analiza la secuencia de pasos que realiza código verde, en forma general, para la determinación de las certificaciones que se ofrecen y la mejor ruta de aprendizaje en el área de la seguridad de la información. Continuando, se especificaron los requerimientos del sistema con el objetivo de establecer qué es lo que se espera que realice el mismo, además de obtener una conclusión que apoye como guía para la creación del diseño de la solución.

En el cuarto capítulo se presenta el diseño de la arquitectura del sistema, lo cual dio paso al desarrollo del prototipo para dar solución a la problemática planteada.

En el quinto capítulo se describe el desarrollo del prototipo que dio solución a la problemática planteada.

En el sexto capítulo se valida la solución desarrollada en la etapa previa del proyecto, realizando pruebas de laboratorio, obteniendo retroalimentación con los resultados obtenidos.

El séptimo capítulo se presentan las conclusiones del proyecto, que se espera que sean las bases para futuras investigaciones, ya que hay variantes que no fueron posibles determinar en la investigación de este proyecto.

2 Marco Teórico

En esta sección se aborda el concepto de ciberseguridad, se da una breve revisión al estado actual de la ciberseguridad, y se aborda el tema de la formación de recursos humanos en ciberseguridad.

Como se habló en el capítulo anterior en la redacción del antecedente, en el planteamiento del problema, como también del objetivo del proyecto, la gestión de información replantea el mercado laboral del profesional de la información, demanda un nuevo tipo de profesional con importantes responsabilidades en el diseño y el desarrollo de sistemas informáticos. En paralelo nace la gestión del conocimiento, considerada como la teoría de gestión que responde a la adaptación de últimas innovaciones tecnológicas en el tratamiento de la misma [34].

Conocer los temas competentes a este proyecto es de importancia para el entendimiento del mismo, por lo que en este apartado se desarrolla la conceptualización y definiciones, que ayudarán a la comprensión metodológica del documento.

2.1 Ciberseguridad

Si bien el término ciberseguridad es ampliamente usado, es un concepto que no ha sido bien definido, representa más bien una especie de generalización de una amplia variedad de conceptos, todos ellos relacionados con riesgos, vulnerabilidades, fallas, etc. de equipos de cómputo, software, sistemas de información, etc. que abarcan aspectos de infraestructura física, software, tecnologías, pasando también por aspectos sociales, políticos, organizacionales, económicos, ecológicos y humanos [26].

La Unión Internacional de Telecomunicaciones en el informe de recomendaciones UIT-T X.1205 define Ciberseguridad como: “El conjunto de herramientas, políticas, conceptos de

seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciber-entorno" [25].

Otras definiciones planteadas es la de fundación telefónica en su libro "ciberseguridad, la protección de la información en un mundo digital" en la cual indica que es un "proceso que implica prevención, detección y reacción o respuesta, y que debe incluir un elemento de aprendizaje para la mejora continua del propio proceso. Dividiendo la gestión de la seguridad en etapas: prevención, detección, respuesta e inteligencia" [8].

Según la fundación telefónica la prevención se refiere a control de accesos y gestión de identidades, prevención de fugas de datos, seguridad de red, gestión de vulnerabilidades [8]. A lo que refiere la detección es la monitorización continua y en combinación a con la prevención, está la gestión de vulnerabilidades. Para la respuesta ante cualquier falla se debe tener sistemas de recuperación o contramedidas para resolverlo. En la etapa de inteligencia en la que se desea hacer frente a amenazas o riesgos desconocidos, se da hincapié en la compartición de datos, pero principalmente los datos open source [8].

En sí, la seguridad de la información es una forma de aplicar conocimientos y tecnologías para proteger todo lo relacionado a las procesos y controles de sistemas, redes, programas, dispositivos y datos. Por ello este concepto se ha convertido en una prioridad total para las organizaciones e incluso particulares que desean tener sus datos seguros.

De las definiciones anteriormente mencionadas ya se deberá tener una perspectiva amplia de lo que es ciberseguridad. La ciberseguridad es un tema de suma importancia en nuestra era, ya que gran parte de la economía, tanto nacional como a nivel mundial se encuentra ligada con la utilización de tecnología digital, con la cual se opera y se procesan los datos, lo que a su vez es un objetivo para los cibercriminales.

2.2 Perspectiva global de la ciberseguridad

En esta época las computadoras, las aplicaciones digitales, dispositivos inteligentes se han vuelto algo común en nuestra sociedad y con ello un aumento en el tráfico y manejo de datos digitales ya sean tratados de manera segura o inseguras por los sectores públicos, privado y sociales.

El entender la necesidad, al igual que la importancia de profesionales especializados como personal con conocimientos en ciberseguridad se requiere conocer la perspectiva a nivel mundial del uso de las tecnologías digitales con más uso y crecimiento, dentro de la población en general. Como ejemplo tenemos las estadísticas del uso del internet por usuario, donde actualmente más del 50% de la población a nivel mundial se encuentra conectada al internet esperando un aumento al 66% para el año 2023. Prácticamente dos tercios de la humanidad poseen un dispositivo móvil, esperando un aumento para el 2023 al 71% de la población [27] (Véase Tabla 1).

Tabla 1. Informe anual de Internet de Cisco. Reporte a nivel mundial [4].

Nivel mundial	Año 2023	Año 2018
Usuarios con Internet	5.300 millones (66% de la población)	3.900 millones (51% de la población)
Usuarios con dispositivos móviles a nivel mundial	5,7 mil millones de usuarios (71% de la población)	5,1 mil millones (66% de la población)
Población a nivel mundial	8.0 mil millones	7.6 mil millones

El aumento del uso del internet está en paralelo con el incremento del uso de equipos conectados al internet. Los dispositivos conectados al internet fueron arriba de 2.4 equipos por persona en 2018, con una proyección a 3.6 dispositivos por persona para el 2023 [4].

En la Tabla 2 se muestra el informe anual de américa del norte de usuarios por millón y el porcentaje de la población total que usaron el internet en el 2018 y su previsión para el 2023.

Tabla 2. Informe anual de Internet de Cisco. Reporte de américa del norte [4].

América del norte	Año 2023	Año 2018
Usuarios con Internet	344,8 millones de usuarios de Internet (92% de la población)	327,9 millones (90% de la población)
Usuarios con dispositivos móviles	329,2 millones de usuarios móviles (88% de la población)	312,8 millones (86% de la población)
Población en américa del norte	375,4 millones	364,2 millones

En la zona de américa del norte (Canadá y Estados Unidos) el uso del internet en la población es arriba del 90%, esperando que para el 2023 sea de un 92%. Los usuarios de dispositivos móviles superaron el 86%, esperando un leve aumento al 88% en el 2023 (véase Tabla 3).

Así mismo, en América del Norte, los dispositivos conectados al internet fueron arriba de 8.2 equipos por persona en 2018, con una proyección a 13.4 dispositivos por persona para el 2023 [4].

Tabla 3.Informe anual de Internet de Cisco. Reporte de México [4].

México	Año 2023	Año 2018
Usuarios con Internet	85,6 millones de usuarios de Internet (64% de la población)	76,2 millones (60% de la población)
Usuarios con dispositivos móviles	102.6 millones de usuarios móviles (77% de la población)	94.2 millones (75% de la población)
Población en américa del norte	132.8 millones	126.2 millones

En México el uso del internet es de casi las dos terceras partes de la población con un 60%, esperando que para el 2023 sea de un 62%. Los usuarios de dispositivos móviles superan el 75%, esperando un leve aumento al 77% para el 2023. (véase Tabla 3)

En México, los dispositivos conectados al internet fueron arriba 2.2 equipos por persona en 2018, con una proyección a 3.2 dispositivos por persona para el 2023 [4].

Según World Economic Forum en el The Global Risks Report 2020 15va edición [44]:

“En la cuarta revolución Industrial (4RI) las tecnologías generan enormes beneficios económicos y sociales para gran parte de la población mundial. […] La medicina de precisión, los vehículos autónomos y los drones son mercados de rápido crecimiento, mientras que se espera que la inteligencia artificial (IA) por sí sola impulse el crecimiento global en un 14% para 2030”.

Se estiman 300 millones de dispositivos conectados para 2025 en México [18]. El crecimiento de 70% de dispositivos para el 2025 requerirá un crecimiento de más de 300% del poder computacional de centros de datos. Más del 94% de este poder computacional estará en la nube [18].

Diagrama 4. Cada vez más dispositivos conectados [18].

En el Diagrama 4 se observa gráficamente el aumento de los dispositivos conectados al internet, ejemplificando lo mencionado en el párrafo anterior. La línea de color morado muestra el aumento de los miles de millones de dispositivos conectados en el mundo desde el 2003 a lo que se espera hasta el 2025. La línea de color verde muestra el aumento en millones de dispositivos conectados en México desde el 2003 a lo que se espera hasta el 2025. La línea gris indica gráficamente la población en millones en México, desde el 2003 hasta lo que se espera para el 2025.

El secretario general de la UIT, Houlin Zhao, comentó que un grupo específico definirá los requisitos del aprendizaje automático en relación con la tecnología, las arquitecturas de red y los formatos de datos [14]. En esta labor tendrá especial importancia la definición de los formatos de datos necesarios y los mecanismos correspondientes para proteger la seguridad y la privacidad [14].

2.2.1 Riesgos de la Ciberseguridad

En México, más de 33 millones de personas fueron afectadas por el cibercrimen en 2017, Es decir, una de cada cuatro personas [18].

La Ley Hypponen de seguridad informática menciona “Cuando un dispositivo es descrito como inteligente se vuelve vulnerable”, en donde se especifica que varias de las nuevas tecnologías que están y las que van a estar conectadas a la red, refiriéndose al Internet de las cosas (IoT), trae consigo un problema de seguridad [10]. Estos dispositivos en general son vulnerables, como ejemplo puede ser una lavadora, un refrigerador, un aire acondicionado, etc., cualquier aparato conectado al internet, por lo que indica la importancia de la ingeniería de la seguridad en la fabricación de estos productos que se encuentran conectados [10].

La complejidad tecnológica de los crímenes y su diversidad son factores que dificultan su persecución y eventual sanción [18]. El aumento de la velocidad y uso de la red en sus avances generacionales, desde las más usadas actualmente la 3G hasta 5G, en conjunto con los avances en equipos inteligentes y con potencias extraordinarias, están creando vulnerabilidades en paralelo con ellas mismas [27].

Las organizaciones de nivel mundial o gubernamental que establecen políticas o reglas para la tecnología deben tener cuidado de que estas no sean ineficientes o no congruentes para resolver el problema de la ciberseguridad, ya que se corre el riesgo de una caída económica o política, entre otras cosas [27].

De acuerdo a la encuesta realizada por World Economic Forum y presentada en The Global Risks Report 2020 15th edición [45], en la que especifica que los ciberataques son un peligro para todas las personas y empresas, indica que los ciberataques son el séptimo riesgo más probable y el octavo más impactante, y el segundo riesgo más preocupante para hacer negocios a nivel mundial en los próximos 10 años [45]. Existen riesgos cibernéticos que no son específicos de una empresa y están relacionados con vulnerabilidades de sistemas utilizados por industrias enteras [18].

Diferentes organizaciones a nivel mundial muestran que entre los principales desafíos a nivel mundial está la ciberseguridad, ejemplo de ello es el informe de riesgos mundiales del Foro Económico Mundial 2017-2019 (véase Tabla 4) [27][44][45].

Tabla 4. Los cinco principales riesgos mundiales en términos de probabilidad [27][44][45].

	2017	2018	2019	2020	2021
1st	Eventos Meteorológicos extremos	Eventos Meteorológicos extremos	Eventos Meteorológicos extremos	Eventos Meteorológicos extremos	Eventos Meteorológicos extremos
2nd	Migración involuntaria a gran escala	Desastres naturales graves	Fracaso de la mitigación del cambio climático y la adaptación a este	Acciones climáticas fallidas	Acciones climáticas fallidas
3rd	Desastres naturales graves	**Ataques Cibernéticos**	Desastres naturales graves	Desastres naturales	Daño ambiental humano
4th	Ataques terroristas a gran escala	**Fraude o robo de datos**	**Fraude o robo de datos**	Pérdida de biodiversidad	Enfermedades infecciosas
5th	**Gran incidente de fraudes o robo de datos**	Fracaso de la mitigación del cambio climático y la adaptación a este	**Ataques Cibernéticos**	Desastres ambientales provocados por el hombre	Pérdida de biodiversidad
6th			Desastres ambientales provocados por el hombre	**Fraude o robo de datos**	**Concentración de la potencia digital**
7th			Migración involuntaria a gran escala	**Ataques cibernéticos**	**Desigualdad digital**

En el informe mencionado, se muestra el panorama de riesgos en evolución 2017–2021 donde se observa que entre los principales riesgos económicos a nivel mundial están aspectos de la seguridad en la tecnología, considerándose gran incidente de fraudes o robo de datos en

el 5to lugar del año 2017; ataques cibernéticos en 3ro y fraude o robo de datos el 4to lugar en el 2018; y en el año 2019 se consideró a los ataques cibernéticos en 5to y fraude o robo de datos en 4to; para él 2020 los fraudes o robos de datos en 6to y a taquetes cibernéticos en el séptimo; ya en el 2021 la concentración de la potencia digital se encuentra en el 6to y desigualdad digital en el 7to [27][44][45]. Estos datos hacen ver que las personas mal intencionadas están presentes en todo el mundo y que continuamente están buscando vulnerabilidades en los sistemas, para cometer delitos.

Se estima que el costo total anual financiero en delitos cibernéticos en la economía mundial sobrepasó los 172 mil millones de USD en el 2017 [18] . El costo financiero del cibercrimen para los consumidores mexicanos en ese año fue de 7.7 miles de millones de USD [18].La importancia de la ciberseguridad para el sistema financiero mexicano se evidencia también por los esfuerzos que se han venido realizando en ámbitos legislativos. Por ejemplo, en el informe anual más reciente de la CNBV, el primer punto abordado corresponde a la denominada Ley Fintech, la cual se enfoca en buscar aprovechar los beneficios del uso de las nuevas tecnologías en el sector financiero, pero también los riesgos que estas conllevan [22].

Quizá el sector en el que más impacta la ciberseguridad en México es el financiero. En este ámbito, la Comisión Nacional Bancaria y de Valores (CNBV), en conjunto con la Organización de Estados Americanos (OEA), en 2019 emitieron un reporte titulado “Estado de la Ciberseguridad en el Sistema Financiero Mexicano”. En el mencionado estudio, se analiza la situación del sector financiero mexicano con respecto a la ciberseguridad, identificando los principales riesgos y su impacto, así como recomendaciones [22]. Es de destacar que dicho informe encontró que el 100% de las instituciones financieras reportan haber sido víctimas de ataques cibernéticos, hayan sido estos exitosos o no. Los eventos de seguridad digital más comúnmente identificados son [22]:

i) El código malicioso o malware (56% del total de entidades).
ii) El phishing dirigido para tener acceso a sistemas de la entidad (47% del total de entidades).

iii) La violación de políticas de escritorio limpio (clear desk) (31% del total de entidades).

Se destaca que un 19% de las entidades e instituciones financieras identifican ocurrencia de eventos de malware diariamente [22]. Los riesgos de seguridad de la información que consideran que merecen mayor atención por parte de las entidades e instituciones financieras de México, sin importar el tamaño de la organización, son:

i) La pérdida / robo de activos de información clasificada (confidencial o sensible),
ii) El secuestro de información, y
iii) El compromiso de credenciales de usuarios privilegiados.

Un dato importante que arroja el reporte mencionado es que "el costo total anual de respuesta y de recuperación ante incidentes de seguridad digital de las entidades e instituciones financieras en México en 2018 fue de $ 107 millones [de dólares] aproximadamente" [22].
Es importante resaltar que no sólo el sector financiero mexicano está expuesto a los riesgos de ciberseguridad; de hecho, se considera que México es uno de los países que más ciberataques recibe, con estimaciones que superan el 82% para empresas que han sido víctimas de ciberataque [9]. Los problemas de ciberseguridad que se han sufrido en el país en los últimos años lo han posicionado en el lugar 52 para el 2020 del índice global en ciberseguridad [13]. Algunos de los eventos más relevantes se listan en la tabla 5.

Tabla 5. Algunos ejemplos de hackeos o incidentes de seguridad en México en los últimos años [46], [47], [48], [49].

Año	Organización	Descripción
2020	Condusef, SAT y Banxico	Sufrieron afectaciones en sus respectivas páginas de internet por causa del "defacement"; la cual es una técnica de hacking con la cual los perpetradores modifican la apariencia de una página web administrada por las víctimas de su ciberataque. [46]
2019	PEMEX	Ataque tipo Ransomware que afectó al 5% de los equipos de cómputo de PEMEX, los cibercriminales exigían casi 5 millones de dólares. [47]
2018	SPEI/Financiero	Ataques a Participantes del Sistema de Pagos Electrónicos Interbancarios (SPEI). [48]
2017	Todos	El virus Wannacry afectó a miles de computadoras de más de 500 empresas entidades públicas, e individuos en 150 países. [49]

En los últimos años la seguridad de la información se volvió un tema que compete a todos, ya que en la actualidad muchos aspectos de la vida diaria están influenciados por la tecnología. Ejemplo de ello es el estudio realizado por INEGI, que en su comunicado de prensa número 179/19, informa las principales actividades que los usuarios de internet realizan; entre las principales están entretenimiento, comunicación, obtener información, entre otras [11].

En la actualidad los ciberataques se han convertido en un tipo de negocio para algunos, los cuales ofrecen sus servicios o venta de información, por lo que se ha vuelto esto en problema para la seguridad de las personas y las empresas.

2.3 Recurso humano en la ciberseguridad

Las entidades e instituciones financieras reportan que necesitan de más profesionales en el área de las tecnologías de la información, llevando en muchos casos a requerir procesos de tercerización, siendo la actividad que más frecuentemente se contrata la relativa a la realización de pruebas de seguridad / análisis de vulnerabilidades con un 34% del total, seguida del monitoreo de la infraestructura de seguridad con un 31% del total [1].

En un estudio publicado en el 2016, ISACA pronosticó que para el 2019 habría una escasez de 2 millones de profesionales de Seguridad Informática en el mundo, y que Cybersecurity Ventures pronosticaba que la brecha aumentaría a 3.5 millones para el 2021. Esto es consistente con lo reportado en Strategies for Building and Growing Strong Cybersecurity Teams. In (ISC)2 Cybersecurity Workforce Study (Vol. 2019), indica que la fuerza laboral de seguridad cibernética necesita crecer un 62% para cumplir con las demandas de las empresas estadounidenses en la actualidad, que se estiman en 805,000, pero al considerar 10 de las principales economías, la cifra sube a 2.8 millones, con estimaciones de hasta 4.07 millones a nivel global, lo que indica que la fuerza de trabajo en ciberseguridad a nivel global

necesita crecer en 145% [1]. Para el caso particular de México, hay estimaciones que sostienen que para 2022 se requerirán entre 1.8 y 2 millones de especialistas en ciberseguridad

El incremento de la necesidad de especialistas en ciberseguridad está muy relacionado con los avances de la denominada Industria 4.0, pues los riesgos relativos a la ciberseguridad representan una de las principales barreras para la adopción de las nuevas tecnologías que esta revolución industrial trae aparejadas [2], lo que convierte a la ciberseguridad en un área esencial para la formación de los profesionales del futuro.

Debido a la dificultad que encuentran las empresas para obtener especialistas en áreas como la ciberseguridad, éstas buscan alternativas de solución, como la tercerización de servicios, o el trabajar de la mano con socios que les permitan lograr especializarse [15]. Todo esto muestra la necesidad de buscar estrategias que permitan ampliar la fuerza de trabajo en ciberseguridad. No obstante, lograr lo anterior no es una tarea fácil, pues la ciberseguridad es un área sumamente amplia, así como los diferentes tipos de perfiles que requieren diversos niveles de especialización.

Aun cuando la ciberseguridad es un área que atrae a los profesionales de las TIs, es un área difícil para especializarse. Por ejemplo, en el estudio reportado en [8], se observó que el 65% de los profesionales de TI que trabajan en empresas relacionadas a la ciberseguridad quisieran trabajar en ciberseguridad por el resto de sus carreras, no obstante, la gran mayoría (81%) reportan que requieren certificaciones o capacitación para prepararse para futuros roles. Entre las áreas donde se reporta la necesidad de estas certificaciones y/o capacitaciones se encuentran las siguientes:

- Seguridad en cómputo en la nube
- Evaluación, análisis y administración de riesgos
- Gobernanza, conformidad y administración de riesgos (GRC)

- Seguridad y análisis inteligente de amenazas
- Ingeniería y administración de seguridad
- Pruebas de penetración
- Detección de intrusiones
- Monitoreo de red

Las motivaciones de los participantes del estudio reportado [26], para obtener esas certificaciones, giran principalmente en torno a un deseo de mejorar en su trabajo o aprender más. De hecho, según los encuestados, el principal motivador para obtener una certificación de ciberseguridad es mejorar o agregar a un conjunto de habilidades. Otros de los motivadores es mantenerse competitivos en la industria, avanzar en su carrera y convertirse en un experto [26]. Mucho más abajo en la lista está el deseo de ganar más dinero. Como resultado, el 84% de los profesionales de ciberseguridad planean buscar una nueva certificación en algún momento, mientras que el 59% actualmente está buscando una nueva certificación o planea hacerlo dentro del próximo año [26].

Todo lo anterior muestra una evidente necesidad de formación de profesionales en el área de la ciberseguridad, una tarea que no es fácil, pues la alta diversidad en alternativas de especialización, así como de perfiles de candidatos a realizar dichas especializaciones, dificulta el diseñar programas para capacitar a profesionales de diversas áreas de las TI, e incluso de otras disciplinas, tarea que representa un reto que es necesario enfrentar.

2.3.1 Ocupación en tecnología de la información y comunicación

Las estadísticas por edad relacionado a la ocupación en las tecnologías de la información y de la comunicación es un dato importante a nivel nacional, ya que muestra una perspectiva de la cantidad de usuarios responsables de mantener segura los datos digitales que se

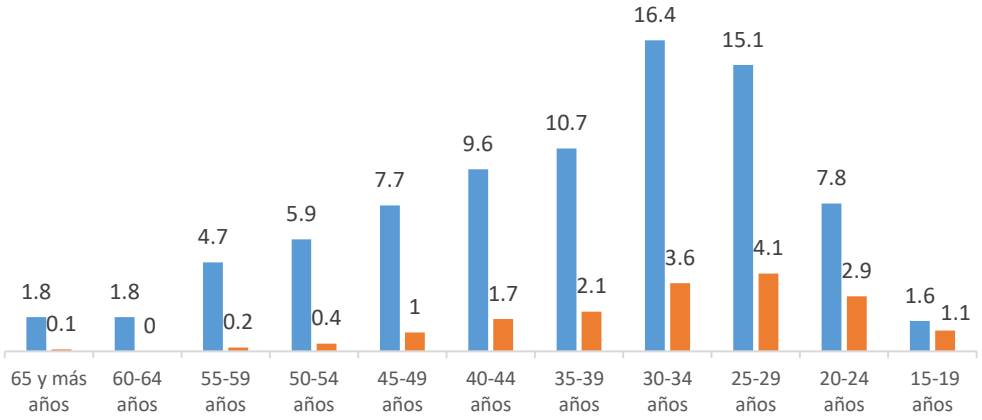

Diagrama 5. Distribución de la población de 15 años y más ocupada en las TIC por edad y sexo, 2018 [12].

manejan, ya sea de manera directa o indirecta. En el Diagrama 5 se muestra los porcentajes de la distribución de la población de 15 años y más ocupada en las TIC por edad y sexo:

Datos de la encuesta nacional de ocupación de empleo, ENOE, realizada por INEGI, en cuarto trimestre del 2018 menciona:

- Al cuarto trimestre de 2018 son poco más de 752 mil las personas ocupadas relacionadas con las tecnologías de la información y de la comunicación (TIC) en el país.
- Su edad promedio es de 36.3 años; 83% son hombres y 17% mujeres.
- De cada 100 personas ocupadas en las TIC, 76 trabajan principalmente en forma subordinada y remunerada, 20 laboran por su cuenta, tres son empleadores y uno trabaja sin recibir remuneración alguna.

2.3.2 Ingresos por trabajo

Las personas ocupadas en las TIC ganan en promedio 56.5 pesos por hora trabajada [11]. Considerando el nivel de ingresos por salario mínimo mensual que perciben las personas con estas ocupaciones, destaca que de cada 100, 45 ganan más de tres salarios mínimos. Por sexo, se advierte la mayor proporción de mujeres respecto de los hombres en los menores niveles de retribución, principalmente entre los que no la reciben y los que perciben hasta un salario mínimo.[1]

Quienes se ocupan en las TIC suelen mantenerse relativamente estables en su trabajo, ya que 68 de cada 100 han durado en su empleo más de tres años; 16 han permanecido entre uno y tres años, y los 16 restantes, de uno a 12 meses [11]. En el Diagrama 6 se muestra el promedio de Ingreso mensual de la población de 15 años y más ocupada en las TIC por nivel de escolaridad según sexo:

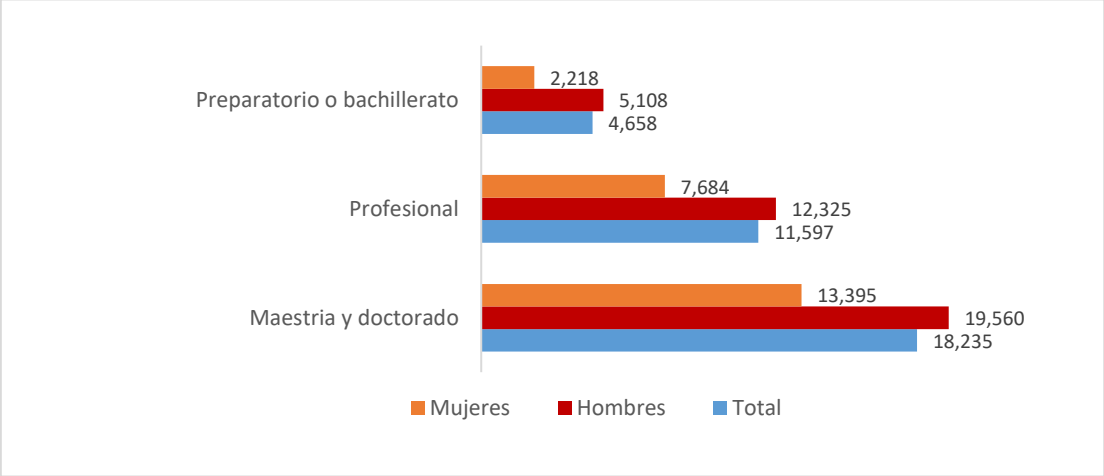

Diagrama 6. Promedio de Ingreso mensual de la población de 15 años y más ocupada en las TIC por nivel de escolaridad según sexo, 2016. [12]

[1] Salario mínimo general diario de $ 88.36 establecido por la Comisión Nacional de Salarios Mínimos Vigentes a partir del 1° de enero de 2018 (Secretaria del Trabajo y Provisión social, 2018)

2.3.3 Perfil y roles del recurso humano en el ámbito de la ciberseguridad

Contar con el recurso humano en ciberseguridad, con los niveles de personal adecuados es un desafío para las empresas, aunque no imposible si se contrata continuamente personal externo y experto en ciberseguridad, además de continuar capacitando a los profesionales internos de TI [1]. Los profesionales internos y encargados de proteger los activos críticos de una organización tienen muchos títulos: director o gerente de seguridad de TI, arquitecto y/o ingeniero de seguridad, especialista en seguridad, consultor, asesor o simplemente personal de TI [1].

Gestionar la información replantea el mercado laboral del profesional actual, demandando nuevos tipos de conocimientos y habilidad e importantes responsabilidades en el diseño y el desarrollo de sistemas informáticos. Por lo que es importante gestionar el conocimiento, considerando como la teoría de gestión que responde a la adaptación de últimas innovaciones tecnológicas en el tratamiento de la misma [26].

En la actualidad los ciberataques pueden afectar a cualquier persona u organización, desde un variado campo de la vida diaria hasta situaciones críticas como en sistemas financiero o infraestructura en un sistema nuclear [26].

Considerando estas amenazas diarias que afectan la integridad, disponibilidad y confiabilidad de la información, incluyendo la seguridad de los sistemas de todos los ámbitos del sector socioeconómico, estructurales entre otras, se deben tener especialistas en el área de la ciberseguridad, ya que no por el hecho de saber que existen los peligros, quiere decir que estamos protegidos [18]. El experto deberá estar capacitado para prevenir la infinidad de riesgos y estar preparado para corregir la variedad de afectaciones causadas por un ciberataque. Se debe dedicar tiempo y esfuerzo en proteger el surgimiento de nuevos modelos de negocio de forma segura al igual que el acceso, ya sea gratuito o de paga, al conocimiento

para la sociedad. El especialista en ciberseguridad debe entender lo que protege, tomando en cuenta los beneficios crecientes del internet, el cual se refleja en un aumento del PIB a nivel mundial, con más de 3%, y las tecnologías de la información que propician productividad y crecimiento de empresas [18].

En las organizaciones se deben definir con anticipación los perfiles y roles del recurso humano como aspecto importante en la planeación laboral y generalmente se designa a un responsable de la seguridad de la información y de todos los aspectos que conlleva mantenerla sin problemas.

En la actualidad hace falta talento calificado en ciberseguridad en todo el mundo, esto es una realidad, y siguen en aumento el déficit del mismo. Se estima que esta crisis alcance los 1.8 millones de empleos sin poder ser cubiertos a nivel mundial para 2022 [7]. Para México, las estimaciones no son menores a los 200 mil profesionales. Esto advierte la importancia de identificar las necesidades específicas para México, mismas que puedan ser expresadas en contextos regionales, ocupacionales y de perfil o materia técnica, con objeto de instrumentar adecuados mecanismos de subsanación. En [3] se menciona que en México existen solo dos programas de licenciatura de seguridad informática, y a nivel posgrado, tres maestrías; pero para el año 2021, de acuerdo a investigación personal, existen una gran variedad de carreras profesionales y maestrías del área de la ciberseguridad, y que en su mayoría se pueden tomar de manera online.

Según una encuesta de ((ISC)2, 2019) [1], los roles más comunes en los equipos de seguridad son: Seguridad de Operaciones, Administración de Rriesgos, Cumplimiento de Gestión Operativo, Seguridad tecnológica, Software seguro, Pruebas de penetración de desarrollo, Forense ((ISC)2.

2.3.4 Formación en ciberseguridad (Cybersecurity Education)

El tamaño de la fuerza laboral actual todavía deja una brecha significativa entre la cantidad de profesionales de ciberseguridad que trabajan en el campo y la cantidad necesaria para mantener seguras a las organizaciones [1], por lo que la concientización, educación y capacitación en materia de ciberseguridad es una de las tareas más relevantes para abordar la problemática de la ciberseguridad en México y otros países, ya que las organizaciones dedican una buena parte de sus esfuerzos en estas áreas [22].

El Sistema Nacional de clasificación de ocupaciones 2018 (SINCO) describe varios puntos para la utilidad de la información sobre ocupaciones, en uno de ellos menciona que sirve para contribuir y anticipar la formación educativa y de capacitación [53]. Se entiende que es importante tener una buena planeación, el cual apoye en determinar los requerimientos mínimos y recomendados de la educación para lograr funcionar de acuerdo a las exigencias del mercado, como para que las personas puedan acceder a ocupaciones formales y bien remuneradas [53].

A medida que aumenta el nivel de desarrollo de un país, mayor importancia adquieren los antecedentes [53].

Con respecto al ámbito de la educación en ciberseguridad se encuentra la Iniciativa Nacional para la Educación en Ciberseguridad (NICE) de los Estados Unidos, el cual es un esfuerzo por definir un marco referencial en el que se define tareas, habilidades y capacidades (KSA) para la fuerza laboral, así como para proporcionar una taxonomía y un léxico comunes para clasificar los puestos, conocimientos y habilidades de los trabajadores [50]. Esta referencia esta exclusivamente diseñada para cumplir con las disciplinas fundamentales de la ciberseguridad.

The National Initiative for Cybersecurity Education National Cybersecurity Workforce Framework (v2.0), se define como:

"Una estructura de referencia que describe la naturaleza interdisciplinaria del trabajo de ciberseguridad y sirve como un recurso de referencia fundamental para describir y compartir información sobre el trabajo de ciberseguridad y el conocimiento, habilidades y capacidades necesarios para completar tareas que pueden fortalecer la postura de seguridad cibernética de una organización" [7].

El NICE Framework (v2.0) está dividido en siete categorías y cada una subdividida en treinta y tres áreas de especialidad. Cada área de especialidad está estructurada en roles de trabajo contando actualmente con un total de cincuenta y dos; a su vez cada una define los conocimientos, habilidades y tareas necesarias para cumplir con el perfil del rol [50]. Las categorías son las siguientes:

1. Securely Provision (Provisión segura).
2. Operate and Maintain (Operar y mantener).
3. Oversee and Govern (Supervisar y gobernar.).
4. Protect and Defend (Proteger y defender).
5. Analyze (Analizar).
6. Collect and Operate (Recoger y operar).
7. Investigate (investigar).

Para más información véase Tabla 38, Anexo A. Donde se muestran las categorías, áreas de especialidad y roles de trabajo propuesto por NICE Framework.

El marco referencial de la ciberseguridad es muy grande, en donde intervienen muchos factores para asegurar la información, los sistemas e incluso el hardware en sí. Ser un programador o técnico en reparación de equipos de cómputo e inclusive un experto en redes, no lo hace un experto en ciberseguridad, aunque algunos de los aspectos que manejan tengan relación, en sí su enfoque principal no es la seguridad. Hay que recalcar que es importante que se deben tener conocimientos específicos de formas de prevenir, analizar y corregir

aspectos inseguros de las tecnologías, las comunicaciones, manejo de datos, entre otros temas específicos. En sí no todos los que trabajan en el área de las TI tienen el mismo concepto de lo que es la ciberseguridad [19], ya que cada uno observa la seguridad desde su punto de vista y necesidades.

Existe una parábola, la cual implica que la experiencia subjetiva de uno puede ser verdadera, pero que dicha experiencia está inherentemente limitada por su incapacidad para explicar otras verdades o una totalidad de la verdad. Esta parábola es **"El síndrome de los seis ciegos y un elefante".** Entonces yace otra idea que dice si no estás seguro de que es seguro, no está seguro [19].

Lo mejor de los casos es tener una buena relación de los planes educativos con la necesidad de formación en ciberseguridad, ya sea para una sola persona u organización e igual se debe tener un plan nacional eficaz de capacitación que sea general en todo el país; considerar los requisitos de actualización de asignaturas y necesidades; importante tomar en cuenta la investigación y desarrollo como una de las principales consideraciones en la educación de la ciberseguridad [3].

Se menciona las variedad de disciplinas involucradas en la ciberseguridad y son: Gestión empresarial, informática, redes, ingeniería de software, ley y aplicación de la ley, estudios de comportamiento, auditoría y evaluación, ética [7]. Tomando en cuenta las diciplinas mencionas se creó la National Initiative for Cybersecurity Education, Workforce Framework (v2.0), en la cual se especifica los roles que una persona puede laborar de acuerdo a ciertas habilidades [50]. Cabe mencionar que este marco referencial le pertenece al NIST (National Institute of Standards and Technology) y la División Nacional de Seguridad Cibernética del Departamento de Seguridad Nacional de los Estados Unidos (DHS-NCSD).

La NIST es una sociedad entre el Gobierno de los Estados Unidos, las universidades y el sector privado, quienes están enfocados en la educación y capacitación en seguridad cibernética y en el desarrollo del personal [6]. Pero su misión es promover la innovación y la

competitividad industrial de los Estados Unidos mediante el avance de la ciencia, los estándares y la tecnología de medición de manera que mejoren la seguridad económica y nuestra calidad de vida [6].

El perfil profesional es la base del diseño curricular, que, a su vez, determina el plan de estudios y sus contenidos; elementos en permanente actualización que se deben ajustar en el tiempo y tienen en consideración variables internas y externas que influyen en la formación académica [20].

Las instituciones de educación y los programas requieren información de diversas fuentes para identificar competencias en áreas de la profesión que atiendan la demanda a distintos contextos de desempeño, lo cual genera la necesidad de disponer de instrumentos o herramientas para agilizar el proceso de recolección, análisis y consolidación de resultados para cada perfil [16].

2.3.5 Instituciones que ofrecen certificaciones en el área de la ciberseguridad

Actualmente existen varias instituciones que ofrecen certificaciones que cubren ciertos conocimientos y habilidades, y una determinada cantidad de certificaciones que cumplen con algún rol de trabajo.

En la Tabla 6 se especifican algunas de las casas certificadoras reconocidas. Algunas instituciones ofrecen certificaciones que constan de un grupo de cursos para lograr habilidades específicas para un rol de trabajo. Como dato, en algunas casas certificadoras, se especifica en qué puestos o roles se pueden desempeñar ofreciendo esas certificaciones. Para mera información se puede ver en anexos la tabla de área de especialidad y roles de puesto de trabajo.

Tabla 6. Algunas de las principales instituciones que ofrecen certificaciones en el área de la ciberseguridad a nivel internacional [51].

No.	Nombre	Página Web
1	ABCHS	https://www.globalhomeland.org
2	Certified Wireless Network Professional	https://www.cwnp.com
3	CERT	https://www.sei.cmu.edu
4	CompTIA	https://certification.comptia.org
5	DAMA	https://www.dama.org
6	DCITA	https://www.dcita.edu/
7	Defense Acquisition University	https://www.dau.edu/
8	EC Council	https://ciso.eccouncil.org
9	FEAC Institute	https://www.feacinstitute.org
10	Federal Acquisition Institute	https://www.fai.gov
11	FISMA Center	https://www.fismacenter.com
12	GIAC	http://www.giac.org
13	ICMB	https://www.axelos.com
14	IEEE	http://www.ieee.org.mx/cursos.html
15	ISACA	http://www.isaca.org
16	ISC2	https://www.isc2.org
17	ISFCE	http://www.isfce.com
18	Logical Operations	http://logicaloperations.com
19	Mile2	https://www.mile2.com/

Para más información ver la Tabla 39, anexo A. Donde se muestran una lista de certificaciones más conocidas.

Considerando las amenazas diarias que afectan la integridad, disponibilidad y confiabilidad de la información, incluyendo la seguridad de los sistemas de todos los ámbitos del sector socioeconómico, estructurales, entre otras, se deben tener especialistas en el área de la ciberseguridad, ya que no por el hecho de saber que existen los peligros, no quiere decir que estamos protegidos [18]. Por otra parte, si se quiere ser un profesional de ciberseguridad eficaz, debe tener una comprensión amplia y detallada de todos los componentes de TI, y aquellos con certificaciones de ciberseguridad tienen habilidades mucho más allá de lo que se requiere de otras certificaciones [1].

2.4 Perfil de conocimientos

Los perfiles de puesto son descripciones concretas de las características, tareas y responsabilidades que tiene un puesto en la organización, así como las competencias y conocimientos que debe tener la persona que lo ocupe [41].

Junior: se asocia directamente con profesionales que están comenzando a dar sus primeros pasos en el sector laboral al que pertenecen, normalmente no suelen tener más de dos años de experiencia, y aunque presentan conocimientos y dominio de cómo desarrollar las actividades básicas en su puesto de empleo, aún requieren cierto grado de acompañamiento y supervisión dentro de sus procesos [42].

Semi - senior: este profesional tiene entre dos y seis años de experiencia laboral. Es autosuficiente y aunque todavía se equivoca, no requiere de supervisión constante. Busca más asignaciones y es proactivo en su tiempo disponible. Su respuesta bajo presión no es excelente, más el resultado de su trabajo es bueno. El trabajador semi-senior tiene buen manejo de las herramientas necesarias para trabajar de manera exitosa [42].

Senior: se define concretamente como un profesional con experiencia, normalmente de más de cinco o seis años de trayectoria laboral dentro de empresas de su sector. Esto los lleva a tener un grado superior de autonomía, conocimientos y dominio general de todos los procesos, herramientas y métodos para desarrollar las actividades centrales de su trabajo aportando el máximo valor [42].

2.5 Resumen

En este capítulo se conceptualizan temas que le darán claridad a lo que se desarrolló como parte de este proyecto, ofreciendo las bases del entendimiento de lo que se investigó, analizó, y diseñó en este proyecto. Se presentan las teorías que existen sobre la problemática

investigada, también incluye los trabajos e investigaciones que existen y antecedentes sobre lo que se investigó.

Los temas como perspectiva global de la ciberseguridad, riesgos de la ciberseguridad, soluciones en ciberseguridad, formación en ciberseguridad establecieron las bases para entender los pasos de la solución planteada en este proyecto, en la cual se enfatiza en los conocimientos de la seguridad de la información. Las etapas en la que se trabajó, apoyado en las bases conceptuales del marco teórico son las siguientes:

1. Definición de los detalles de los requerimientos necesarios del sistema, en conjunto con la empresa.
2. Continuando con la definición de la mejor forma de desarrollar la aplicación, de acuerdo a los requerimientos del sistema, mediante un diseño de alto y bajo nivel y Posteriormente se estableció una propuesta que determine los perfiles de conocimiento para cada colaborador.
3. Se continuó con el desarrollo del sistema prototipo (véase capítulo 5).
4. En este paso se determinó el proceso para establecer cursos de capacitación para cada participante.
5. Posteriormente se verificaron los requerimientos del sistema desarrollado, realizando pruebas de laboratorio.
6. Se validó el sistema, en un entorno real y se identificaron elementos factibles para la mejora.

3 Análisis del sistema

Dada la importancia del tema de la ciberseguridad, y la necesidad de personas capaces de capacitar o enseñar en esta área, el Tecnológico Nacional de México, a través del Instituto Tecnológico de Hermosillo ha emprendido acciones con miras a solventar, al menos en parte el problema planteado en este proyecto. Una de estas acciones ha sido la firma de un convenio de colaboración con una de las principales empresas especialistas en ciberseguridad en México, la cual ofrece cursos de capacitación y certificación de las principales casas certificadoras en el área a nivel mundial.

En esta etapa del proyecto se analizaron los datos necesarios para determinar cursos de acción en el desarrollo del sistema, obteniéndose información relevante que ayudó a definir la forma de trabajo de la empresa código verde para el establecimiento de rutas de capacitación.

3.1 Análisis del proceso de establecimientos de rutas de capacitación

Como se estableció en el planteamiento del problema, se enfatiza el deseo de automatizar los procesos de selección de las rutas de capacitación en ciberseguridad, los cuales están dirigidos a un grupo de usuarios en una organización o de forma individualizada. Se requería que el software recolecte los datos de los participantes y este detecte las necesidades de aprendizaje de los mismo, considerando sus deficiencias en temas de la ciberseguridad, finalizando con la oferta de un plan de capacitación.

Este software permitirá a los interesados agilizar, prever y planear la preparación de los diversos programas educativos en el área de la seguridad tecnológica, aunque depende en gran grado de la aceptación del usuario potencial, de que este acepte la propuesta que se le realiza.

3.1.1 Proceso de selección.

En esta sección se analiza la secuencia de pasos, en forma general, que se toman en cuenta para la determinación de cada propuesta educativa que se ofrece en el área de la seguridad de la información.

En el Diagrama 7 se observan los pasos para definir participantes, con el objetivo de identificar la necesidad de capacitación en el área de la ciberseguridad. En este paso se analiza una organización, en donde se evalúa las habilidades, responsabilidades y conocimientos del personal específico, al igual se analiza de forma ligera la tecnología que se utiliza en la misma empresa para conocer sus posibles deficiencias en el cuidado de la información que maneja y así tener una perspectiva más amplia al momento de definir rutas de capacitación. Según los resultados obtenidos se delibera, por un grupo de expertos, recomendando una ruta de capacitación para el personal de la organización.

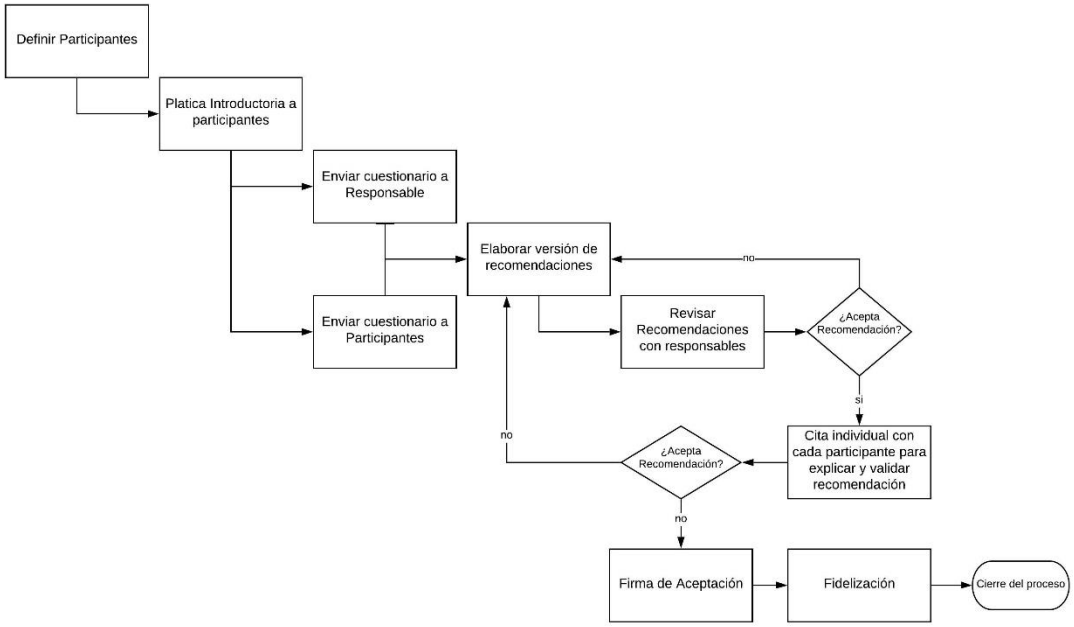

Diagrama 7. Proceso general de selección de rutas de capacitación en el área de la ciberseguridad.

La empresa especialista en ciberseguridad con la que se tiene convenio, efectúa sus exámenes de diagnóstico por medio de preguntas generales sobre temas de la seguridad de la información, continuando posteriormente con el análisis de las respuestas. Esta revisión es realizada por expertos del área, los cuales evalúan los conocimientos del individuo, con el fin de determinar el rol de trabajo adecuado a sus responsabilidades, además de cubrir sus intereses a corto plazo, siguiendo con el establecimiento de una o varias recomendaciones de rutas de capacitación en el área de la ciberseguridad.

Realizar el análisis de conocimientos que poseen diferentes individuos es un trabajo arduo, además de ser limitado a una cierta cantidad de preguntas y exámenes, ya que depende del tiempo disponible de los expertos (persona con experiencia, conocimientos y habilidades en alguna tarea o actividad) [16]. Al momento de la revisión y definición del curso de la capacitación creada dependerá en gran medida de la experiencia del evaluador del área o rol determinado.

Otra situación para definir participantes es cuando una organización interesada requiere de expertos capacitados en el área de la ciberseguridad, con tiempo completo en la empresa. En la que analicen los aspectos de seguridad de la información a todo momento. Un ejemplo sería una empresa desarrolladora de software, la cual debe tener varios expertos con diferentes especialidades en seguridad del software y su entorno, ya que estos deben tener un plan de calidad apropiado. El software deberá ser eficiente y seguro, que cumpla con los estándares internacionales, cubriendo las necesidades de los clientes, al mantener un buen plan de desarrollo seguro durante el ciclo de vida del software. Otro ejemplo serían las empresas financieras que requieren procesos seguros, software seguro, auditorías internas fuertes que garanticen la disponibilidad, confiabilidad e integridad de los datos, entre otros. Entonces en este tipo de organizaciones se necesita de un fuerte equipo de trabajo en el área del aseguramiento de la información, que corrijan cualquier problema que está o que pueda ocurrir.

El primer paso es importante para que los expertos en seguridad de la información, además de ser capacitadores, realicen el proceso en la evaluación de perfiles y roles necesarios para cubrir el déficit de conocimientos de ciberseguridad de los colaboradores. Aunque este paso por sí solo no define el proceso de capacitación, ya que depende también de la visión y motivación de los participantes.

En el segundo paso se realiza una reunión con los interesados para informar la situación en seguridad de la empresa y al mismo tiempo se conoce a los participantes del proceso, con lo cual se rompe el hielo, además se les explican los pasos a realizar en el proceso de selección de rutas de aprendizaje. Al responsable de la organización se le ofrece un informe detallado de los problemas con los que cuentan y sus repercusiones si no se resuelven. Si los interesados deciden solucionar las deficiencias de la empresa o desean resolver un probable problema a futuro, refiriéndose principalmente de las habilidades de las personas con respecto en la seguridad de la información; como tercer paso se envía un cuestionario online a responder a todos los participantes.

Con las respuestas obtenidas, estas son analizadas con el objetivo de definir las recomendaciones de capacitación para los participantes. Los cursos propuestos se mandan a revisión con el responsable, este da su punto de vista para asentir para una aceptación o rechazo. Si la propuesta es aceptada se cita a cada uno de los participantes, de manera individual, para explicar las recomendaciones y que las valide. Si estas son aceptadas se cierra el trato con la obtención de las firmas de aceptación, continuando el contrato legal, donde se especifican los derechos y obligaciones de cada una de las partes involucradas (contratante del servicio y del que lo ofrece).

3.1.2 Obtención de datos del colaborador

En este punto se explica la forma de recopilar los datos de los participantes, con el objetivo de proponer un plan de capacitación personalizado con base en las deficiencias de conocimiento, responsabilidades e intereses actuales o futuras de cada participante. No se olvide que lo que se busca es determinar los cursos de certificación que establezcan una buena calidad en la seguridad de la información en la empresa. Se menciona los pasos en forma enumerada para la obtención de información de los participantes:

1. **Solicitud de los datos generales.** A continuación, se enumeran las cuestiones que se solicitan:
    a) Nombre.
    b) Correo.
    c) Organización.
    d) Ubicación geográfica de la oficina.
    e) Comprensión del inglés.

2. **Responsabilidades actuales.** A continuación, se enumeran las cuestiones que se solicitan:
    a) Departamento de trabajo.
    b) Puesto actual.
    c) A que puesto se reporta.
    d) Principales Responsabilidades.
    e) Tiempo desempeñando el puesto actual.
    f) Puesto anterior.
    g) Tiempo en el puesto anterior.
    h) Perfil del puesto (básico, intermedió, avanzado, experto).

i) Principales responsabilidades en cuanto a seguridad informática en su organización.
j) Personas a su cargo.

3. **Intereses Profesionales.** A continuación, se enumeran las cuestiones que se solicitan:
   a) Áreas de interés. (Seleccionar solamente cuatro).
   b) Puesto en el que se visualiza de 3 a 5 años.
   c) Perfil en el que se visualiza (básico, avanzado, experto).

4. **Nivel Técnico**. A continuación, se enumeran las cuestiones que se solicitan:
   a) Identifica en su puesto actual, hacia donde es la inclinación principal de las actividades realizadas, determinando si son de tipo: **Técnico** o **administrativo,** aunque bien este punto se estable en un rango del 1 al 4 (véase Ilustración 46, Anexo). Este punto indica que se debe seleccionar un numero entre 1 a 4 máximo, indicando que mientras más cercano al 1 sea la selección del colaborador, el trabajo realizado es más técnico y en contra, mientras más cercano al 4, el trabajo realizado es más administrativo. Dependiendo del grado responsabilidad, facilita ofrecerles cursos no muy técnicos o no muy administrativos, dependiendo del nivel seleccionado, esto se valida en conjunto con la carrera que estudió. Ejemplo: si sus estudios son el área de las TI, y el colaborador selecciona un numero entre el 3 y 4, quiere decir que su responsabilidad es más administrativa, por lo que se le toma en cuenta para unas certificaciones más acorde a sus responsabilidades administrativas. Mientras, al contrario, si la selección es entre 1 y 2, quiere decir que las actividades son más técnicas.
   b) Nivel técnico de los participantes. Esta opción muestra varias tecnologías con la que el participante deberá responder si no las comprende o las utilizó alguna vez o las usa regularmente o si las domina totalmente.

5. **Estudios profesionales y experiencia laboral.** El objetivo es conocer el nivel de conocimiento de los participantes. A continuación, se enumeran las cuestiones que se solicitan:
    a) Estudios a nivel profesional y de posgrado.
    b) Áreas de trabajo en la que ha laborado y mencionar el tiempo de experiencia.
    c) Obtención de perfil de Linkedin o currículo vitae.

6. **Certificaciones y cursos.** A continuación, se enumeran las cuestiones que se solicitan:
    a) Cursos relacionados a seguridad informática.
    b) Con qué tipo de certificación cuenta el colaborador.

Cuestionario para el encargado, jefe de área o responsable de la empresa en el proceso de seguridad de la información. El objetivo de estos puntos es de obtener información para proponer un plan de capacitación para los colaboradores, basado en las necesidades de su departamento de trabajo y su organización. Se mencionan los pasos en forma enumerada para la obtención de información de los responsables:

1. **Datos generales**
    - Nombre.
    - Correo.
    - Nombre de la organización.
    - Ubicación.

2. **Motivos**

- Principal factor que está impulsando la Seguridad Informática en la organización.
- Metas concretas de Seguridad Informática que desean alcanzar.
- Periodo de tiempo en que quiere alcanzar sus metas en seguridad informática.

3. **Estructura organizacional**
   - Puesto actual.
   - Puesto al que reporta.
   - Estructura organizacional del área. Este le sirve al experto para determinar el equipo de seguridad, tomando en cuenta cada área.

4. **Visualización**
   - Cambios que visualiza en la estructura organizacional del departamento en los siguientes 3 a 5 años.
   - Cambios en responsabilidades que visualiza en los colaboradores que forman parte del alcance del plan de seguridad de la información, dentro de los planes de capacitación que se ofrecen.

3.1.3 Criterios basados en experiencia, responsabilidad y visión.

Los expertos en ciberseguridad que evalúan y participan en el proceso de selección, usan su criterio personal, evalúan el conocimiento, analizan responsabilidades y la visión de los responsables, como también la de los participantes o colaboradores, con el objetivo de ofrecer la mejor propuesta de capacitación. Se habla entonces de definir lo más aceptable posible un curso de capacitación, tomando en cuenta los siguientes puntos:

1. **Responsabilidades actuales.**
   - Puesto y departamento.

- Principales responsabilidades.
- Validar responsabilidades vs puesto. Se les pregunta a los participantes si sus responsabilidades abarcan las que se tienen mapeadas (establecida en el manual de operación de la empresa) en su puesto o si tienen otras actividades.
- Identificar nivel operativo vs gerencial.
- Identificar nivel técnico vs administrativo.

2. **Formación académica del participante.**
    - Certificaciones con las que cuenta el participante.
    - Cursos realizados.
    - Título universitario.
    - Título de Post-grados.
    - Obtención de currículo, en un formato especifico, puede ser Linkedin.

3. **Áreas de experiencia**
    - Obtención de puestos anteriores y tiempos.
    - Áreas de experiencia.

4. **Intereses Profesionales**
    - Obtener áreas de interés.
    - En qué puesto se visualiza en 2 a 5 años.

5. **Visión del responsable del área.**
    a. Que motiva la realización del ejercicio.
    b. Obtención del organigrama del área.
    c. Necesidades del departamento.
    d. Necesidades de la empresa.

e. Cambios a corto y mediano plazo.

3.1.4 Criterios para recomendación de un plan de capacitación.

Las realizaciones de las versiones, con respecto a las recomendaciones de la planeación las rutas de aprendizaje, es un proceso deductivo, realizado por un conjunto de expertos en el área de las tecnologías de información (TI). Estos expertos analizan la información recolectada y usando su criterio, el cual está basado en la experiencia, conocimientos, responsabilidades y la visión de los participantes y el/los responsables. Estos expertos establecen las propuestas, tomando en cuenta estos puntos:

1. Establecer un perfil común de conocimiento de todos los participantes que pertenecen a una organización. Es importante recalcar la obtención de la formación académica y de la evaluación de los conocimientos de los participantes. Aunque la evaluación especializada se realiza solo cuando la problemática en la empresa lo amerita.
2. Desarrollar especializaciones con base en roles de trabajo de los participantes. Se toma en cuenta los puestos de trabajo, responsabilidades y visión.
3. Formar un equipo de seguridad de la información completo. En ocasiones se ocupan varios expertos en un área específica para la seguridad de la información. Por ejemplo, en área de desarrollo de software de necesita mínimo un Risk Management (RSK), un Software Development (DEV), Systems Architecture (ARC), Technology R&D (TRD), Systems Requirements Planning (SRP), Test and Evaluation (TST), Systems Development (SYS).
4. Mantener cierto nivel de redundancia. Tomar en cuenta los cambios constantes en la empresa, ya que un participante que se especializó puede que se cambie de área o que renuncie a su puesto de trabajo, por lo que se tiene que tener personal capacitado que tome su lugar.
5. Complementar roles y funciones:

a. Con base en el tamaño, se determina la dependencia de la TI con la empresa. Depende de si la empresa es pequeña o mediana o grande se definen los grupos de seguridad.
b. Definir puestos mínimos recomendados.

3.2 Determinación de los requerimientos generales del Sistema

Los requerimientos de un sistema describen los servicios que ha de ofrecer el sistema y las restricciones asociadas a su funcionamiento. En este subtema se establecieron los requerimientos de manera general, con lo que posteriormente se estableció la arquitectura del software

Lo que el cliente solicita que el sistema realice:

1. Almacenar información general de los participantes.
2. Almacenar responsabilidades de los participantes.
3. Almacenar intereses de los participantes.
4. Almacenar educación de los participantes.
5. Almacenar experiencia de los participantes.
6. Almacenar visión a futuro de los participantes.
7. Almacenar estudios profesionales y de posgrado (técnica o administrativa).
8. Ligar palabras claves de cada sección mencionada anteriormente.
9. Determinar nivel de conocimientos de los participantes para recomendar cada curso.
10. Filtrar todas las recomendaciones realizadas por los expertos en ciberseguridad por las certificaciones vigentes.
11. Ofrecer varias recomendaciones opcionales para cada participante.
12. Ofrecer varias recomendaciones opcionales por grupo de seguridad.
13. Elaborar un conjunto de certificación recomendados para cada participante.
14. Obtener retroalimentación de los interesados, para ofrecer una nueva lista de recomendaciones. (Este punto solo si el usuario no queda conforme con la recomendación sugerida).

El cliente definió las necesidades que se ocupan para determinar las recomendaciones y para que el proceso de selección sea el adecuado a lo que se ocupa para el sistema que se deseaba desarrollar:

- Recolectar información:
  - Responsabilidades: Puestos y cuanto le reportan.
  - Intereses de la organización e individuo.
  - Educación: Educación profesional y de posgrado, certificaciones, cursos.
  - Experiencia del usuario.
  - Visión a futuro del usuario.
- Identificar que la educación sea de una carrera relacionada a la tecnología de la información (TI).
- El sistema recomendará certificaciones de conocimiento general, si el colaborador no comprende las TI.
- De manera automática deberá detectar datos claves, para ligarlos a la necesidad de capacitación. (Detectar el nivel de conocimiento)
- Ofrecer una lista de certificaciones por valoración, de acuerdo a la necesidad de conocimientos.
- Criterios para recomendar cada curso:
  - Primero lista de recomendación deberá ser de acuerdo a las responsabilidades actuales del personal.
  - La segunda lista de recomendación deberá ser de acuerdo a la visión a futuro.
  - La tercera lista una combinación de acuerdo de las dos primeras listas.
- Filtrar todas las recomendaciones por las certificaciones vigentes y seleccionar las más adecuadas.

3.3 Ejemplo de proceso de selección de rutas de capacitación

En este subtema se analizará un ejemplo del proceso de selección de rutas de capacitación para un colaborador, se enumera los pasos como sigue:

A. Se envía cuestionario a llenar al colaborador.

B. Se ordena la información recibida (véase tabla 7) y se analizan los datos obtenidos del cuestionario para establecer el rol de trabajo y las rutas de capacitación (véase tabla 8).

Tabla 7. Ejemplo de respuestas al cuestionario del proceso de selección, realizado por un colaborador.

Resultado de la Evaluación	**Datos del colaborador**
¿Cuál es tu puesto?	Information Security Sr. Manager
En tu puesto actual, tus actividades son principalmente de tipo (Técnico vs administrativo)	3
¿Cuánto tiempo tienes desempeñando este puesto?	0.5 años
¿Cuál era tu puesto anterior?	Gerente Corporativo de Auditoría y Procesos
¿Cuánto tiempo estuviste en tu puesto anterior?	1 años
¿Cuáles son tus principales responsabilidades en cuanto a seguridad informática en tu organización? Selecciona máximo 4 opciones.	Gestionar la seguridad en los proyectos, Garantizar el cumplimiento legal y contractual, Auditar políticas de seguridad, Auditar controles de seguridad/TI
¿Cuántas personas tienes a tu cargo?	8
¿Cuáles son tus áreas de interés? Selecciona máximo 4 opciones.	Pruebas de seguridad a la infraestructura, Forense digital, Auditoría controles de seguridad / TI, Gestión de riesgos de TI
¿En qué puesto te visualizas de 3 a 5 años?	Auditor Global de Seguridad de Información
¿Cuentas con alguna de estas certificaciones? (seleccione todas las que aplique)	Ninguna
Enumera tus principales responsabilidades	Gestionar al equipo de Especialistas de Seguridad de Información para el cumplimiento de las políticas internas de Teleperformance, así como dar seguimiento a los incidentes de seguridad detectados en los sites y atención a las auditorías internas y externas de los más de 40 clientes del mercado Doméstico.
¿Puedes leer y comprender materiales técnicos en Inglés?	Sí
¿Cuál es tu nivel de conocimiento sobre las siguientes tecnologías? [Comandos básicos de Linux / Unix]	No lo conozco
¿Cuál es tu nivel de conocimiento sobre las siguientes tecnologías? [Nmap]	No lo conozco

¿Cuál es tu nivel de conocimiento sobre las siguientes tecnologías? [Switches de red]	Lo utilicé alguna vez
¿Cuál es tu nivel de conocimiento sobre las siguientes tecnologías? [Ruteadores de red]	Lo utilicé alguna vez
¿Cuál es tu nivel de conocimiento sobre las siguientes tecnologías? [Firewalls]	Lo utilicé alguna vez
¿Cuál es tu nivel de conocimiento sobre las siguientes tecnologías? [Modelo OSI de ISO]	Lo utilizo regularmente
¿Cuál es tu nivel de conocimiento sobre las siguientes tecnologías? [Conceptos de seguridad como: confidencialidad, integridad y disponibilidad]	Lo domino
¿Cuál es tu nivel de conocimiento sobre las siguientes tecnologías? [IPs y puertos]	Lo utilicé alguna vez
¿Cuál es tu nivel de conocimiento sobre las siguientes tecnologías? [Parches de seguridad]	Lo utilizo regularmente
¿Cuál es tu nivel de conocimiento sobre las siguientes tecnologías? [SIEM, IDS, IPS]	Lo utilicé alguna vez
¿Cuál es tu nivel de conocimiento sobre las siguientes tecnologías? [Burp, ZAP]	No lo conozco
¿Cuál es tu nivel de conocimiento sobre las siguientes tecnologías? [OWASP top 10]	Lo utilicé alguna vez
¿Cuál es tu nivel de conocimiento sobre las siguientes tecnologías? [SQLmap]	No lo conozco
¿Cuál es tu nivel de conocimiento sobre las siguientes tecnologías? [Wireshark]	Lo utilicé alguna vez
¿Cuál es tu nivel de conocimiento sobre las siguientes tecnologías? [Ping]	Lo utilizo regularmente
¿Cuál es tu nivel de conocimiento sobre las siguientes tecnologías? [Secure Software Development Lifecycle]	Lo utilizo regularmente
¿Cuál es tu nivel de conocimiento sobre las siguientes tecnologías? [Gestión de Riesgos de TI]	Lo utilizo regularmente
¿Qué cursos relacionados a seguridad informática has tomado?	Ninguno
¿Qué estudios a nivel profesional y de posgrado tienes?	Ninguno
¿En qué áreas laborales tienes experiencia?	Ninguno

C. Se establecen las recomendaciones de rutas de aprendizaje.

Tabla 8. Rutas de aprendizaje para el IS Manager Senior.

Ruta de aprendizaje			
Rol de trabajo: Senior Information systems manager			
Opción	**Certificación 1**	**Certificación 2**	**Certificación 3**
1	CISSP	CRISC	CISA
2	CISSP	CRISC	CEH
3	CISSP	CRISC	CAP

Diagrama 8. Representación gráfica de la ruta de aprendizaje

En la Tabla 8 y el Diagrama 8, se puede observar las rutas de aprendizaje para el rol de trabajo Information Systems Manager Senior. En la Tabla 8, la columna de "Opción" indican la cantidad de rutas de aprendizaje y en la fila indica el seguimiento que debe tener cada certificación. En las rutas de capacitación se muestran tres opciones viables y cada una está compuesta por certificaciones que en conjunto cumplen con el objetivo de aprendizaje necesario para el colaborador. Es importante detectar cuál será el primer certificado

(Certificación 1) a realizar, posteriormente el segundo (Certificación 2) y terminando con la tercera (Certificación 3), esto representan las filas de cada opción. Si diferentes certificados se encuentran en la misma columna se considera que tienen jerarquías similares con respecto al rol de trabajo y conocimientos del colaborador, como se puede observar en la Tabla 7, certificado 3, en donde existen a lo largo de la columna, tres certificaciones diferentes con la misma jerarquía o nivel. Esto quiere decir que cualquiera de las tres rutas cumple con el rol de trabajo planteado y los interese del colaborador. Recordar que a última instancia el que decide qué ruta de aprendizaje es la que más le interesa y le beneficia es el colaborador.

D. Entrega de resumen ejecutivo a los colaboradores. Este documento informa un resumen general de las respuestas de los colaboradores y muestra los resultados de las evaluaciones. Como retroalimentación a los colaboradores, este informe detalla las características de cada certificación recomendada

3.4 Conclusión del análisis del proyecto

Al momento de realizado el análisis del sistema se contaba con ocho colaboradores que participaron en el llenado del cuestionario, por lo que solo se contaba con ocho diferentes tablas de información, a los cuales se les estableció rutas de capacitación individual a cada uno (véase la Tabla 9, pág. 71). Concluyéndose que son pocos los datos para desarrollar un sistema inteligente utilizando un algoritmo de aprendizaje automático por lo que se planteó que el proceso general de desarrollo de la solución se dividiera en cinco etapas, donde primero se identifican las casas certificadoras en ciberseguridad, se definen los roles de trabajo, se establece el formulario para obtener datos de los colaboradores y definición de la escala en la que se evaluarán los datos. Continuando con la segunda fase, en donde se crea un formulario web usando el cuestionario de la empresa código verde, con el objetivo de facilitar la obtención de datos. La tercera fase es diseñar una base de datos que contendrá toda la información recabada por los participantes por medio del formulario web, además de

las evaluaciones realizadas por los expertos en ciberseguridad. En la cuarta fase se determinó desarrollar una aplicación web como apoyo a la determinación de rutas de capacitación y almacenamiento de datos. Como última fase, la quinta, se estableció una solución que facilite la determinación de los perfiles de conocimiento y de las rutas de capacitación. En el Diagrama 9 se muestra la información de manera resumida y estructurada.

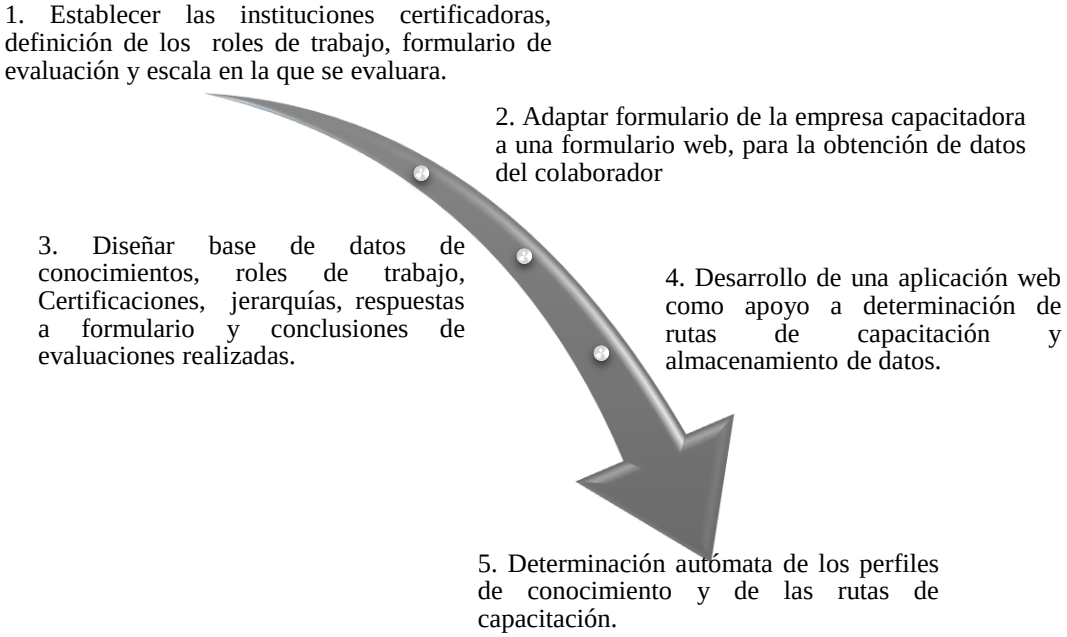

Diagrama 9. Esquema general que especifica las fases de solución del proyecto.

Con el esquema general realizado se platea determinar una funcionalidad real, eficaz y congruente para el desarrollo del proyecto y de la aplicación web, la cual debe ser segura, con una interfaz de usuario responsivo, fácil de usar y que contenga todos los módulos necesarios para la obtención y almacenamiento de datos de manera segura, además de apoyar en la determinación de rutas de aprendizaje en seguridad de la información.

Recapitulando al respecto de la recopilación de evaluaciones realizadas por los expertos en ciberseguridad, se obtuvieron cuatro roles de trabajo diferentes, de las cuales se establecieron 18 rutas de aprendizaje diferentes. Se contaba con ocho colaboradores con un rol de trabajo, a los cuales se establecieron tres rutas de aprendizaje recomendadas a cada uno. Se consideró que eran pocos datos, por lo que en este punto no es conveniente el uso de un algoritmo de aprendizaje automático para definir niveles de conocimiento, tampoco certificaciones y mucho menos rutas de capacitación. Así que la función del sistema a desarrollar en su primera etapa (finalidad principal de este proyecto), es de apoyo para la recopilación de información de los candidatos y facilitar la evaluación por parte de los expertos o evaluadores. Las respuestas de los candidatos son almacenadas en una base de datos, al igual que las evaluaciones realizadas por los expertos. Para obtener resultados tangibles se requiere la participación de expertos para:

1. La evaluación del conocimiento actual de los participantes.
2. Relacionar los resultados de la evaluación con un perfil que cumpla con las necesidades e intereses a futuro del participante, con respecto a un puesto de trabajo.
3. Determinación de las mejores rutas de capacitación, tomando en cuenta los dos puntos anteriores.

4 Arquitectura del software

Par entender esta sección es importante saber qué es y para qué sirve la arquitectura del software. De acuerdo al Software Engineering Institute (SEI), la Arquitectura de Software se refiere a “las estructuras de un sistema, compuestas de elementos con propiedades visibles de forma externa y las relaciones que existen entre ellos” [35]. Más allá de los algoritmos y estructuras de datos de la computación; el diseño y especificación de la estructura global del sistema es un nuevo tipo de especificación a tomar en cuenta. Para entender mejor, un ejemplo clásico son los planos de una construcción de un edificio, en el cual se especifican cada una de las partes que incluirá e indican la estructura, funcionamiento e interacción entre las partes de cada una. Cada parte se desarrolla en un plano independiente, pero también existe un plano más genérico o abstracto del proyecto en donde se especifica la estructura completa, es aquí donde se plasma todo el conjunto en uno solo, para después desglosarlo en partes específicas y bien definidas, con lo que se basará el equipo de producción para al desarrollo del proyecto planteado.

4.1 Contextualización del proyecto

Para la realización de la arquitectura del sistema, con anterioridad, se analizó y se determinó la metodología de trabajo utilizada por la empresa capacitadora para establecer las certificaciones que ofrece a sus clientes, como la ruta de aprendizaje. Realizar esto de manera manual consume mucho tiempo y limita el alcance de la empresa en términos de la cantidad de personas que puede atender. Para mejorar el rendimiento de selección de las rutas y certificaciones, en este proceso se adaptó y desarrolló una aplicación web, con lo que se espera que, con la automatización de varios procesos, se pueda incrementar el alcance de la empresa. En este sentido, la principal aportación de la empresa al proyecto fue su experiencia.

En el contexto general del software que se desarrolló, garantiza la seguridad de los datos, como también administra las autorizaciones para ingresar al sistema en los diferentes módulos, dependiendo de los permisos de los usuarios; se puede implementar en el sistema operativo Windows y Linux (véase Diagrama 10). Los usuarios que ingresen a la aplicación lo podrán hacer por medio de un portal web, para hacer uso de las diferentes funciones del mismo (véase Diagrama 11). El sistema web es adaptable tanto para navegadores de equipos móviles como para equipos de escritorio. Los siguientes diagramas muestran los componentes generales del sistema:

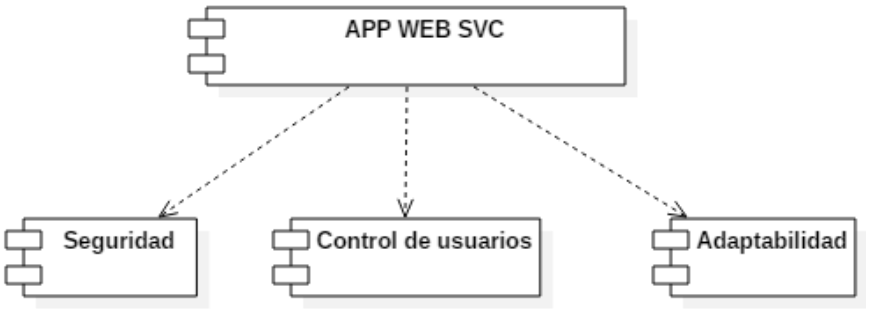

Diagrama 10. Contexto abstracto de la arquitectura del sistema

Diagrama 11. Comunicación entre el servidor y el equipo cliente es bidireccional

Los componentes del equipo servidor son los mostrados en el Diagrama 12:

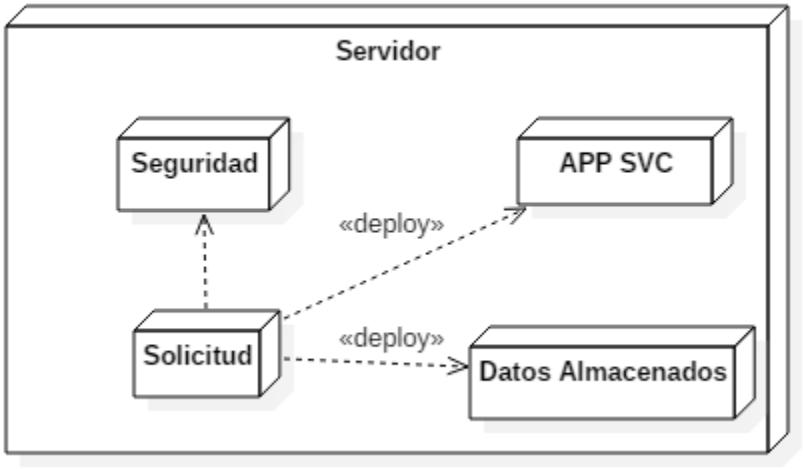

Diagrama 12. Componentes del servidor

Los componentes que se procesarán en el equipo cliente se presentan en el Diagrama 13:

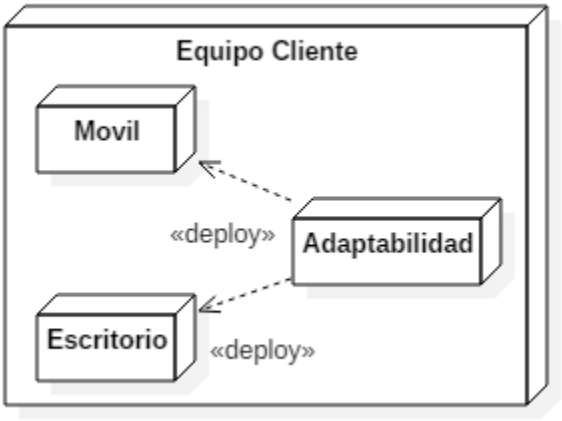

Diagrama 13. Componentes que se procesarán en el equipo cliente

4.2 Actores del sistema

Existen tres tipos de usuarios que se tomaron en cuenta para la realización del sistema, los cuales tienen diferentes permisos, dentro del mismo:

1. Colaborador. Profesional con interés de obtener conocimientos de algún rol de trabajo en el área de la seguridad de la información. Este usuario contesta cierto número de preguntas, para que el experto las analice y defina las mejores rutas de aprendizaje. El único permiso en el sistema es la de loguearse para contestar el formulario y enviar respuestas. (Véase Diagrama 14).

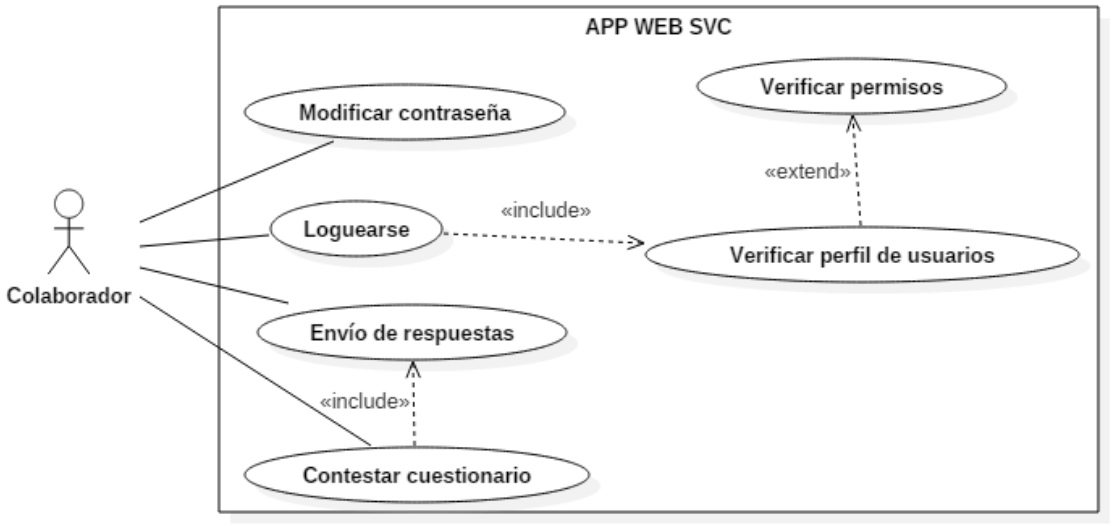

Diagrama 14. Caso de uso del usuario colaborador

2. Experto. Usuario experto en el área de la ciberseguridad, quien realizará la evaluación de los conocimientos de los colaboradores. Los principales permisos de este son:

    1) Vista de usuarios
    2) Crear usuario/s de tipo colaborador.
    3) Modificar usuario/s tipo colaborador.
    4) Eliminar usuario/s tipo colaborador.
    5) Importar usuarios desde un archivo CSV
    6) Crear una evaluación.
    7) Modificar una evaluación.
    8) Eliminar una evaluación.
    9) Vista de reportes por cada evaluador.
    10) Vista a reportes general de los resultados de las evaluaciones.
    11) Exportar resultados de las evaluaciones en formato PDF de los usuarios.
    12) Exportar resultados de las evaluaciones en formato CSV de los usuarios.
    13) Exportar datos de los formularios realizados por los colaboradores.
    14) Vista de certificaciones actualmente disponibles.
    15) Vista de los elementos que comprenden el framework NICE (roles de trabajo, áreas de especialidad, categorías).
    16) Agregar, editar y eliminar algún elemento del framework NICE.
    17) Enviar correo.

En el Diagrama 15 se muestra el diagrama de caso de uso del usuario experto.

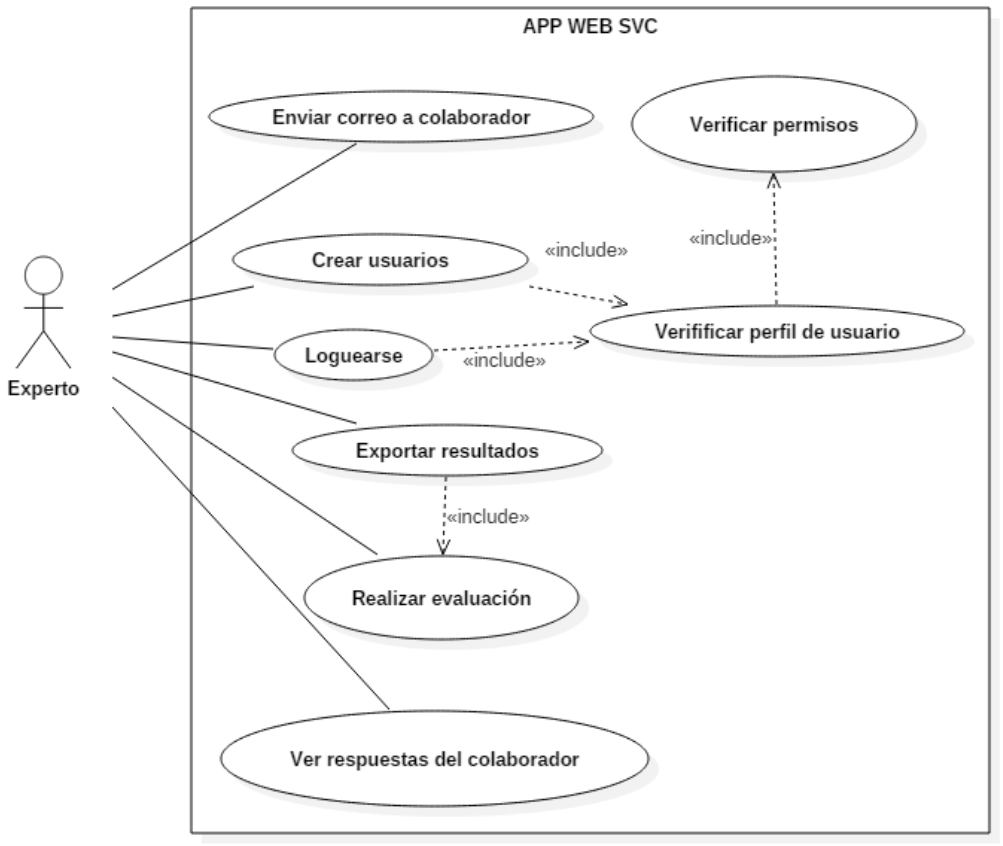

Diagrama 15. Caso de uso del usuario experto.

3. Admin (administrador del sistema). Usuario con todos los permisos del colaborador y experto, además de crear, eliminar y modificar usuario experto. (Véase Diagrama 16).

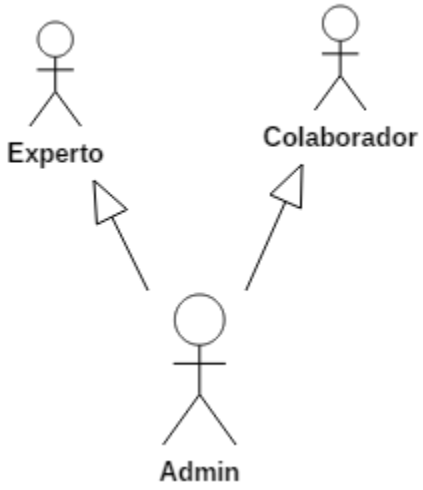

Diagrama 16. Caso de uso del usuario admin.

4.2.1 El usuario colaborador y el sistema de evaluación de conocimientos (SVC)

Por parte del colaborador, este llena un cuestionario, ya previamente creado por la empresa especialista (Código Verde). Estas preguntas se representarán en el sistema por medio de un formulario exclusivo para los colaboradores. El formulario que contesta el colaborador está dividido en las siguientes áreas de recolección de información: (1) datos generales, (2) responsabilidades actuales, (3) intereses profesionales, (4) nivel técnico, (5) formación académica, (6) área de experiencia. Al terminar de responder el formulario el colaborador confirma la finalización por medio de un botón de tipo submit, el cual realiza el proceso de envió de las respuestas para su revisión. Después de esto el colaborador no podrá modificar sus respuestas, pero todavía puede ingresar al sistema, mostrándose una pantalla de finalización y resultados de la evaluación (véase Diagrama 17). El único que tiene

autorización de activar el formulario para que el colaborador lo realice de nuevo es el usuario experto. Este mismo tiene la autorización de desactivar al usuario colaborador para que este no pueda volver a entrar al sistema.

La aplicación tiene la opción de enviar correos electrónicos a los colaboradores con el objetivo de entregar un enlace (para crear por primera vez la contraseña) y el username, con el cual entrarán al cuestionario del sistema de evaluación de conocimientos (véase Diagrama 18). Por seguridad la contraseña no se le proporciona al colaborador en el correo recibido, para ello utiliza un enlace proporcionado, el cual lo redirigiré hacia un sitio web, donde por primera y única vez se teclea una contraseña con una longitud mínima de 20 letras alfanuméricas, para uso propio. La contraseña se guarda en la base de dato de forma encriptada.

En el Diagrama 17 se muestran las actividades que realiza el colaborador (participante) en el sistema, de manera secuencial.

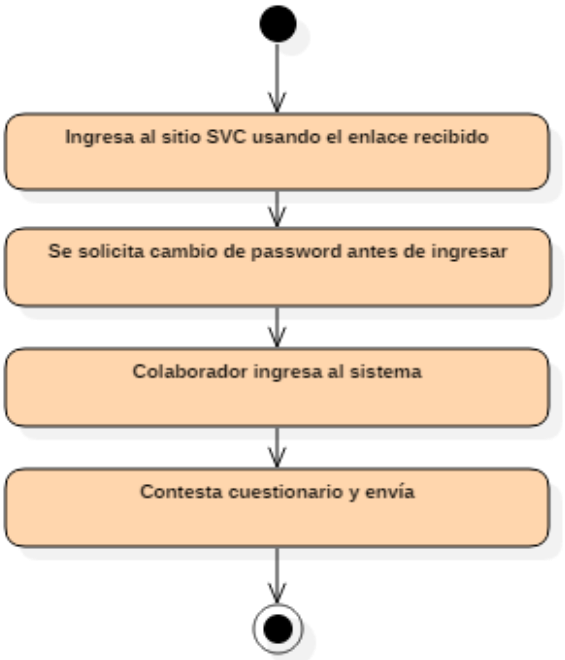

Diagrama 17. Actividades que realiza el colaborador en el sistema.

4.2.2 El usuario experto y el sistema de evaluación de conocimientos (SVC)

En esta sección se muestra el nombre del colaborador, un input para ingresar el rol del puesto de trabajo a capacitarse, opciones para establecer una escala del conocimiento del colaborador antes de las certificaciones. También se establece una escala, la cual se obtiene después de realizar las certificaciones. por ejemplo: básico, intermedio, avanzado, experto. Ya establecidas las bases, anteriormente mencionadas, se determinan las mejores rutas de certificaciones, considerando el análisis obtenido de las respuestas de los colaboradores. (Véase Ilustración 2. Ejemplo de bosquejo en la sección de evaluación.)

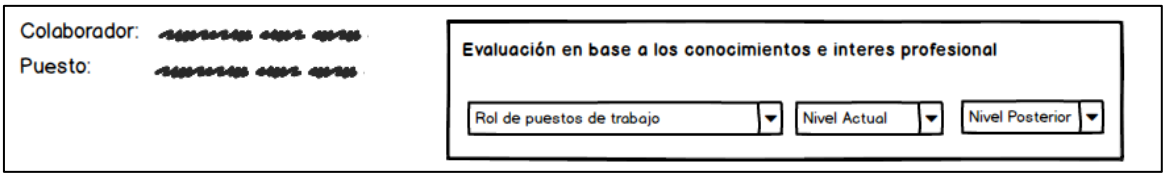

Ilustración 2. Ejemplo de bosquejo en la sección de evaluación.

El sistema consta de una sección de evaluación en donde los evaluadores observan un informe de las respuestas de los colaboradores, esta es cómoda y fácil de analizar con el objetivo de realizar el análisis de los conocimientos e intereses del colaborador (Véase Ilustración 3).

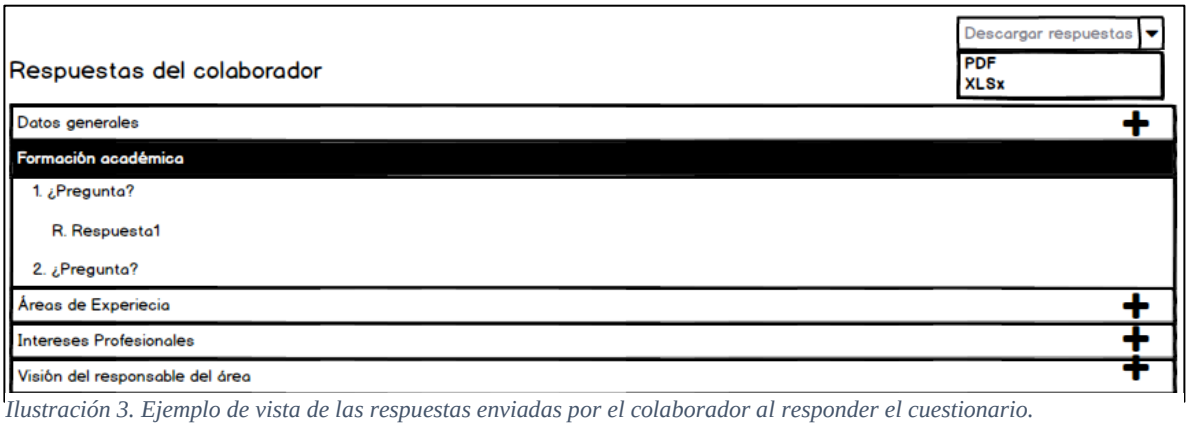

Ilustración 3. Ejemplo de vista de las respuestas enviadas por el colaborador al responder el cuestionario.

El software ofrece una manera fácil de referenciar las certificaciones al momento de seleccionar rutas de aprendizaje (véase Ilustración 4). El número máximo de rutas de aprendizaje son tres y por opción solo se pueden agregar tres certificaciones (Tabla 8, página 54).

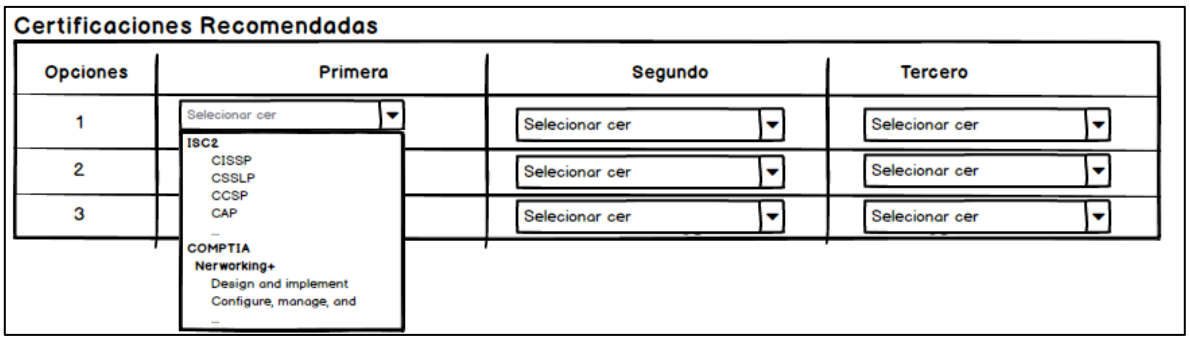

Ilustración 4. Ejemplo de selección de ruta de aprendizaje

El sistema ofrece la opción de seleccionar reporte individual por usuario y por conjunto de usuarios. En estos reportes se muestra el nombre del usuario, rol de trabajo que se le estableció y certificaciones recomendadas. Cada reporte de las rutas de capacitación es claro, tanto para los usuarios como para los expertos evaluadores. No se incluye respuesta de los colaboradores, en este caso se considera un reporte por separado por usuario, con el objetivo de exportar (véase Tabla 8 y Diagrama 8, página 54). En la siguiente Tabla 9 se muestra un

ejemplo de Reporte general de las evaluaciones obtenidas de un grupo de colaboradores de una sola organización:

Tabla 9. Reporte general de las evaluaciones obtenidas de un grupo de colaboradores de una sola organización.

Rol	Participante	Opción	Certificación 1	Certificación 2	Certificación 3
VP IS	----------	**1**	CCISO	CRISC	CISSP
		2	CCISO	CRISC	CISM
IS Manager Sr	----------	**1**	CISA	CRISC	CISSP
		2	CISA	Security+	CISSP
IS Manager Sr	----------	**1**	CISSP	CRISC	CISA
		2	CISSP	CRISC	CEH
		3	CISSP	CRISC	CAP
IS Manager	----------	**1**	CISSP	CISA	CRISC
		2	CISSP	Network+	Security+
IS Manager	----------	**1**	CISSP	CISA	CSSLP
		2	CISSP	CISA	CRISC
		3	CISSP	CISA	CEH
IS Manager	----------	**1**	CISSP	CRISC	CEH
		2	CISSP	CRISC	CISA
IS Coordinator	----------	**1**	CISA	CEH	ECSA
		2	CISA	CEH	CRISC
IS Manager	----------	**1**	CISSP	CISA	CRISC
		2	CISSP	CISA	CEH

El sistema tiene almacenados los roles de trabajo, conocimientos, tareas y habilidades establecidas en el marco de referencia NICE. Además, permite agregar nuevos roles de trabajo, los cuales queda a libertad de los expertos.

Una de las funciones principales del experto y del sistema de evaluación es la de dar de alta a los usuarios que responderán el formulario del colaborador. Posteriormente, ya que estos estén dados de alta, el experto debe enviar un correo a los colaboradores con su usuario y un enlace para crear su contraseña. (Véase Diagrama 18. Actividades iniciales del experto evaluador)

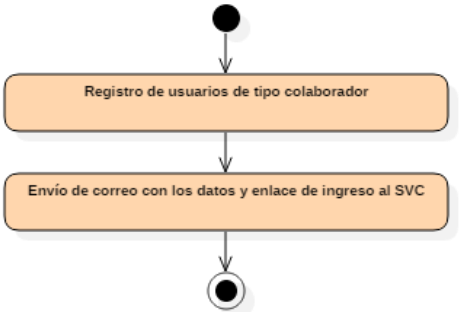

Diagrama 18. Actividades iniciales del experto evaluador

En general el trabajo principal realizado por el experto es el siguiente (véase Diagrama 19. Actividades del experto evaluador después de recibir datos por parte del colaborador.):

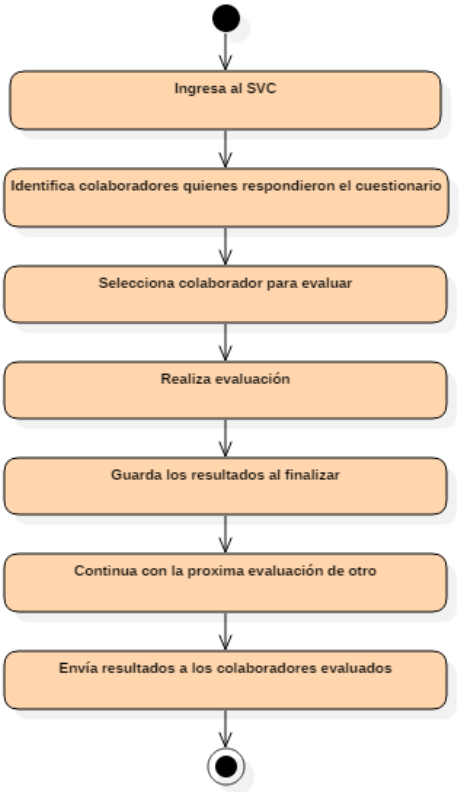

Diagrama 19. Actividades del experto evaluador después de recibir datos por parte del colaborador.

Nota: Para más información del proceso del experto y del colaborador véase el tema 4.2.3.

Un dato importante, no se almacenan permanentemente datos personales de los usuarios que los identifique, como: nombre, apellido, región, país, correo, username, password. Para el caso de futuras investigaciones, solo se almacena de forma permanente la información que no comprometa al participante, como los resultados obtenidos de la evaluación y respuestas realizadas en el cuestionario, sin contar datos generales. Por seguridad el colaborador no cargará ningún tipo de archivo en el cuestionario proporcionado. Como primera opción de solución se establece un solo modo de eliminación de datos personales y como segunda opción se crea una base de datos para respaldar. En cualquiera de las dos opciones se remplaza la referencia del colaborador por uno genérico sin los datos de identificación personal.

4.2.3 Diagramas generales arquitectónicos que expresan el negocio del sistema.

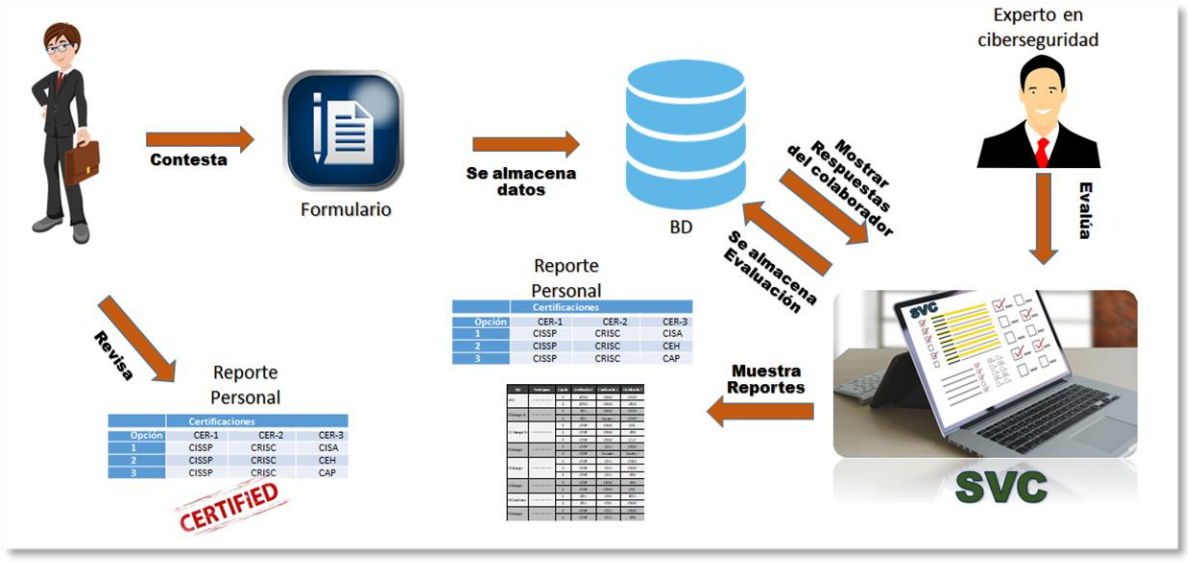

Ilustración 5. Flujo del proceso de negocio del sistema a desarrollar.

En la Ilustración 5 se observa el flujo del proceso de negocio del sistema, empezando con la contestación del cuestionario por parte del colaborador, hasta finalizar en la obtención de un reporte con las rutas de aprendizaje recomendados, cuyo trabajo del sistema y funciones de los actores y componentes del sistema se resumen en estos pasos: Antes de contestar el cuestionario el experto deberá: (1) enviar los datos de ingreso al sistema, incluyendo un enlace para que el colaborador cree una contraseña (véase Diagrama 20). (2) El colaborador contesta el formulario y envía por medio de un botón submit para que estas respuestas se almacenen en la base de datos (véase Diagrama 21). (3) El experto analiza las respuestas recibidas, evalúa y determina las rutas de capacitación recomendadas, al finalizar realiza el submit para que esta evaluación se almacene en la base de datos (véase Diagrama 22). (4) El sistema crea reportes de las evaluaciones, las cuales pueden ser observadas por el experto evaluador en cualquier momento que lo necesite. El experto debe notificar a los colaboradores las rutas de aprendizaje obtenida por medio de un archivo PDF y también puede revisar sus evaluaciones en el mismo sistema. (5) El colaborador recibe propuesta de certificados recomendados, de acuerdo a sus intereses y necesidades. En los siguientes diagramas se muestran de forma gráfica, cada uno de los procesos mencionados.

En el Diagrama 20 se muestra, en forma general, la secuencia de la creación de usuarios y el proceso de informar a los colaboradores de los datos para ingresar al sistema.

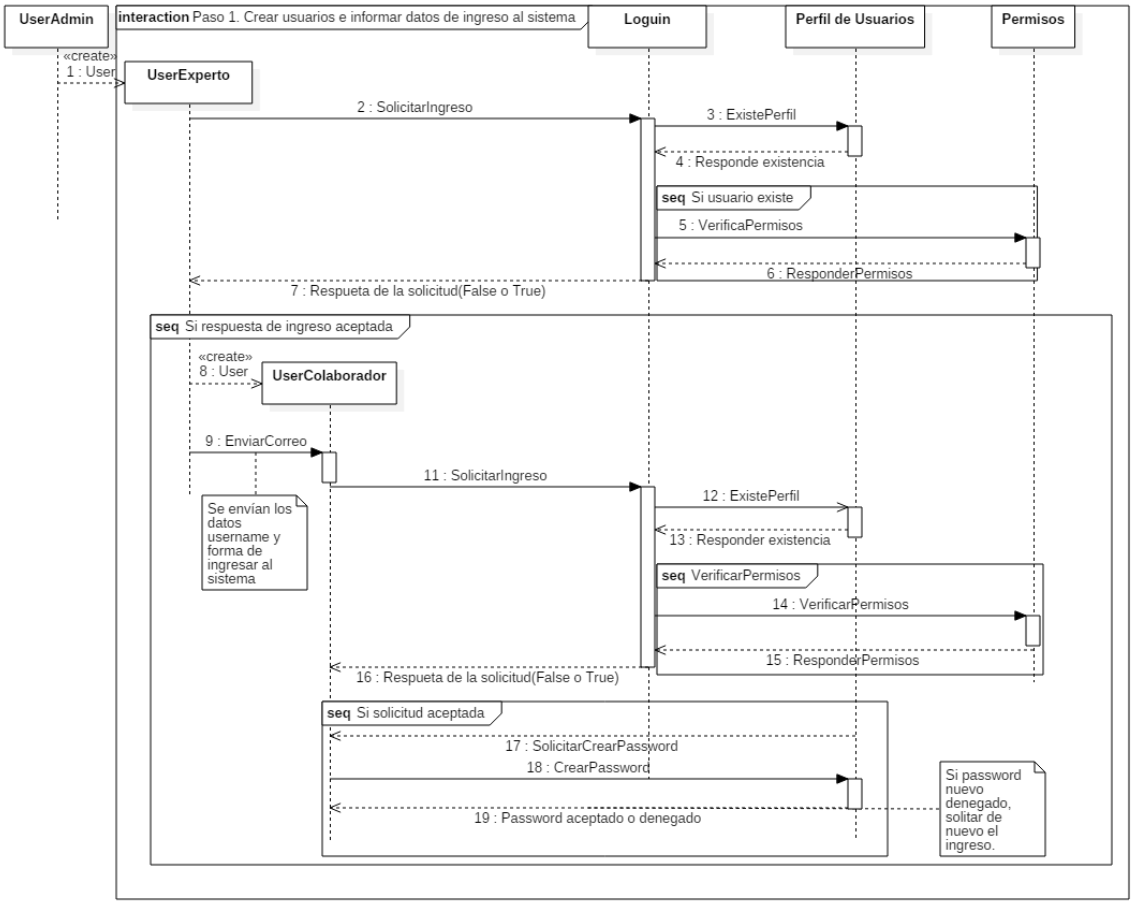

Diagrama 20. Diagrama secuencial de la creación de usuarios y procedimiento de ingreso al sistema de validación de competencias (SVC).

En el Diagrama 21 se muestra el proceso secuencial del colaborador para responder el formulario.

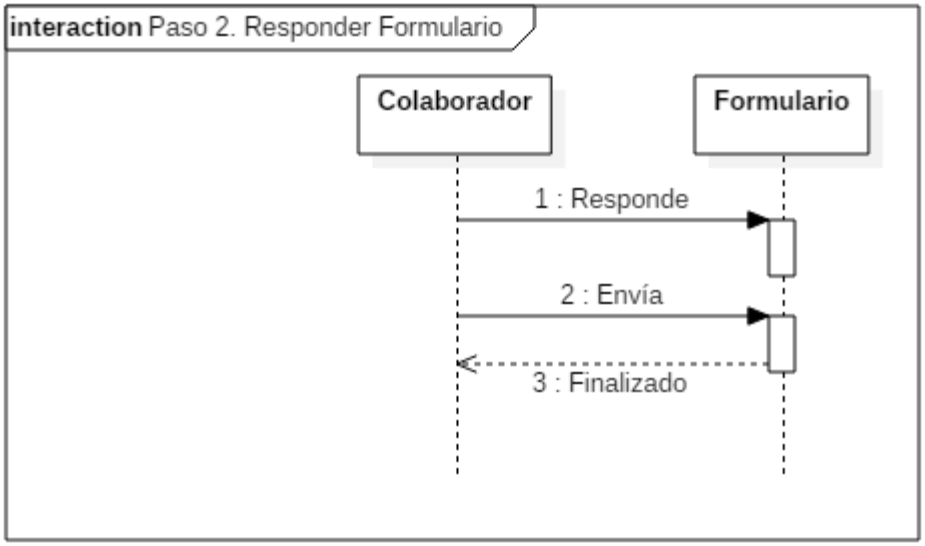

Diagrama 21. Diagrama secuencial del proceso de responder el formulario y enviar, por parte del colaborador.

En el siguiente Diagrama 22 se muestra la secuencia de paso del proceso de evaluación por parte de los expertos evaluadores.

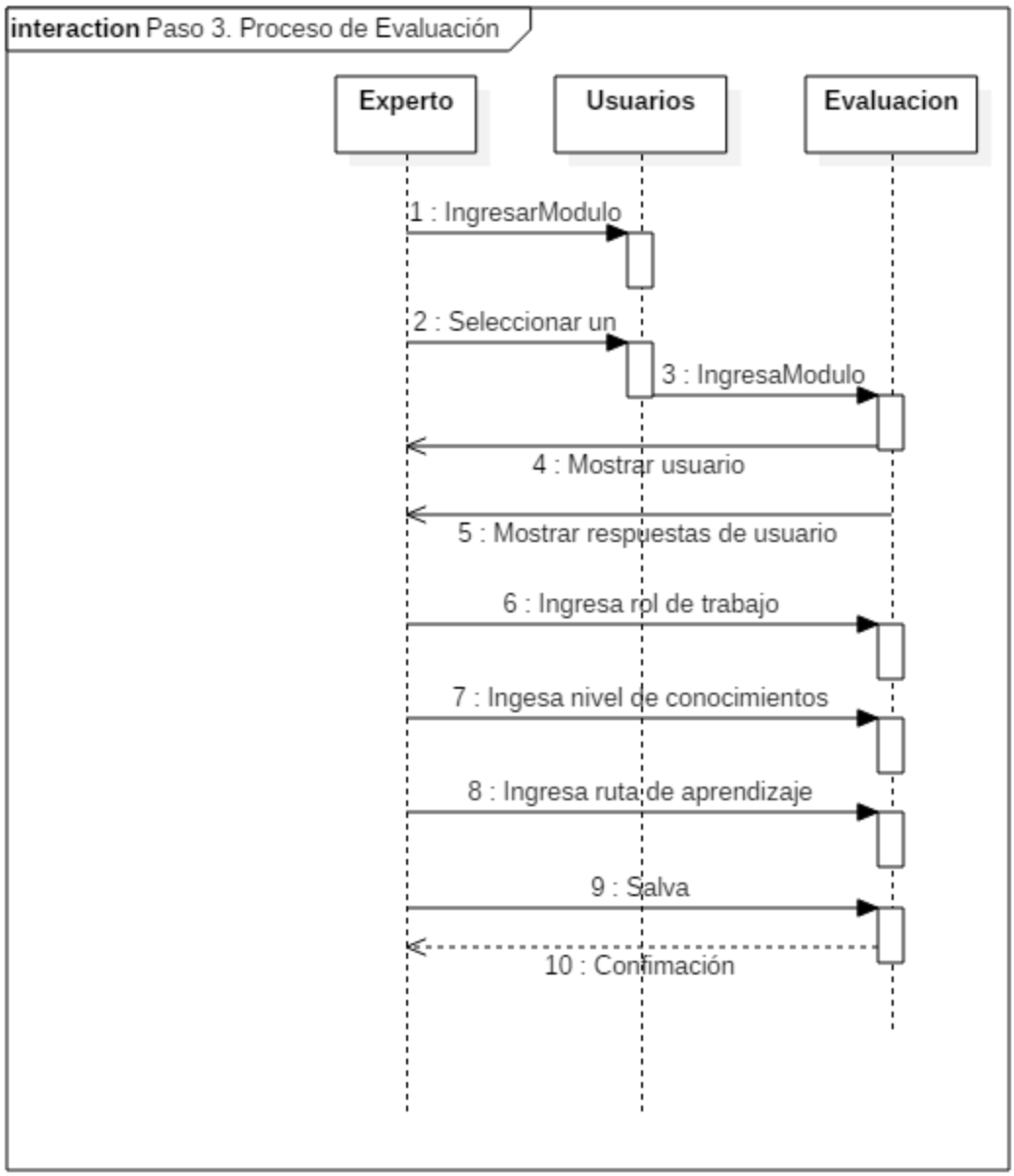

Diagrama 22. Diagrama secuencial que muestra el proceso de evaluación en el sistema.

4.3 Requerimientos de arquitectura

4.3.1 Requisitos funcionales.

Los requerimientos funcionales (RFs) engloban los distintos tipos de requerimientos que se reflejan en los comportamientos de la aplicación y que se engloban como: requerimientos de negocio, requerimientos de usuario, requerimientos funcionales detallados y requerimientos de sistema [29]. En la Tabla 10. Requerimientos funcionales del sistema. se muestran y se describe los requerimientos funcionales del sistema.

Tabla 10. Requerimientos funcionales del sistema.

Requerimientos Funcionales							
Id	**Titulo**	**Tipo**	**Complejidad**	**Impacto**	**Relación**	**Descripción (estímulo)**	**Solución propuesta**
RF-1	Loguin	Seguridad	Baja	Alta		El sistema incluye un procedimiento de autorización de usuarios, en el cual los usuarios deben identificarse usando un nombre de usuario y contraseña. Sólo los usuarios autorizados pueden acceder a los datos del sistema.	El sistema contiene una página de Loguin para la identificación y verificación del usuario.
RF-2	Encriptar password	Seguridad	Media	Alta	RF-1	El sistema encripta el password del usuario.	Utiliza métodos de hashing para el encriptado del password con iteraciones de mínimo 10. Debe incluir clave privada y salt.
RF-3	Longitud de password	Seguridad	Baja	Alta	RF-1	La longitud mínima del password es de 20 caracteres alfanuméricos.	El desarrollo se planteó con el programador, de acuerdo al lenguaje a usar.
RF-4	Lista de usuarios	Funcionalidad	Media	Alta		El sistema genera una lista de usuarios a evaluar.	Página con lista de usuario. Este debe ser parte del módulo de usuario.
RF-5	Estatus del usuario	Usabilidad	Baja	Alta	RF-4	Se establece una referencia que indique el estatus	*Si al usuario está activo y sin evaluar se

						del usuario. Los estatus posibles son: Evaluar, no activo, editar.	muestra la referencia: Evaluar. *Si el usuario ya se evaluó se muestra la referencia: Editar. *Si al usuario se le desactivo, se muestra la referencia: No activo. *Si el usuario es eliminado, no aparecerá en la lista de usuarios.
RF-6	Existencia de las respuestas al cuestionario por parte del colaborador	Usabilidad	Baja	Media	RF-4	Se establece una referencia en la lista de usuarios para indicar si existen datos del cuestionario. Estas referencias son: Sin datos, con datos.	Se definió el desarrollo con el programador, de acuerdo al lenguaje a usar.
RF-7	Colores de las referencias en lista de usuarios	Usabilidad	Baja	Media	RF-4	Establece colores que faciliten la identificación de las referencias al status.	Cada status tiene un color que facilite la identificación.
RF-8	Usuario con autorización a contestar el cuestionario	Usabilidad	Media	Alta	RF-4	El usuario colaborador puede ingresar a contestar el cuestionario.	Se desarrolló módulo de control de permisos de los usuarios.
RF-9	Número de veces que se puede contestar el cuestionario	Modificabilidad	Baja	Alta	RF-16	El cuestionario solo puede ser contestado solo una vez. Para poder modificarlo se debe eliminar el existente.	Definido en el desarrollo con el programador, de acuerdo al lenguaje a usar.
RF-10	Relleno automático de los inputs del formulario	Usabilidad	Baja	Baja	RF-16	Desactivado el relleno automático de los inputs de los formularios.	Definido en el desarrollo con el programador, de acuerdo al lenguaje a usar.
RF-11	Resultados del colaborador	Usabilidad	Media	Alta	RF-11	El usuario colaborador y experto puede observar el reporte de los resultados individual del colaborador.	Desarrollo del módulo de control de permisos de los usuarios.
RF-12	Exportación de los resultados	Usabilidad	Media	Media	RF-11	El sistema permitir la exportación de los resultados de la evaluación.	Desarrollo de módulo de exportación de datos.

RF-13	Generar reporte individual del colaborador	Usabilidad, Funcionalidad	Baja	Alta	RF-11	El sistema genera un reporte individual de cada colaborador, donde se muestren los resultados de la evaluación.	Definido en el desarrollo con el programador, acuerdo al lenguaje a usar.
RF-14	Generar reporte general de todos los colaboradores	Usabilidad, Funcionalidad	Baja	Alta	RF-11	El sistema genera reporte general de los resultados de todas las evaluaciones e identificable por cada colaborador.	Definido en el módulo de reportes.
RF-15	Descarga de resultados individuales.	Usabilidad	Media	Alta	RF-11	El usuario colaborador y experto pueden descargar los resultados individuales.	Desarrollo de módulo de control de permisos de los usuarios.
RF-16	Cuestionarios o formulario	Usabilidad	Baja	Alta		El sistema contiene un cuestionario que solicita datos a los colaboradores.	Desarrollo de módulo de formulario.
RF-17	Correo para el colaborador con los datos de ingreso al SVC.	Usabilidad, Funcionalidad	Media	Media		El sistema tiene una forma de enviar correo electrónico a los colaboradores, donde se muestren los datos de ingreso al sistema.	Desarrollo de módulo de envío de correos a los usuarios.
RF-18	Correo de resultado de la evaluación.	Usabilidad, Funcionalidad	Media	Media		El sistema permite el envío de correo electrónico a los colaboradores, para informales de los resultados de la evaluación.	Desarrollo de módulo de envío de correos a los usuarios.
RF-19	Listas de los elementos que componen el marco de referencia NICE.	Usabilidad	Media	Media		El sistema tiene una vista donde se muestren a los roles de trabajo, conocimientos, tareas y habilidades establecidas en el marco de referencia NICE.	Desarrollo del módulo de control de datos almacenados estáticos.
RF-20	Opciones del módulo del marco de referencia NICE	Usabilidad	Media	Media		El sistema permite agregar, modificar y eliminar cada uno de los componentes del marco de referencia NICE.	Contiene tablas propias para cada uno de los datos mencionados anteriormente.

RF-21	Opciones del módulo de usuarios	Usabilidad	Media	Alta	RF-4	El sistema permite agregar, modificar, eliminar usuarios colaborador y experto.	Definido en el desarrollo con el programador, acuerdo al lenguaje a usar. Las opciones se establecerán en el módulo de usuarios.
RF-22	Alta de usuario	Usabilidad	Media	Alta	RF-4	El registro de usuarios contiene: nombre, apellido, correo, username, password, organización, status (activo o inactivo), usuario experto o colaborador. Por default el usuario debe estar activo y ser colaborador.	Definido en el desarrollo con el programador, acuerdo al lenguaje a usar.
RF-23	Alta de varios usuarios desde un archivo CSV	Usabilidad	Media	Media	RF-4	El sistema contiene un apartado para dar alta a usuarios a partir de la importación de un archivo CSV. La cantidad de usuarios que se podrán dar de alta en un solo archivo son de 1 a 500.	Desarrollo de módulo de importación de datos.
RF-24	Quienes pueden agregar usuarios de tipo colaborador	Fiabilidad	Media	Alta		El alta de usuarios solo lo pueden realizar el administrador y el experto.	Desarrollo de módulo de control de permisos de los usuarios.
RF-25	Reporte general de las evaluaciones	Usabilidad, Funcionalidad	Media	Alta		El sistema genera un reporte general de todas las evaluaciones realizadas.	Desarrollo de un módulo de reportes.
RF-26	Módulo de evaluación	Usabilidad	Alta	Alta		El sistema contiene un módulo para realizar las evaluaciones de los colaboradores.	Desarrollo de módulo de evaluación.
RF-27	Opciones de la evaluación	Usabilidad	Media	Alta	RF-26	La evaluación se puede modificar y eliminar.	Definido en el desarrollo con el programador, acuerdo al lenguaje a usar. Las opciones se establecerán en el módulo de evaluación.
RF-28	Escala de evaluación	Funcionalidad	Baja	Alta	RF-26	La vista de evaluación tiene establecido una escala de evaluación	Establecido por los stakeholders.

						para ingresar el conocimiento actual y posterior del colaborador (por ejemplo: novato, master, experto).	
RF-29	Número de rutas de aprendizaje	Funcionalidad	Baja	Alta	RF-26	En la vista de evaluación tiene máximo tres rutas de aprendizaje.	Definido el diseño con el desarrollador.
RF-30	Número de certificaciones por ruta de aprendizaje	Funcionalidad	Baja	Alta	RF-26	En la vista de evaluación: por cada ruta de aprendizaje se selecciona tres certificaciones diferenciando de la opción uno hasta la tres.	Establecido por los stakeholders.
RF-31	Input de las certificaciones	Funcionalidad	Baja	Alta	RF-26	La vista de evaluación contiene las referencias a las certificaciones para facilitar su selección.	Definido en el diseño con el desarrollador.
RF-32	Nombre del colaborador en la evaluación.	Funcionalidad	Baja	Alta	RF-26	La vista de evaluación muestra nombre del colaborador.	Definido el diseño con el desarrollador.
RF-33	Input del rol de trabajo	Funcionalidad	Baja	Alta	RF-26	La vista de evaluación contiene una entrada donde el experto defina su rol de trabajo del colaborador.	Definido en el diseño con el desarrollador.
RF-34	Mostrar respuestas del colaborador.	Funcionalidad	Media	Alta	RF-26	En vista de evaluación se observa las respuestas realizadas por los colaboradores, con el objetivo de analizarlas.	Definido en el diseño con el desarrollador.
RF-35	Mostrar rutas de aprendizaje de manera autómata	Funcionalidad	Alta	Alta	RF-26	Al seleccionar un rol de trabajo, se muestran las rutas de aprendizaje recomendadas. Estas se pueden modificar.	Definido en el diseño con el desarrollador.

4.3.2 Drivers de Atributos de calidad.

Los requerimientos no funcionales (RNFs) tienen que ver con la manera en que el sistema soporta a los RFs. Esto incluyen: reglas de negocio, atributos de calidad, restricciones, interfaces externas [29]. La Tabla 11 muestra el conjunto completo de requerimientos no funcionales del sistema desarrollado. Cada RNF se muestra su título, tipo, complejidad del requerimiento, impacto en el sistema, muestra una descripción general y por último una solución a implementar en el sistema.

Tabla 11. Requerimientos no funcionales.

Requerimientos no funcionales						
Id	Titulo	Tipo	Complejidad	Impacto	Descripción	Solución
RNF-1	Seguridad entre el equipo cliente y el servidor	Seguridad	Baja	Alto	La comunicación cliente-servidor esta cifradas y autenticadas.	Certificados de seguridad SSL/DDoS.
RFN-2	Protección de datos a personas no autorizadas	Seguridad	Media	Alto	El sistema asegura que los datos estén protegidos del acceso no autorizado.	El sistema incluye un procedimiento de autorización de usuarios, en el cual los usuarios deben identificarse usando un nombre de usuario y contraseña. Sólo los usuarios autorizados de esta forma podrán acceder a los datos del sistema.
RFN-3	Permisos de exportación de reporte general de las evaluaciones	Fiabilidad	Media	Alta	La exportación del reporte general de todas las evaluaciones solo se permite para los evaluadores.	Desarrollo de módulo de control de permisos de usuarios.
RFN-4	Permisos de acceso al sistema admin	Fiabilidad	baja	Alta	Los permisos de acceso al sistema admin solo se pueden cambiar por el administrador de acceso a datos.	Desarrollo de módulo de control de permisos de usuarios.
RFN-7	Permisos de acceso al formulario	Fiabilidad	baja	Alta	Los permisos de acceso al sistema formulario solo pueden ser cambiados por el administrador y el experto.	Desarrollo de módulo de control de permisos de usuarios.

RFN-8	Status de usuario colaborador	Permisos	Baja	Alta	Activar y desactivar un usuario colaborador solo puede ser realizarlo el administrador y el experto.	Desarrollo de módulo de control de permisos de usuarios.
RFN-9	Tipo de aplicación: web.	Usabilidad	Baja	Alto	La interfaz del usuario se ejecuta en un navegador web para permitir el acceso desde cualquier lugar con conexión a internet.	Se realiza el sistema en lenguaje de programación web. Usando HTM y apoyándose con JavaScript.
RFN-10	Disponibilidad del sistema.	Disponibilidad	Baja	Media	Disponibilidad promedio del 99%	Se tiene una infraestructura de hosting con buen historial de servicio.
RFN-11	Carga de trabajo por hora.	Distribución	Baja	Media	La aplicación es capaz de soportar una carga pico de 50 usuarios concurrentes en una hora, durante la realización del formulario.	Se utiliza un servidor dedicado con un núcleo, memoria RAM mínima de 1 GB y un disco duro con almacenamiento de 20 GB SSD.
RFN-12	Cantidad de bases de datos necesarias.	Almacenamiento	Baja	Media	Se tiene de un servicio, que permita trabajar con tres bases de datos a la vez.	Contratación de servidor dedicado con escalabilidad a la utilización de más base de datos.
RFN-13	Escalabilidad del sistema	Escalabilidad	Media	Media	Utilización de un hardware que permita escalabilidad a futuro, con el objetivo de permitir un buen rendimiento de futuras investigaciones.	Hardware o servicio de hosting que permite actualizarse para adaptarlo a la fase dos del proyecto.
RFN-14	Tiempo de respuesta de apertura	Rendimiento	Baja	Baja	El tiempo de respuesta de las solicitudes de apertura de la aplicación máximo 4 segundos en el 90% de las veces.	Servidor dedicado con un núcleo, memoria RAM de 1 GB
RFN-15	Interoperabilidad entre sistemas operativos	Interoperabilidad	Media	Alta	El sistema se puede implementarse en el sistema operativo Windows y Linux.	El sistema se realizó usando un framework de programación web, usando una máquina virtual como Docker.

RFN-16	Aplicación responsiva	Interoperabilidad	Baja	Media	La aplicación web posee un diseño "Responsive" a fin de garantizar la adecuada visualización en múltiples computadores personales, dispositivos tableta y teléfonos inteligentes.	Se tienen herramientas de apoyo para realizar una página responsiva. Se probó con diferentes navegadores en diferentes navegadores. Se usó templetes responsivos que usen librerías CSS y JavaScript.
RFN-17	Aspectos éticos en el almacenamiento de datos personales.	Confiabilidad	Alta	Alta	No se puede almacenar permanentemente datos personales de los usuarios que los identifique, como nombre, apellido, región, país, correo.	Se da la alternativa a los evaluadores de eliminar la información personal de usuario sin afectar los datos generales. Los datos generales se le asigna id y usuario de uso genérico con lo cual lo identifique.
RFN-18	Aspectos éticos en la vista de datos personales	Confiabilidad	Media	Alta	El sistema no revela a usuarios colaboradores datos personales de los otros colaboradores, solamente el personal.	Desarrollo de módulo de control de permisos de usuarios.
RFN-19	Facilidad de evaluación	Usabilidad	Media	Alta	El sistema ofrece a los evaluadores un reporte cómodo y fácil de analizar con el objetivo de realizar las evaluaciones de los participantes.	Evaluación de pruebas heurísticas de UX.
RFN-20	Búsqueda de roles de trabajo y certificaciones	Usabilidad	Media	Media	El sistema ofrece a los evaluadores una forma fácil de buscar los roles y certificaciones.	El tiempo de muestra de datos no es mayor a 0.5 ms.
RFN-21	Referencia que facilite la selección de una ruta de capacitación	Usabilidad	Media	Media	El software ofrece una manera fácil de referencias las certificaciones al momento de seleccionar una ruta de capacitación.	Evaluación de pruebas heurísticas de UX. El tiempo de apertura de la información no es mayor a 0.5 ms.
RFN-22	Reportes claros	Usabilidad	Media	Alta	El reporte de las rutas de capacitación es claro, tanto para los usuarios como para los evaluadores.	Evaluación de pruebas heurísticas de UX.

RFN-23	Tasa de errores cometidos por los usuarios	Fiabilidad	Media	Media	La tasa de errores cometidos por el usuario es menor del 1% de las transacciones totales ejecutadas en el sistema.	Definido en las opciones de respuesta con el desarrollador.
RFN-24	Tiempo para aprender a usar el sistema	Usabilidad	Media	Media	El tiempo de aprendizaje del sistema por un usuario experto es menor a 30 minutos.	Evaluación de pruebas heurísticas de UX.
RFN-25	Mensajes de error	Fidelidad	Media	Media	El sistema proporciona mensajes de error que sean informativos y orientados a usuario final.	Se usa JavaScript del lado del equipo cliente para verificar los datos. Usar modos de verificación del lado del servidor.
RFN-26	Perdidas de mensajes	Confiabilidad	Alta	Alta	No se permite la pérdida de mensajes, y todos los mensajes de salida son conocidos en 3 segundos como máximo.	Utiliza técnicas y herramientas de programación para la detección de errores en el envío de mensajes.
RFN-27	Tiempo de ejecución.	Tiempo	Media	Baja	El tiempo para iniciar la página principal no podrá ser mayor a 5 segundos.	Realizar pruebas heurísticas.
RFN-28	Compatibilidad en los navegadores	Compatibilidad	Media	Alta	La aplicación es compatible con las versiones posterior al 2016 en navegadores Chrome, Mozilla, zafarí, Edge, Microsoft Internet Explorer, Brave versiones posteriores de Windows 7.	Usa tecnologías de desarrollo web compatible en estos navegadores. Algunos de ellos: JavaScript, HTML, CSS
RFN-29	Documentación	Estándares	Alta	Alta	El procedimiento de desarrollo de software a usar está definido explícitamente (en manuales de procedimientos) y debe cumplir con los estándares ISO 9000.	* Documentación del análisis y diseño del proyecto. * Documentación del desarrollo de proyecto. *Manual de usuario.
RFN-30	Leyes y reglamentos de protección de datos	Legales	Alta	Alta	El nuevo sistema y sus procedimientos de mantenimiento se cumplen con las leyes y reglamentos de protección de datos.	Desarrollo del sistema respetando: *La ley Federal de Protección de Datos Personales en Posesión de los Particulares * Toma en cuenta las guías y documentos emitidos por el Instituto Nacional de

						Transparencia, Acceso a la Información y Protección de Datos Personales ("INAI"). *Se apoya en la hoja de referencia de OWASP.
RFN-31	Tiempo de inactividad	Seguridad	Media	Media	Si algún usuario no se encuentra activo durante 10 minutos en la cuenta personal del sistema esta se cierra automáticamente.	Definido la funcionalidad con el desarrollador, considerando el lenguaje de programación.

4.3.3 Atributos de calidad.

Los atributos de calidad forman parte de los "Requerimientos No Funcionales (RNFs)" del sistema [29]. Son características medibles que permiten expresar y evaluar el grado de satisfacción de los usuarios y/o diseñadores (es decir la calidad) con respecto al sistema [29]. Existen diferentes métricas de calidad, entre las más comunes se encuentran el: desempeño, seguridad, modificabilidad, usabilidad y facilidad de prueba [29]. En la Tabla 12 se muestran los atributos de calidad del sistema desarrollado; incluye el tipo, su complejidad, impacto, descripción y solución utilizada para satisfacer el atributo e implementado en el sistema.

Tabla 12. Atributos de calidad del sistema de validación de conocimientos.

Atributos de calidad							
Id	**Requerimiento**	**Fuente del estímulo**	**Estimulo**	**Artefacto**	**Entorno**	**Respuesta**	**Medida de la respuesta**
AC-1	La comunicación cliente-servidor son cifradas y autenticadas.	Sistema (SVC)	Solicitud de ingreso a la página	Comunicación entre navegadores más conocidos del mercado	En cualquier entorno.	Certificado SSL	Se muestra certificado de seguridad SSL de fuentes seguras en el navegador
AC-2	El sistema asegura que los datos estén protegidos del acceso no autorizado.	Usuario (experto o colaborador)	Intento de ingreso a módulos sin autorización.	Loguin	En cualquier entorno.	Acceso denegado	Mensaje de acceso denegado y no ingreso al sistema.

AC-3	Disponibilidad promedio del 99%	Usuario (experto, colaborador o admin)	Ingreso al sistema	Módulo de formulario y experto	Condiciones normales de operación del hosting contratado	Acceso al sistema	50 intentos de ingreso al sistema por tres días. Disponibilidad promedio del 99%
AC-4	La aplicación es capaz de soportar una carga pico de 50 usuarios concurrentes en una hora, durante la realización del formulario.	Usuario (colaborador)	La aplicación debe ser capaz de soportar una carga pico de 50 usuarios concurrentes en una hora, durante la realización del formulario.	Módulo formulario	Condiciones normales de operación con 50 usuarios en una hora.	Acceso al sistema	50 colaboradores ingresan al sistema en una hora. Se realizó pruebas de conexión.
AC-5	El tiempo de respuesta de las solicitudes de apertura de la aplicación es máximo 4 segundos en el 90% de las veces.	Usuario (experto, colaborador o admin)	Ingreso al sistema	Loguin	Condiciones normales de operación	Tiempo de apertura 4 segundos.	50 colaboradores ingresan al sistema en una hora. Se realizó pruebas de conexión.
AC-6	La aplicación web posee un diseño "Responsive" a fin de garantizar la adecuada visualización en múltiples computadores personales, dispositivos tableta y teléfonos inteligentes.	Usuario (experto, colaborador o admin)	Cargar sistema evaluación y experto.	Celular, Laptop, equipo de escritorio	Condiciones normales de operación	Vista responsive	Se muestra la vista cómoda para el usuario. Se realizó pruebas heurísticas de UX.
AC-7	No se almacenan permanentemente datos personales de los usuarios que los identifique, como nombre, apellido, región, país, correo.	Usuario (experto, colaborador o admin)	Eliminar datos	Almacenamiento en base de datos.	Condiciones normales de operación	Eliminar los datos confidenciales. No se eliminar los datos generales.	Eliminación de los datos que identifican al usuario.

RFN-8	El sistema no revela a usuarios colaboradores datos personales de los otros colaboradores, solamente el personal.	Usuario (colaborador)	Ingreso al sistema	Módulo formulario.	En cualquier entorno	No se muestra datos personales de otros colaboradores.	Se realizan tests de inyección de script y SQL.
AC-09	El sistema ofrece a los evaluadores un reporte cómodo y fácil de analizar con el objetivo de realizar las evaluaciones de los participantes.	Usuario (experto)	Realizar evaluaciones	Módulo evaluación	Condiciones normales de operación	Buena experiencia del usuario	Test heurístico de UX.
AC-10	La tasa de errores cometidos por el usuario es menor del 1% de las transacciones totales ejecutadas en el sistema.	Usuario (experto, colaborador o admin)	Ingreso de datos y dar submit	Módulo formulario, Módulo experto	Condiciones normales de operación	La tasa de errores cometidos por el usuario deberá ser menor del 1% de las transacciones totales ejecutadas en el sistema.	Test. de UX.
AC-13	El tiempo para iniciar la página principal no puede ser mayor a 30s.	Usuario (experto, colaborador o admin)	Ingreso a los sitios principales.	Módulo de experto, módulo de formulario	Condiciones normales de operación. Condiciones con conexión degradada.	El tiempo para iniciar la página principal menor a 30s.	Test. en varios navegadores.
AC-14	La aplicación es compatible con las versiones posterior al 2016 en navegadores Chrome, Mozilla, zafarí, Edge, Microsoft Internet Explorer, Brave versiones	Navegadores.	Navegar en diferentes navegadores	Navegadores con las versiones posterior al 2016 en navegadores Chrome, Mozilla, zafarí, Edge, Microsoft Internet Explorer, Brave versiones	Condiciones normales de operación	Mostrar y realizar cualquier operación permitida.	Test en los navegadores.

	posteriores de Windows 7.			posteriores de Windows 7.			
AC-15	Cierre de la cuenta en 10 minutos de inactividad.	Sistema (SVC)	Inactividad en la cuenta	Cuenta del usuario activa	En cualquier entorno	Cierre de la cuenta en 10 minutos de inactividad.	Test de inactividad en la cuenta. Realizar el test con varios usuarios, varios dispositivos.

4.3.4 Driver de restricciones.

Las restricciones también son consideradas como parte de los drivers arquitecturales [29], en este proyecto se presentan en la Tabla 13, para su mejor comprensión.

Tabla 13. Drivers de restricciones del sistema de validación de conocimientos.

Id	Tipo	Descripción
Res-1	Tecnología	El sistema se desarrolló con el framework django
Res-2	Seguridad	El sistema asegura los datos personales de las personas.
Res-3	Calendarización	El tiempo límite de entrega del proyecto fue a más tardar el 01 de marzo del 2021
Res-4	Éticos	Se almacena permanentemente la información que no comprometa al participante, usando para ello tablas por separado en donde los datos se almacenan con un identificador no relacionado al participante.
Res-5	Negocio	El proyecto aporte conocimientos para la realización de la tesis, adaptadas a las necesidades tanto personales como de la empresa a la que se le desarrolla el sistema.

4.4 Diseño arquitectónico

Durante esta etapa se definió las estructuras que componen la arquitectura del sistema. La creación de estas estructuras se hiso en base a patrones de diseño, tácticas de diseño y elecciones tecnológicas. El diseño que se realizado busca ante todo satisfacer los requerimientos que influencian a la arquitectura, y no simplemente incorporar diversas tecnologías porque están “de moda” [29].

La determinación y recopilación de los requerimientos nos llevó un paso más allá, en el desarrollo del diseño, continuando con la documentación y finalizando con la validación del diseño arquitectónico. De este último se definió la necesidad de una nueva iteración al proceso de diseño arquitectónico.

4.4.1 Estructura general del sistema

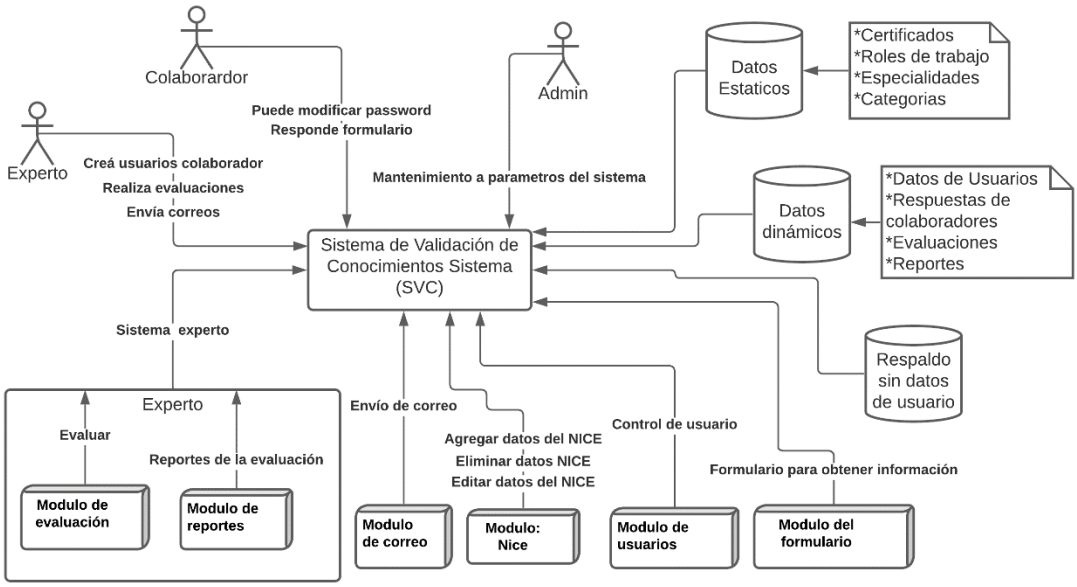

Ilustración 6. *Estructura general del sistema.*

En la Tabla 14 se describe la Ilustración *6*, estructura general del sistema.

Tabla 14. Descripción de la estructura general del sistema de validación de conocimientos.

Descripción de la estructura general del sistema (Primera iteración del diseño)	
Usuarios	En general el sistema es manejado por tres tipos de usuarios: Colaborador, experto, admin
Módulos principales del sistema	Utiliza cinco módulos principales: evaluación, reportes, usuarios, formularios, correo. El componente experto incluye los módulos principales para cumplir con la capa de negocio en el proceso de evaluación y control de reportes.
Almacenamiento	Contiene tres bases de almacenamiento lógica para satisfacer la primera etapa del proyecto, estos son. Datos estáticos, datos dinámicos y respaldo de datos de identificación del usuario. Para esta etapa se pueden crear tablas en una sola base de datos, que satisfagan el almacenamiento lógico. Posteriormente se puede migrar a la utilización de tres bases de datos para cada una de la lógica de almacenamiento.

En la Tabla 15 se describe de forma detallada los permisos de acceso de los usuarios. La información mostrada en la tabla muestra más información que ayuda a comprender mejor la estructura general del sistema.

Tabla 15. Detalles de usuarios con los permisos de acceso.

Detalle de usuarios con los permisos de acceso	
Colaborador	• Modificar su propio password. • Ingresar al formulario. • Enviar respuestas del formulario. • Ver informe de respuestas enviadas. • Ver reporte del resultado personal de la evaluación.
Experto	• Ver lista de usuarios a evaluar. • Registrar colaborador. • Modificar colaborador. • Eliminar colaborador. • Importar usuarios. • Registrar evaluación.

	• Guardar evaluación. • Modificar evaluación. • Eliminar evaluación. • Ver reporte personal de un colaborador. • Ver reporte dividido por colaborador. • Ver reporte general. • Registrar, eliminar, modificar certificados. • Registrar, eliminar, modificar roles de puesto de trabajo. • Registrar, eliminar, modificar especialidades de puesto de trabajo. • Registrar, eliminar, modificar categorías de puesto de trabajo. • Enviar correo a uno o más colaboradores con los datos de ingreso al sistema. • Enviar correo a uno o más colaboradores con los resultados obtenidos de la evaluación.
Admin	• Tiene todos los permisos del colaborador y experto. • Ingreso al panel del administrador. • Agregar o remover permisos de los usuarios.

4.4.2 Despliegue de la solución

Por condiciones de los drivers restrictivos de los requerimientos el sistema este se desarrolló con el framework django (RES-1) el cual usa el patrón MVT (Modelo-Vista-Plantilla) y el lenguaje base es Python. La otra restricción que satisface este framework es la seguridad de los datos. En la Ilustración 7se observa la estructura, de forma general, el MVT.

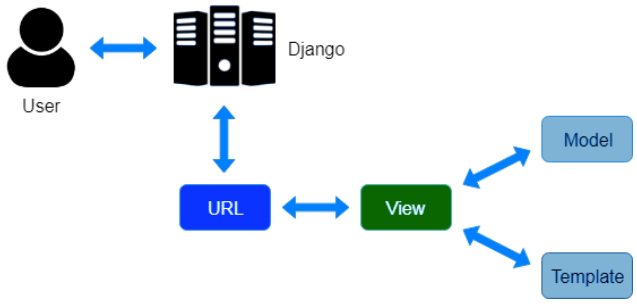

Ilustración 7. Patrón Vista Témplate en django

En la página oficial de django podemos ver que se pueden ver destacadas páginas que lo utilizan, como: Instagram, Mozilla foundation, national geographic, open knowledge foundation, pinterest [40].

Las ventajas y desventajas principales que se encontraron de usar este framework son las siguientes (véase Tabla 16):

Tabla 16. Ventajas y desventajas de usar el framework Django.

Ventajas principales	**Desventajas principales**
Django fue creado para trabajar bajo un patrón MVC (Modelo Vista Controlador) quien se encarga del manejo de controladores, esto lo caracteriza en un framework reusable y permite el desarrollo ágil.	A pesar de su excelente documentación, es muy extensa y tiende a ser confusa.
Según la comunidad que desarrolla bajo Python, los API's REST que genera Django son mucho mejores, debido a que se pueden convertir en páginas HTML como puntos finales (en inglés Endpoints).	A la hora de realizar un API REST conlleva cierta condición de dificultad a comparación de Flask.
Provee una estructura del proyecto autogenerado, muy útil a la hora de organización y optimización de tiempo y código.	
Tiene un panel de administración para gestionar bases de datos.	
Implementa ORM, con una muy buena interfaz para acceso a la base de datos	
Seguridad: implementa por defecto algunas medidas de seguridad, las más clásicas, para que no haya SQL Injection, no haya Cross site request forgery (CSRF) o no haya Clickjacking por JavaScript. Django se encarga de manejarlo.	
Es gratuito y de código abierto.	

Utilizando el framework django y MVT se determinó el Diagrama 23, el cual es la arquitectura general del sistema para un ambiente de desarrollo y pruebas locales. Este diagrama apoya al entendimiento general de la construcción del sistema desarrollado.

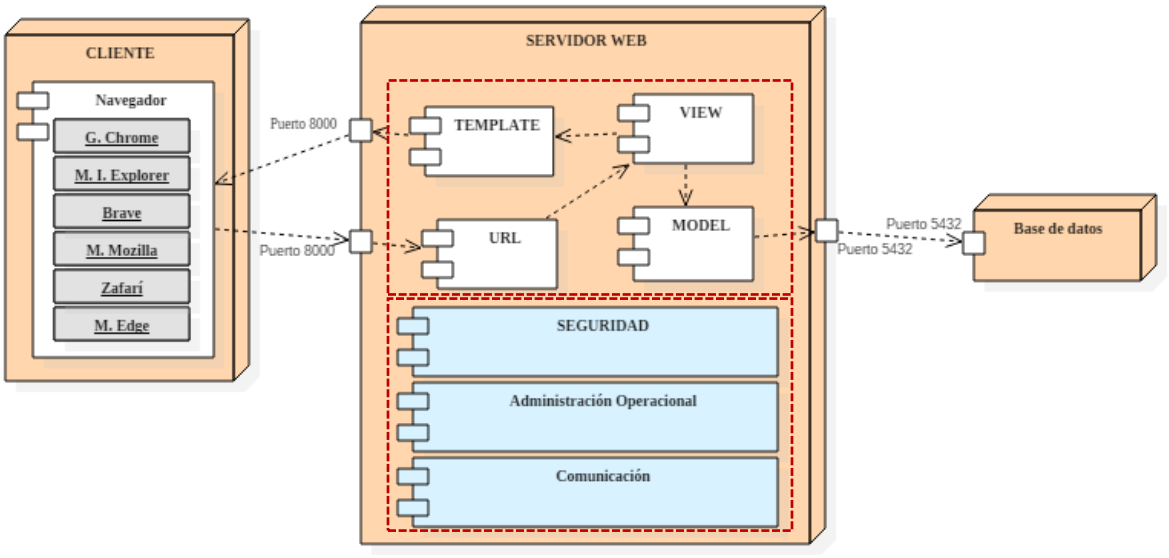

Diagrama 23. Arquitectura general de sistema para realizar las pruebas en servidor local.

El Diagrama 23 establece una arquitectura a nivel físico de tipo cliente-servidor, en donde el cliente por medio del navegador web realiza solicitudes al servidor web, el cual utiliza el puerto 8000 para la comunicación. La solicitud es recibida por el controlador de URL, este redirecciona hacia la vista solicitada. La vista despliega el témplate y los datos que se requieran, en tal caso si se realizó una petición de datos. La descripción de cada componente que tiene responsabilidades y propiedades que se requieren en el servidor para el desarrollo de esta arquitectura es la mostrada en la Tabla 17:

Tabla 17. Componentes principales en framework DJANGO [40].

No.	Elemento	Responsabilidades	Propiedades
1	Cliente	Equipo que soporta un navegador web.	*Equipo portátil de cómputo o Equipo de escritorio utilizado para acceder al sistema. *Sistema operativo mínimo Windows 7. *Contiene instalado mínimo un navegador.
2	NAVEGADOR	*Componente cliente. *Aplicación o programa que permite el acceso a la Web, interpretando la	*Implementa protocolo de comunicaciones. *Puerto de comunicación 8000.

		información de distintos tipos de archivos y sitios web para que estos puedan ser vistos.	* Navegadores: Chrome 15 o superior, Firefox 10 o superior, Internet Explorer 9 o superior, Opera 20 o superior, Safari 5 o superior.
3	SERVIDOR WEB	*Equipo de gran potencia que se encarga de prestar servicios. En este caso se puede contratar un hosting (Servidores VPS). Este implementa programas informáticos que procesa una aplicación del lado del servidor, realizando conexiones bidireccionales o unidireccionales y síncronas o asíncronas con el cliente y generando o cediendo una respuesta en cualquier lenguaje o aplicación del lado del cliente.	*La arquitectura del sistema operativo puede ser Linux o Windows. *Componentes a implementar: manejador de base de datos (postgreSQL), servidor de aplicaciones (UWSGI) (Que implemente un servidor HTTP WSGI), servidor web/proxy (Nginx). *Hardware para iniciar el proyecto: HDD mínimo de 20 Gb, RAM mínima de 1 Gb, CPU 1 Core. *Conexión de carga: 20 Mbps *Conexión de descarga: 50 MB/s *Seguridad: certificado SSL y protección DDoS, acceso al servidor por contraseña.
4	URL	Mapeador URL para redirigir las peticiones HTTP a la vista apropiada basándose en la URL de la petición. A pesar de que éste podría contener todo el código del mapeo URL, es más común delegar algo del mapeo a las propias aplicaciones.	*Importa cada una las vistas del sistema. *PATCH que establece un nombre y redirige a la vista.
5	SETTINGS	Contiene todos los ajustes del sitio.	Es donde se registran todas las aplicaciones que creamos, la localización de nuestros ficheros estáticos, los detalles de configuración de la base de datos, etc.
6	VIEW	Función de gestión de peticiones que recibe peticiones HTTP y devuelve respuestas HTTP. Las vistas acceden a los datos que necesitan para satisfacer las peticiones por medio de modelos, y delegan el formateo de la respuesta a las plantillas ("Témplates").	*Componente del patrón de diseño que implementa django 3.1. (Model, View, Témplate). * Lenguaje de programación Python 3.8
7	TEMPLATE	fichero de texto que define la estructura o diagrama de otro fichero (tal como una página HTML), con marcadores de posición que se utilizan para representar el contenido real. Una vista puede crear dinámicamente una página usando una plantilla, rellenándola con datos de un modelo.	*Componente del patrón de diseño que implementa django 3.1. (Model, View, Template). * Lenguaje de programación Python 3.8
8	MODEL	Objetos de Python que definen la estructura de los datos de una aplicación y proporcionan mecanismos para gestionar (añadir, modificar y borrar) y consultar registros en la base de datos.	*Parte del patrón de diseño que implementa django 3.1. (Model, View, Template). * Lenguaje de programación Python 3.1

9	SEGURIDAD	*Administrar cuentas de usuario y contraseñas. *Administrar la información de la sesión de la cuenta. *Monitorea los informes de seguridad para enviar mensajes de error.	*Funcionalidad implementada en django 3.1 como apoyo a los desarrolladores en los errores comunes de seguridad. * Lenguaje de programación Python 3.8
10	ADMINISTRACIÓN OPERACIONAL	Área dentro del sitio que puedes usar para monitorear, crear, consultar, actualizar y borrar registros de todos los aspectos del sistema.	*Esta página o modulo está definida como panel de control en django 3.1. *Lenguaje de programación Python 3.8
11	COMUNICACIÓN	Administra la comunicación en django, permitiendo las solicitudes y envió de datos. Si ocurre un error envía información en un mensaje de error.	*Funcionalidad automática que implementa django para la comunicación y control de envío y solitudes de datos. * Lenguaje de programación Python 3.8
12	BASE DE DATOS	Equipo que permite almacenar y administrar un gran número de información de una forma organizada para su futura consulta, nuevo ingreso de datos, modificaciones, eliminación.	*Implementa el manejador de base de datos PostgreSQL 12 o posterior. Protegido por contraseña (mínimo 20 caracteres) de acceso a los datos. *El acceso a la base de datos es a través del puerto 5432.

4.4.2.1 Integración de las funcionalidades del “Modelo Vista Témplate”

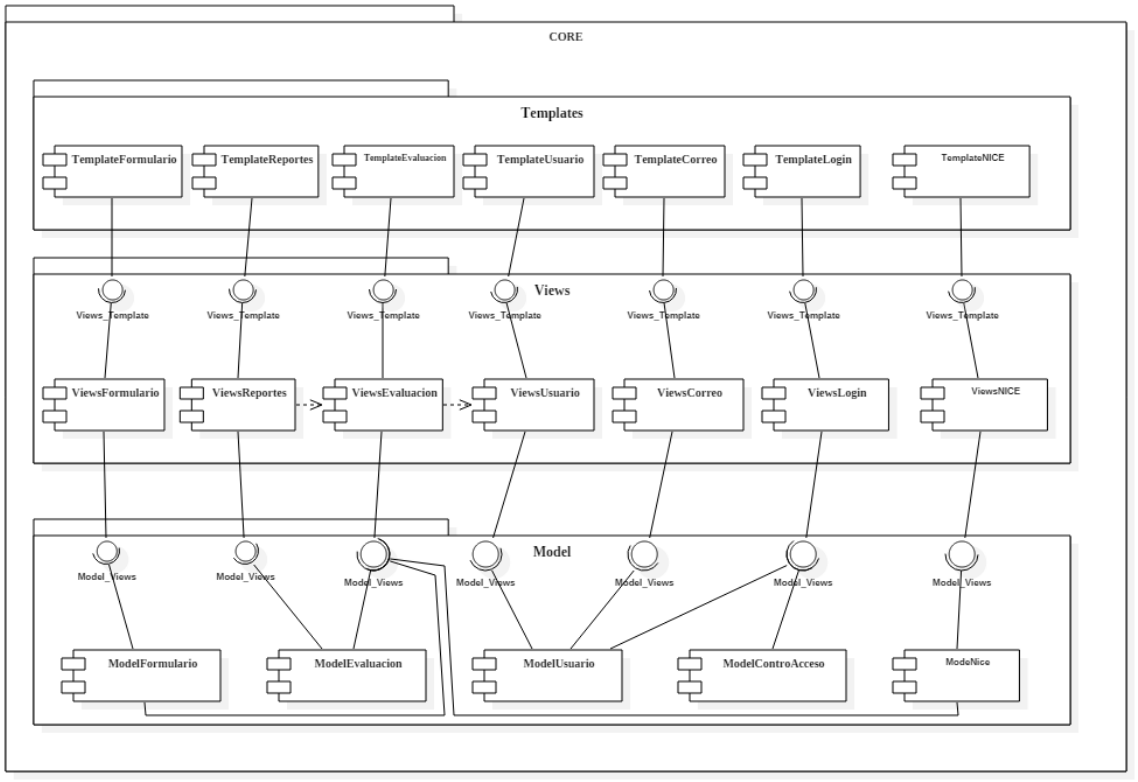

Diagrama 24. Módulos (componentes) necesarios para el desarrollo de las clases del "Sistema Validación de Conocimientos” representado en la modelo vista témplate

Cada componente del “Modelo Vista Témplate” pertenece a un paquete. Por ejemplo, del Diagrama 24 el componente “TemplateUsuario” pertenece al paquete de “Templates”, el componente “ViewsUsuario” pertenece al paquete “Views” y el componente “ModelUsuario” pertenece al paquete “Model”. El conjunto de paquetes pertenece a un paquete de capa superior llamado “CORE”.

También en el Diagrama 24 se tienen las relaciones y dependencias de cada componente, donde se establece quien ofrece y quien solicita un servicio o funcionalidad. La comunicación entre cada componente relacionado es bidireccional, al menos que se indique lo contrario.

Un concepto importante en django es lo que representa una aplicación y la diferencia entre proyecto**.** Una aplicación es un conjunto portable (reutilizable) de una funcionalidad de django, típicamente incluye modelos y vistas, que conviven en un solo paquete de Python, a este paquete se le llama apps. Django apuesta por un sistema de reutilización de código organizado en apps, algo así como aplicaciones internas que implementan funcionalidades específicas. El proyecto es un conjunto de configuraciones a las que se "conectan" esas apps para que todo unido de lugar a un sitio web completo. Un proyecto puede contener múltiples apps, y una app puede ser incluida en múltiples proyectos.

Ya que se conoce la diferencia entre una aplicación y proyecto, continuamos con la organización estructural del proyecto, representando cada módulo como apps que corresponde al conjunto de componente de la modelo vista témplate con una relación. Respetando el modelo MVT y la filosofía de django, la app se organiza de la siguiente manera (véase Ilustración 8):

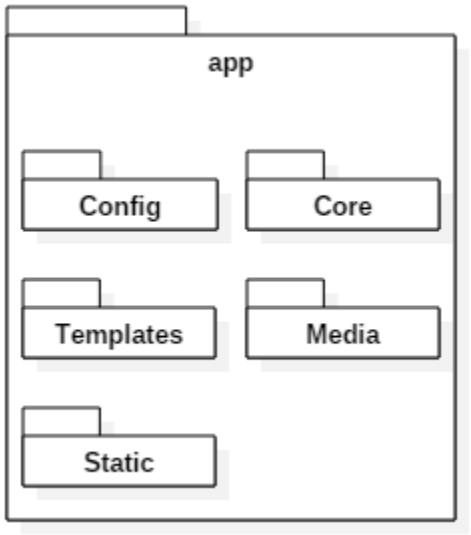

Ilustración 8. Organización de los paquetes principales necesarios para el desarrollo del sistema.

Config: contiene todas las configuraciones generales que afectan a todo el sistema.

Core (ver ilustración 8): contiene todos los módulos divididos por aplicación.

Templates: contiene los templetes básicos que se usaran en todas las aplicaciones.

Media: contiene videos, imágenes, sonidos, archivos que son estáticos en la aplicación.

Static: contiene todos los paquetes de script CSS, script de JavaScript, plugin externos, etc.

Cada módulo principal necesarios para el desarrollo del sistema esta constituidos de los componentes “Templates”, “Views”, “model.py”, “url.py”, esto se muestra en Ilustración 9:

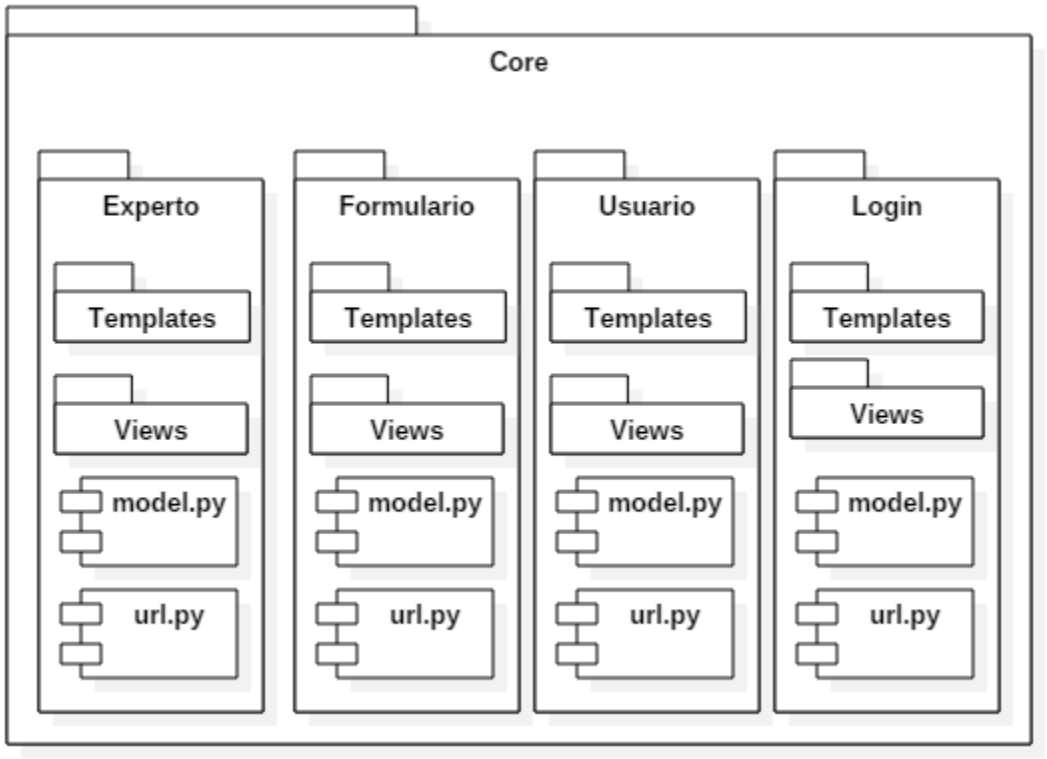

Ilustración 9. Organización interna del paquete "Core" donde se muestran las app y componentes incluidos.

Nota: A cada módulo principal dentro de “Core” también se le llama aplicación (APP).

En las siguientes ilustraciones se muestra la organización general interna de cada APP (véase Ilustración 10):

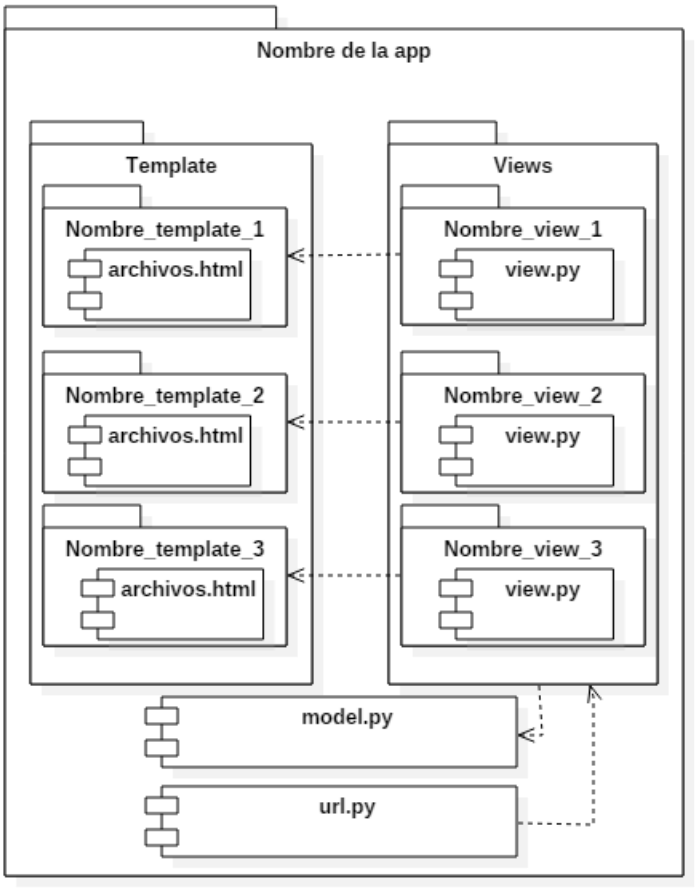

Ilustración 10. Organización interna general de las APP.

Para ejemplificar la Ilustración 10, la Ilustración 11 muestra la organización interna de la APP “experto”:

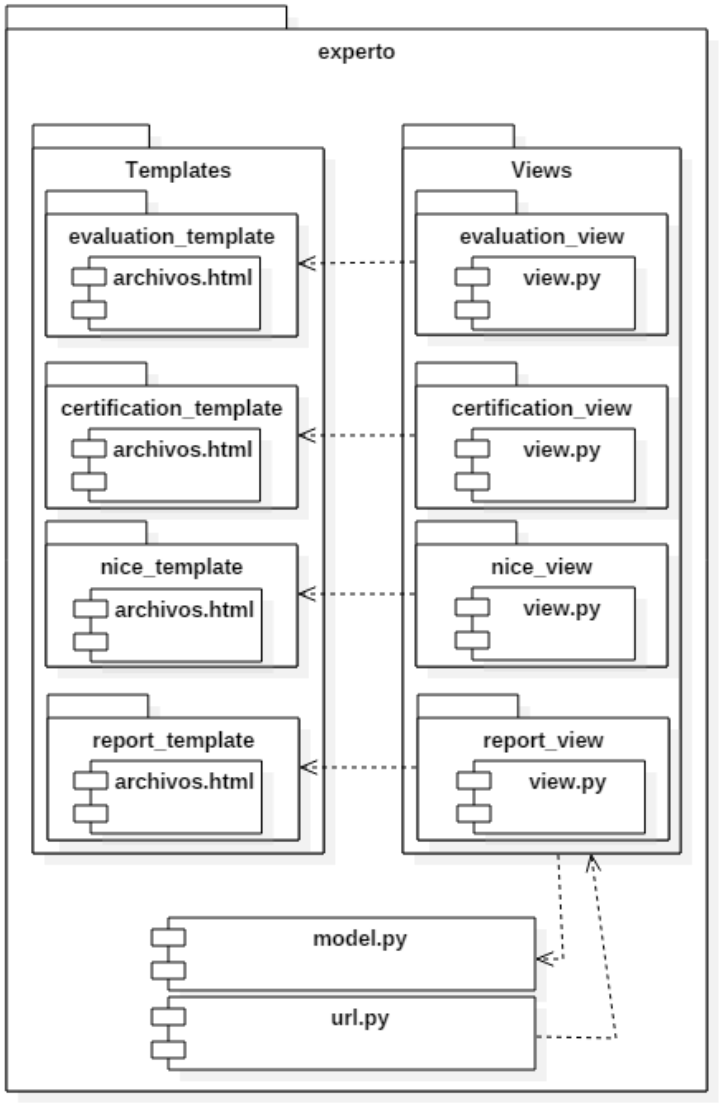

Ilustración 11. Ejemplo de la composición interna de la app experto.

.

En el Diagrama 25 se muestra la estructura jerárquica de los paquetes y componentes internos de la app “experto”.

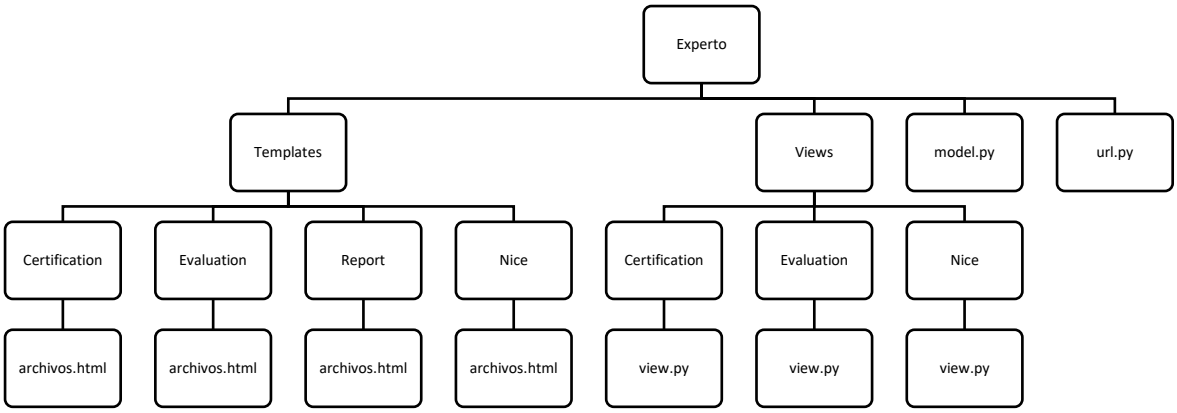

Diagrama 25. Estructura jerárquica de los paquetes y componentes internos de la app “experto”.

En el Diagrama 26 se muestra la estructura jerárquica de los paquetes y componentes internos de la app “formulario”.

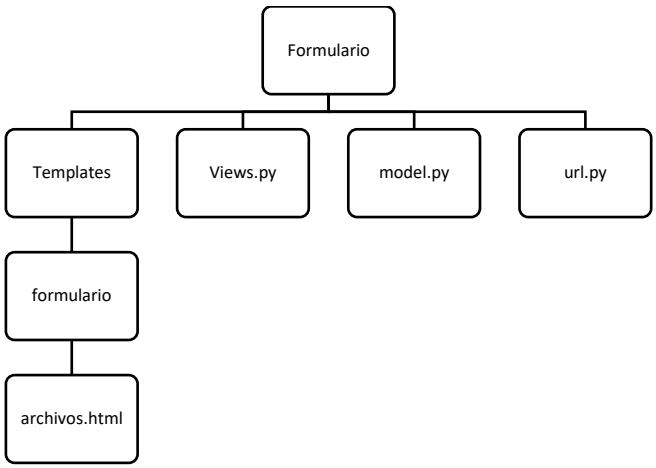

Diagrama 26. Estructura jerárquica de los paquetes y componentes internos de la app "Formulario".

En el Diagrama 27 se muestra la estructura jerárquica de los paquetes y componentes internos de la app “User”.

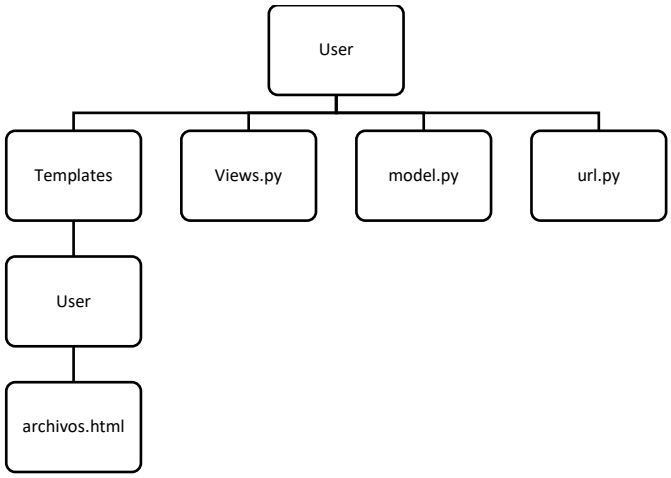

Diagrama 27. Estructura jerárquica de los paquetes y componentes internos de la app "User".

En el Diagrama 28 se muestra la estructura jerárquica de los paquetes y componentes internos de la app “Login”.

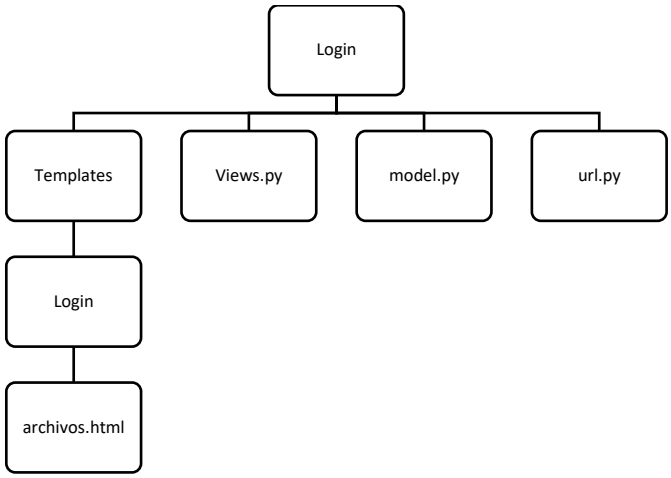

Diagrama 28. Estructura jerárquica de los paquetes y componentes internos de la app "Login".

La Tabla 18 muestra de forma detallada las funcionalidades que contiene de la APP "experto":

Tabla 18. Detalle de las Funcionalidad de la app "experto".

	Detalle de las Funcionalidad de la app "experto"			
Id	**Funcionalidad**	**Nombre paquete**	**Nombre del componente view (.py)**	**Nombre del componente template (.html)**
EXP-01	Crear evaluación	Evaluation	view.py	create.html
EXP-02	Modificar evaluación	Evaluation	view.py	Edit.html
EXP-03	Eliminar evaluación	Evaluation	view.py	delete.html
EXP-04	Listar certificaciones	Certification	View.py	list.html
EXP-05	Crear certificación	Certification	view.py	create.html
EXP-06	Modificar certificación	Certification	view.py	Edit.html
EXP-07	Eliminar certificación	Certification	view.py	delete.html
EXP-08	Listar roles de puesto de trabajo	Nice	view.py	list.html
EXP-09	Crear roles de puesto de trabajo	Nice	view.py	create.html
EXP-10	Modificar roles de puesto de trabajo	Nice	view.py	Edit.html
EXP-11	Elimina roles de puesto de trabajo	Nice	view.py	delete.html
EXP-12	Listar especialidades de los roles de puesto de trabajo	Nice	view.py	list.html
EXP-13	Crear especialidades de los roles de puesto de trabajo	Nice	view.py	create.html
EXP-14	Modificar especialidades de los roles de puesto de trabajo	Nice	view.py	Edit.html
EXP-15	Elimina especialidades de los roles de puesto de trabajo	Nice	view.py	delete.html
EXP-16	Listar categorías de los roles de puesto de trabajo	Nice	view.py	list.html
EXP-17	Crear categorías de los roles de puesto de trabajo	Nice	view.py	create.html
EXP-18	Modificar categorías de los roles de puesto de trabajo	Nice	view.py	Edit.html
EXP-19	Elimina categorías de los roles de puesto de trabajo	Nice	view.py	delete.html
EXP-20	Crear reporte individual de cada evaluación existente.	Report	view.py	report_individual.html
EXP-21	Crear reporte general del conjunto de todas las evaluaciones.	Report	view.py	report_general.html
EXP-22	Crear reporte general filtrado y dividido por nombre de usuario.	Report	view.py	report_general_filter.html

4.5 Diseño de los modelos de datos

El Diagrama 29, Diagrama 30 y Diagrama 31, muestran el modelado de las tablas de la base de datos, los cuales también están definidas en la mismo código de la aplicación en el componente “model”, ya que django permite crear las tablas en la base de datos a partir de la definición de las clases. Cada una de las tablas está compuesta del nombre de la clase y sus atributos. Se observa en la clase Form_svc (Diagrama 29) la composición del modelo de datos utilizados para definir el módulo formulario. Así de la misma manera, en el Diagrama 30 y Diagrama 31 también están compuestos de los nombres de clase y atributos que se representan igual en la tabla de la base de datos.

Diagrama 29. Clase y atributos en el Model de la app "Formulario"

Diagrama 30. Clases y atributos en el Model de la app "User".

El Diagrama 31 muestra los nombres de las clases y los atributos utilizados para crear la app del módulo experto, pero además se observa la correlación entre cada una de las clases o tablas. La tabla o clase Evaluation depende de otras tablas, teniendo relación por medio de los atributos con llaves foráneas.

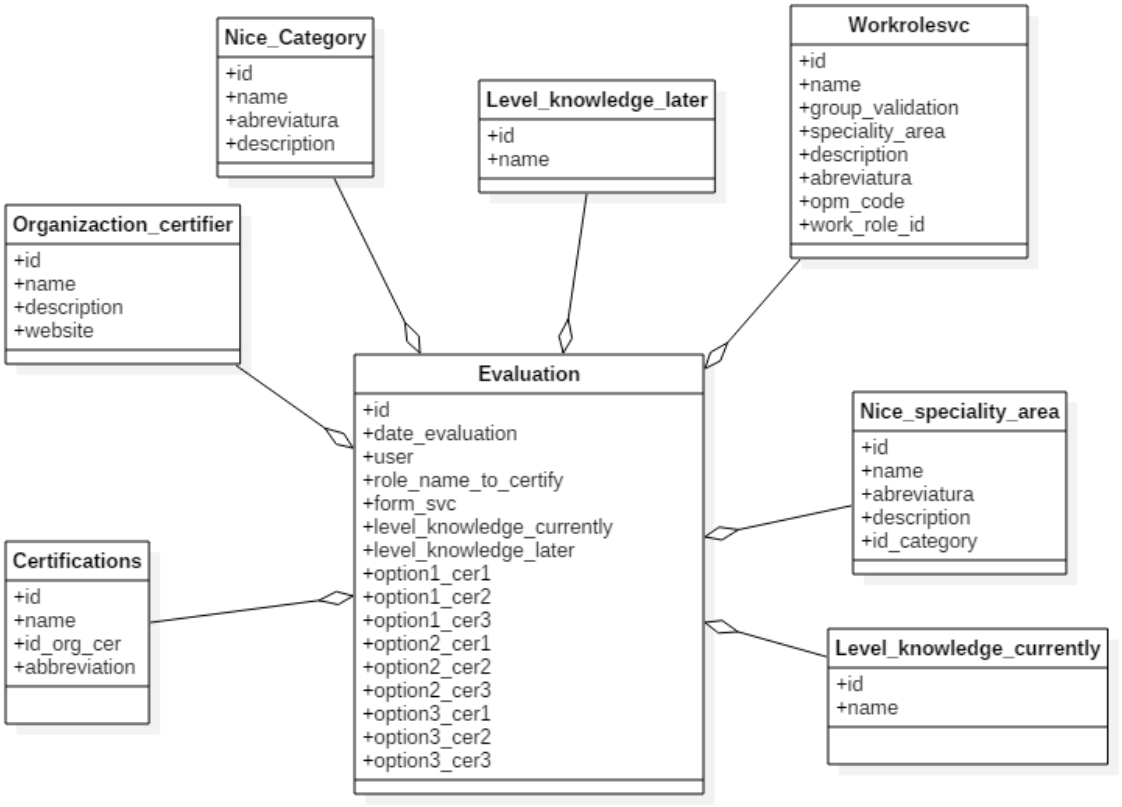

Diagrama 31. Clases y atributos en el Model de la app "Experto".

El Diagrama 32 muestra los nombres, atributos y relaciones en conjunto de todas las tablas que componen la base de datos del sistema de validación de conocimientos.

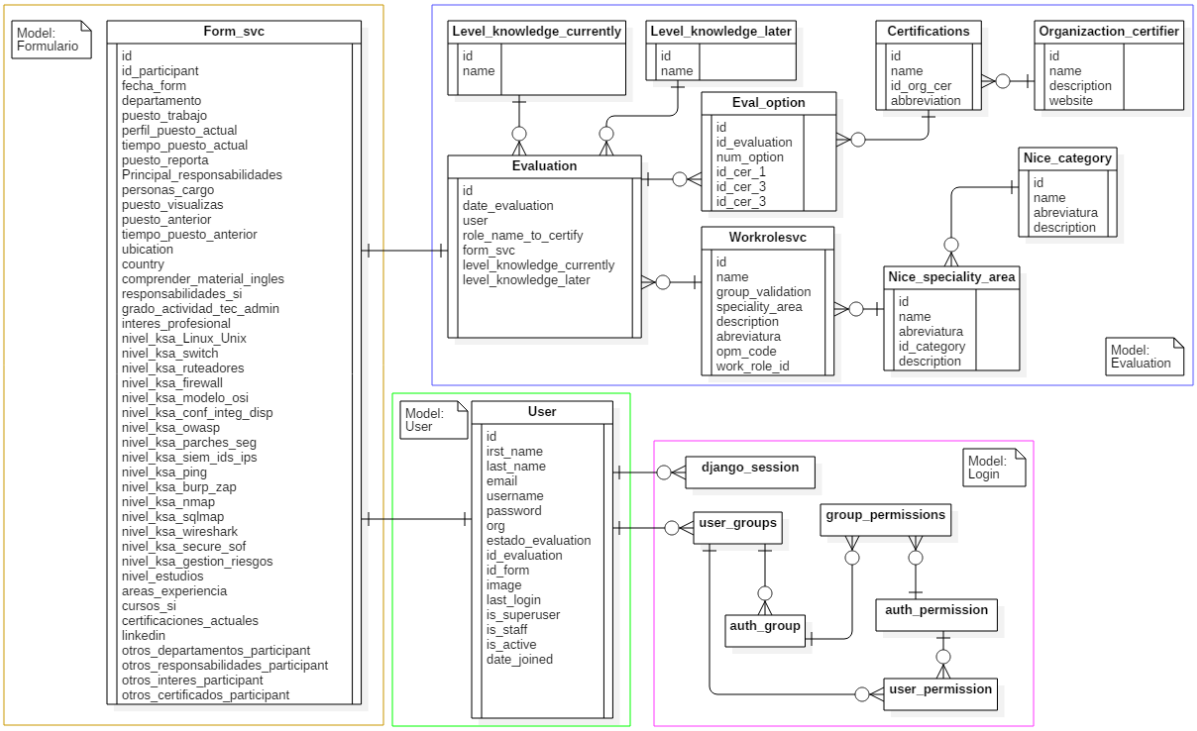

Diagrama 32. Tablas y atributos de la base de datos del "SVC"

4.6 Validación de los perfiles de conocimiento

Basados en la información obtenida del llenado de los colaboradores (Tabla 7, página 52) y de las evaluaciones de los expertos en ciberseguridad (Tabla 8, página 54 y Tabla 9, página 68) se realizó la siguientes propuesta de cuestionarios para validar los puntajes de cada perfil de conocimientos (véase Ilustración 2, página 66):

- Cuestionario en la definición de niveles de conocimientos por habilidades técnicas
- Propuesta de encuesta en la definición de niveles de conocimientos por experiencia y capacitación

La suma de los totales del cuestionario en la definición de niveles de conocimientos por habilidades técnicas más la propuesta de cuestionario para la determinación de los componentes de una ruta de capacitación en ciberseguridad; determinan en el perfil de conocimiento.

Es importante destacar que la idea de la determinación de puntajes a cada perfil de conocimientos y que estos puntos son establecidos por los expertos en base a la tesis de Jorge Armando Rosas Daniel con el tema de "Construcción de un modelo de lógica difusa para validación de perfiles de conocimiento de personal" [23] y la "Iniciativa Nacional para carreras y estudios de ciberseguridad" (NICCs). Los perfiles de conocimientos que se implementaron en el sistema son los siguientes (véase Tabla 19):

Tabla 19. Perfiles de conocimientos y su equivalencia.

No.	Nombre de perfil	Equivalencia
0	No comprende	No comprende
1	Pre-Junior	Básico
2	Junior	Intermedio
3	Semi - senior	Avanzado
4	Senior	Experto

Importante: el perfil de conocimiento, en este proyecto, es el nivel de competencia del colaborador en el área de la ciberseguridad.

4.6.1 Niveles de conocimientos por habilidades técnicas

En esta propuesta es un cuestionario para la definición de niveles de conocimientos por habilidades técnicas, el cual deberá ser completado por el experto en ciberseguridad.

Cada una de las siguientes preguntas ayudan a determinar el nivel de conocimientos técnicos que requiere un colaborador para ser considerado en uno de los siguientes perfiles del área de la ciberseguridad: básico (Junior, véase Tabla 21**¡Error! No se encuentra el origen de la referencia.**), Intermedio (Semi – senior, véase Tabla 22), avanzado (Senior, véase Tabla 23), utilizar la Tabla 20 como referencia para los puntajes.

Tabla 20. Definición de las respuestas con su equivalencia en puntos.

Respuesta	Valor
No lo conoce	0
Lo utilizo alguna vez	1
Lo utiliza regularmente	2
Lo domina	3

Las tablas para la determinación del puntaje mínimo de conocimiento técnico requerido para el perfil de conocimiento se especifican en las siguientes páginas y cada uno de los cuestionarios de los perfiles mencionados ordenados por incisos, para su entendimiento. El inciso “A” hace referencia al cuestionario de determinación del puntaje mínimo de conocimiento técnico requerido para el perfil "junior". El inciso “B” hace referencia al cuestionario de determinación del puntaje mínimo de conocimiento técnico requerido para el perfil "semi - senior". El inciso “C” hace referencia al cuestionario de determinación del puntaje mínimo de conocimiento técnico requerido para el perfil "senior".

A. Contestar en la columna agregando el valor mínimo de conocimiento técnico para cada una de las cuestiones, para obtener el puntaje para el perfil “junior” (Tabla 21).

Tabla 21. Determinación del puntaje mínimo de conocimiento técnico requerido para el perfil "junior".

Intermedio (Junior)	
Conocimiento valorado	**Valor**
Comandos básicos de Linux / Unix	
Switches de red	
Ruteadores de red	
Firewalls	
Modelo OSI de ISO	
Conceptos de seguridad como: confidencialidad, integridad y disponibilidad.	
OWASP top 10	
Parches de seguridad	
SIEM, IDS, IPS	
Ping	
Burp, ZAP	
Nmap	
SQLmap	
Wireshark	
Secure Software Development Lifecycle	
Gestión de Riesgos de TI	
Total, de puntos considerados para perfil “junior” (Intermedio):	

El total indica el puntaje técnico mínimo que debe tener un usuario para ser considerado en el perfil de conocimiento “Junior”.

B. Contestar en la columna agregando el valor mínimo de conocimiento técnico para cada una de las cuestiones, para obtener el puntaje para el perfil “semi - senior” (Tabla 22**¡Error! No se encuentra el origen de la referencia.**), utilizando los valores de la Tabla 20.

Tabla 22. Determinación del puntaje mínimo de conocimiento técnico requerido para el perfil "Semi - senior".

Avanzado (Semi - senior)	
Conocimiento valorado	**Valor**
Comandos básicos de Linux / Unix	
Switches de red	
Ruteadores de red	
Firewalls	
Modelo OSI de ISO	
Conceptos de seguridad como: confidencialidad, integridad y disponibilidad.	
OWASP top 10	
Parches de seguridad	
SIEM, IDS, IPS	
Ping	
Burp, ZAP	
Nmap	
SQLmap	
Wireshark	
Secure Software Development Lifecycle	
Gestión de Riesgos de TI	
Total, de puntos considerados para perfil “Semi - senior” (Avanzado):	

El total indica el puntaje técnico mínimo que debe tener un usuario para ser considerado en el perfil de conocimiento “Semi - senior”.

C. Contestar en la columna agregando el valor mínimo de conocimiento técnico para cada una de las cuestiones, para obtener el puntaje para “senior” (Tabla 23), utilizando los valores de la Tabla 20.

Tabla 23. Determinación del puntaje mínimo de conocimiento técnico requerido para el perfil "senior".

Experto (Senior)	
Conocimiento valorado	**Valor**
Comandos básicos de Linux / Unix	
Switches de red	
Ruteadores de red	
Firewalls	
Modelo OSI de ISO	
Conceptos de seguridad como: confidencialidad, integridad y disponibilidad.	
OWASP top 10	
Parches de seguridad	
SIEM, IDS, IPS	
Ping	
Burp, ZAP	
Nmap	
SQLmap	
Wireshark	
Secure Software Development Lifecycle	
Gestión de Riesgos de TI	
Total, de puntos considerados para perfil “Senior” (Experto):	

El total indica el puntaje técnico mínimo que debe tener un usuario para ser considerado en el perfil de conocimiento “Senior”.

4.6.2 Niveles de conocimientos por experiencia laboral y capacitación

En esta sección se propuso un cuestionario para la definición de niveles de conocimientos por experiencia y capacitación del colaborador, el cual deberá ser completado por el experto en ciberseguridad.

Cada una de las siguientes preguntas determinan el nivel de conocimientos que requiere un colaborador para ser considerado en uno de los siguientes perfiles del área de la ciberseguridad: básico (Junior, véase Tabla 24), Intermedio (Semi – senior, véase Tabla 25), avanzado (Senior, véase Tabla 26).

Contestar en la columna agregando el valor mínimo a cada una de las cuestiones, para obtener el puntaje para “junior”, “Semi - senior” y “Senior”.

Tabla 24. Determinación del puntaje mínimo de conocimiento por experiencia laboral y capacitación requerido para el perfil "junior".

Intermedio (Junior)	
Conocimiento valorado	**Valor**
Requiere comprensión de inglés para el perfil de junior. (Si: tres puntos, No: cero puntos)	Si: _____ No: _____
Cuanto tiempo en el puesto actual requiere para el perfil de junior: 1 años: 0 puntos. 2 años: 1 punto. 3 a 4 años: 2 puntos. 5 a 6 años: 3 puntos.	Años: _____
Cuanto tiempo en el puesto anterior en algunas de las áreas de ciberseguridad requiere para el perfil de junior. **1 años:** 0 puntos. **2 años:** 1 punto. **3 a 4 años:** 2 puntos. **5 a 6 años:** 3 puntos.	Años: _____
Se requiere estudios profesionales a nivel licenciatura: Si: tres puntos. No: cero puntos	Si: _____ No: _____
Se requiere estudios a nivel de posgrado: Si: tres puntos. No: cero puntos.	Si: _____ No: _____
Se requiere alguna certificación: Si: tres puntos por cada certificación. No: cero puntos.	Si: _____ No: _____
Se requiere algún curso en el área de la ciberseguridad: Si: un punto por cada curso. No: cero puntos.	Si: _____ No: _____
Total, de puntos considerados para perfil “junior” (intermedio):	

Tabla 25. Determinación del puntaje mínimo de conocimiento por experiencia laboral y capacitación requerido para el perfil "semi - senior".

Avanzado (Semi - senior)	
Conocimiento valorado	**Valor**
Requiere comprensión de inglés para el perfil de Semi - senior. (Si: tres puntos, No: cero puntos)	Si: _____ No: _____
Cuanto tiempo en el puesto actual requiere para el perfil de Semi - senior: **1 años:** 0 puntos. **2 años:** 1 punto. **3 a 4 años:** 2 puntos. **5 a 6 años:** 3 puntos.	Años: _____
Cuanto tiempo en el puesto anterior en algunas de las áreas de ciberseguridad requiere para el perfil de Semi - senior. **1 años:** 0 puntos. **2 años:** 1 punto. **3 a 4 años:** 2 puntos. **5 a 6 años:** 3 puntos.	Años: _____
Se requiere estudios profesionales a nivel licenciatura: Si: tres puntos. No: cero puntos	Si: _____ No: _____
Se requiere estudios a nivel de posgrado: Si: tres puntos. No: cero puntos.	Si: _____ No: _____
Se requiere alguna certificación: Si: tres puntos por cada certificación. No: cero puntos.	Si: _____ No: _____
Se requiere algún curso en el área de la ciberseguridad: Si: un punto por cada curso. No: cero puntos.	Si: _____ No: _____
Total, de puntos considerados para perfil "Semi - senior" (Avanzado):	

Tabla 26. Determinación del puntaje mínimo de conocimiento por experiencia laboral y capacitación requerido para el perfil "senior".

Experto (Senior)	
Conocimiento valorado	**Valor**
Requiere comprensión de inglés para el perfil de Senior. (Si: tres puntos, No: cero puntos)	Si: _____ No: _____
Cuanto tiempo en el puesto actual requiere para el perfil de Senior: **1 años:** 0 puntos. **2 años:** 1 punto. **3 a 4 años:** 2 puntos. **5 a 6 años:** 3 puntos.	Años: _____
Cuanto tiempo en el puesto anterior en algunas de las áreas de ciberseguridad requiere para el perfil de Senior. **1 años:** 0 puntos. **2 años:** 1 punto. **3 a 4 años:** 2 puntos. **5 a 6 años:** 3 puntos.	Años: _____
Se requiere estudios profesionales a nivel licenciatura: Si: tres puntos. No: cero puntos	Si: _____ No: _____
Se requiere estudios a nivel de posgrado: Si: tres puntos. No: cero puntos.	Si: _____ No: _____
Se requiere alguna certificación: Si: tres puntos por cada certificación. No: cero puntos.	Si: _____ No: _____
Se requiere algún curso en el área de la ciberseguridad: Si: un punto por cada curso. No: cero puntos.	Si: _____ No: _____
Total, de puntos considerados para perfil "Senior" (Experto):	

Cada una de las preguntas anteriormente mostradas en las tablas (Tabla 24, Tabla 25, Tabla 26) tienen un valor diferente, ya que depende en gran media de la importancia de cada una de ellas. Descripción de cada una de ellas:

- La comprensión del inglés tiene un valor de tres puntos si la respuesta es "Si" y cero puntos si es "no."
- El tiempo en el puesto actual requerido para el perfil de "Junior", "Semi - senior", "Senior" tiene un valor referente a los años trabajados. Por ejemplo, si tiene menos de dos años trabajados el puntaje es 0, si tienen 2 años o más trabajando es un punto, si se tienen entre 3 a 4 años son 2 puntos y de 5 a 6 o más son 3 puntos. Es importante que el trabajo debe ser en el área de las TI.
- El tiempo en el puesto anterior requerido para el perfil de "Junior", "Semi - senior", "Senior" es similar al anterior.

- Los requerimientos de estudios profesionales aumentan o no el puntaje, dependiendo de la importancia para un perfil. Se agrega tres puntos si la respuesta es “Si” y cero puntos si es “no.”
- Referente al posgrado es similar a los requerimientos de estudio profesional.
- Los requerimientos de certificaciones son similares a los estudios, con la diferencia que se toman en cuenta la cantidad de certificaciones que se poseen, ya que por cada certificación que tenga se multiplica por 3, esto con referente a los participantes a quienes se les establecerán rutas de aprendizaje.
- Los cursos son similares a las certificaciones, solo que por cada curso que se tenga, se multiplica por 1.
- La última fila (total) indica el puntaje mínimo por experiencia y por capacitación obtenida que debe tener un usuario para ser considerado en el perfil de conocimiento “junior”, “Semi - senior” o “Senior”.

Para ver un ejemplo de esta propuesta y la cual se implementó en el sistema, ver la sección de anexo B de este proyecto.

4.6.3 Ejemplo de propuesta de solución de la perfilación de conocimientos

Este ejemplo muestra los resultados obtenidos de la valoración de los conocimientos técnicos, experiencia laboral y estudios mostrados en el anexo B de este proyecto. Los resultados totales obtenidos son los siguientes:

De los Conocimiento técnico:

Total, mínimo de puntos considerados para perfil “junior” (Intermedio): 17 puntos

Total, mínimo de puntos considerados para perfil “Semi - senior” (Avanzado): 28 puntos

Total, mínimo de puntos considerados para perfil “junior” (Experto): 36 puntos

De los conocimientos por experiencia laboral y capacitación:

Total, de puntos mínimo considerados para perfil “junior” (Intermedio): 2 puntos

Total, de puntos mínimo considerados para perfil “Semi - senior” (Avanzado): 10 puntos

Total, de puntos mínimo considerados para perfil “Senior” (Experto): 16 puntos

Los datos mostrados anteriormente se encuentran ordenados en la Tabla 27

Tabla 27. Totales generales de los resultados obtenidos en el ejemplo de valoración de perfiles. (Véase Anexo B)

Perfil	Valor de conocimiento técnico	Valor de conocimientos por experiencia laboral y capacitación	Total, general
No comprende			
Pre – junior (básico)			
Junior (intermedio)	17	2	**18**
Semi - senior	28	10	**38**
Senior	36	16	**52**

Los resultados muestran que para ser considerado el colaborador en perfil “Junior” se necesita tener una valoración de mínimo 18 a 37 puntos. Para ser considerado en el perfil “Semi - senior” se necesita tener una valoración de mínimo 38 a 51 puntos y para ser considerado en el perfil “Senior” se necesita una valoración de mínimo 52 puntos.

Con la puntuación obtenida se obtiene una forma de valorar los perfiles, aunque para verificar los resultados se necesita que varios expertos en ciberseguridad y que varios usuarios colaboren para confirmar esta propuesta. Por el momento es una manera de validar los conocimientos en el sistema desarrollado, pero se espera que mejore con la obtención de más datos a futuro.

4.7 Diseño de las pantallas arquitectónicas de “SVC”

El Diagrama 34 muestra el mapa general del sitio web del sistema de validación de competencias (SVC).

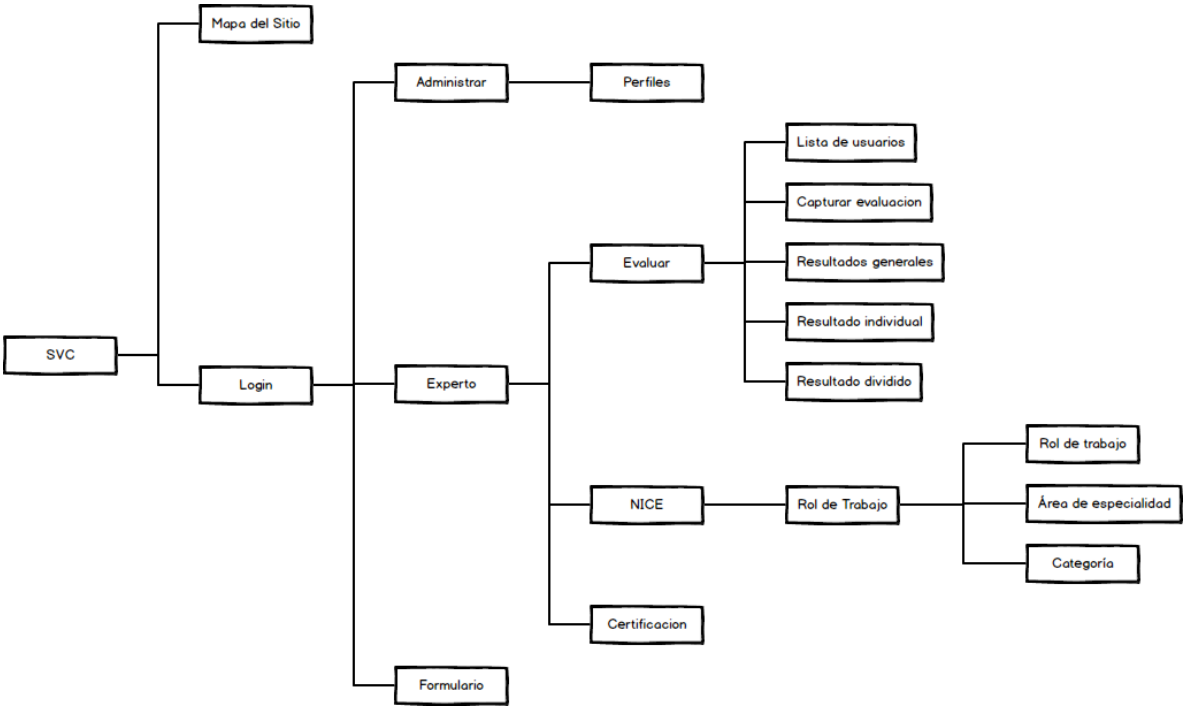

Diagrama 33. Mapa del sitio web del sistema de validación de competencias.

Login del sistema: primera pantalla para todos los usuarios antes de autentificarse. (véase Ilustración 12)

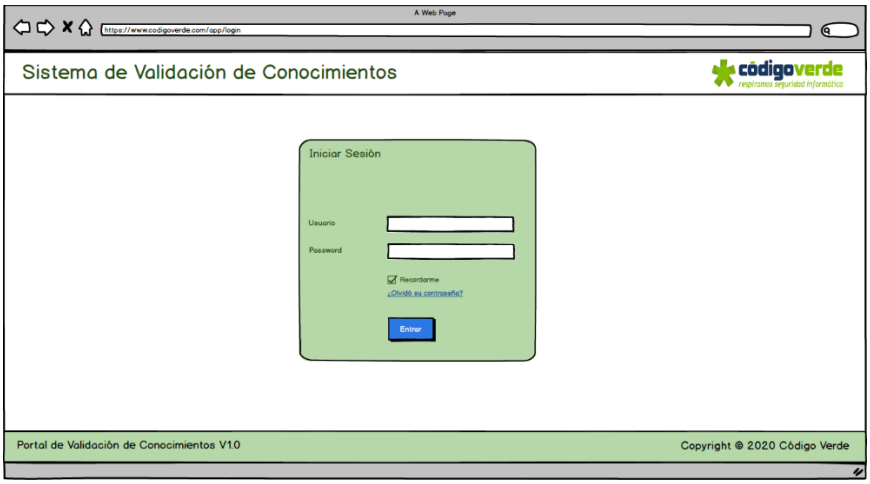

Ilustración 12. Ejemplo del login del sistema

En la pantalla mostrada en la Ilustración 13 se puede observar un ejemplo de lista de usuarios, correspondiente al panel de control del administrador.

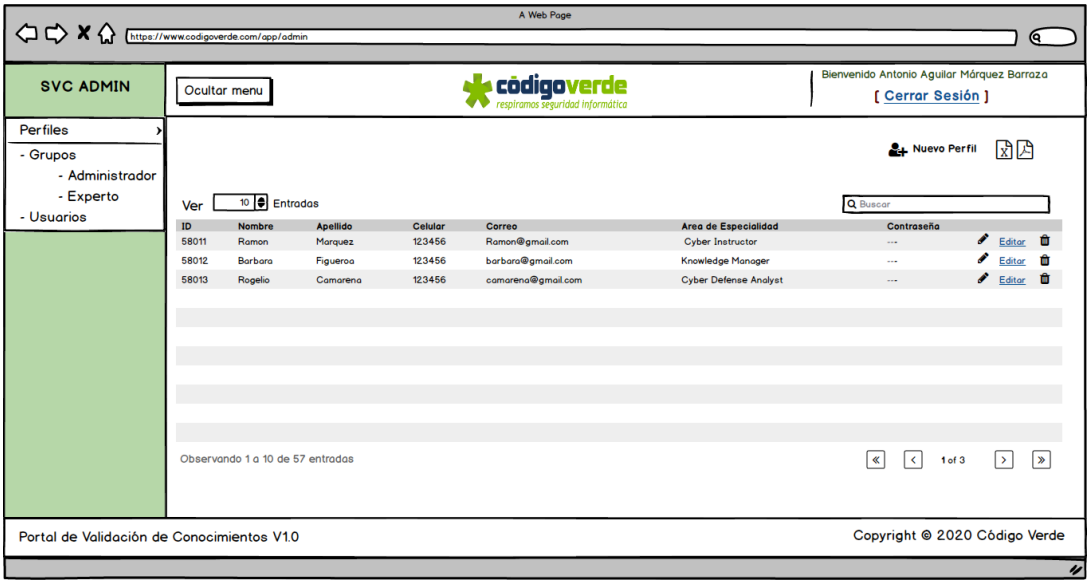

Ilustración 13. Ejemplo de la pantalla perfil en el panel de control del administrador.

En la pantalla mostrada en la Ilustración 14 se puede observar un ejemplo de lista de usuarios en el módulo del experto.

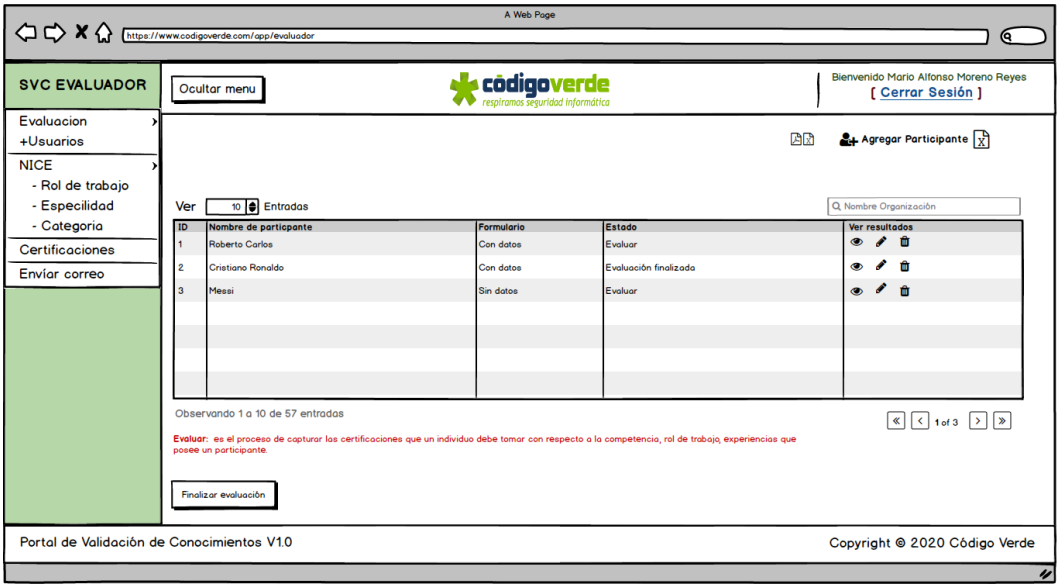

Ilustración 14. Ejemplo de la lista de usuarios.

En la pantalla mostrada en la Ilustración 15 se puede observar un ejemplo de vista de reporte de los resultados de la evaluación por colaborador.

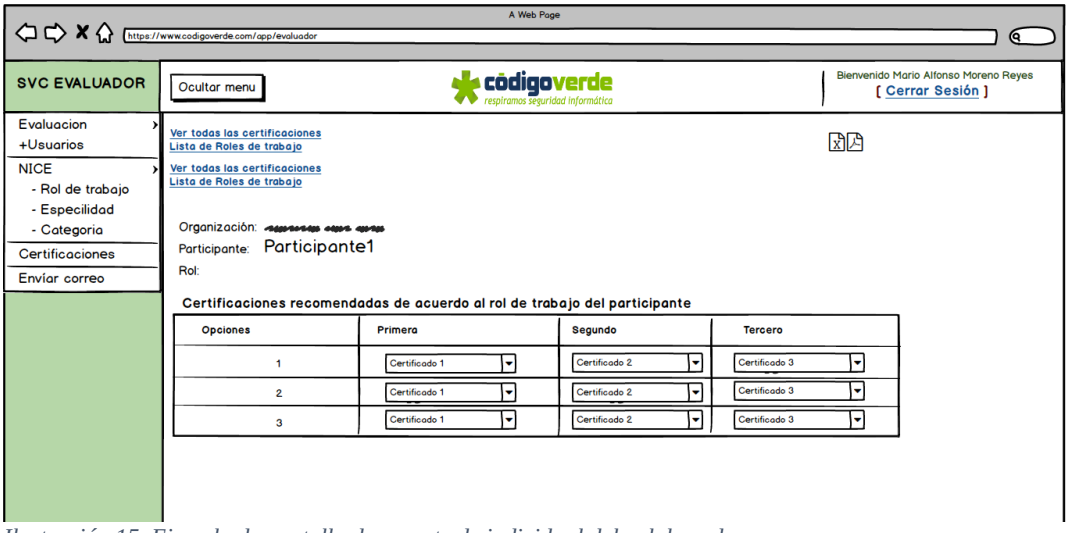

Ilustración 15. Ejemplo de pantalla de reporte de individual del colaborador.

En la pantalla mostrada en la Ilustración 16 se observa un ejemplo de vista de reporte de los resultados de las evaluaciones, ordenados por colaborador.

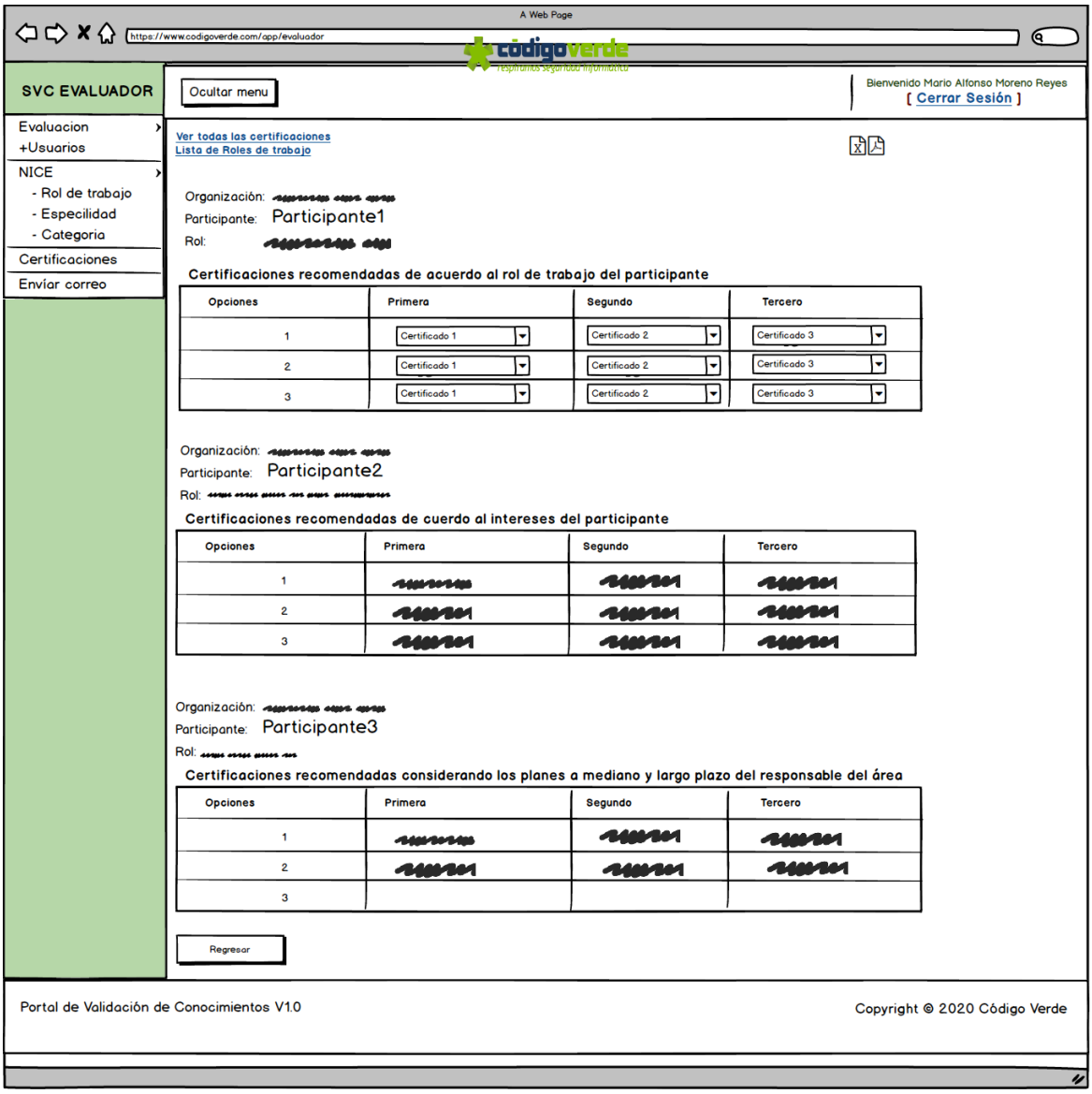

Ilustración 16. Ejemplo del reporte de los resultados ordenados por colaborador.

En la Ilustración 17 se presenta el diseño de la pantalla que muestra los resultados generales de todos los colaboradores.

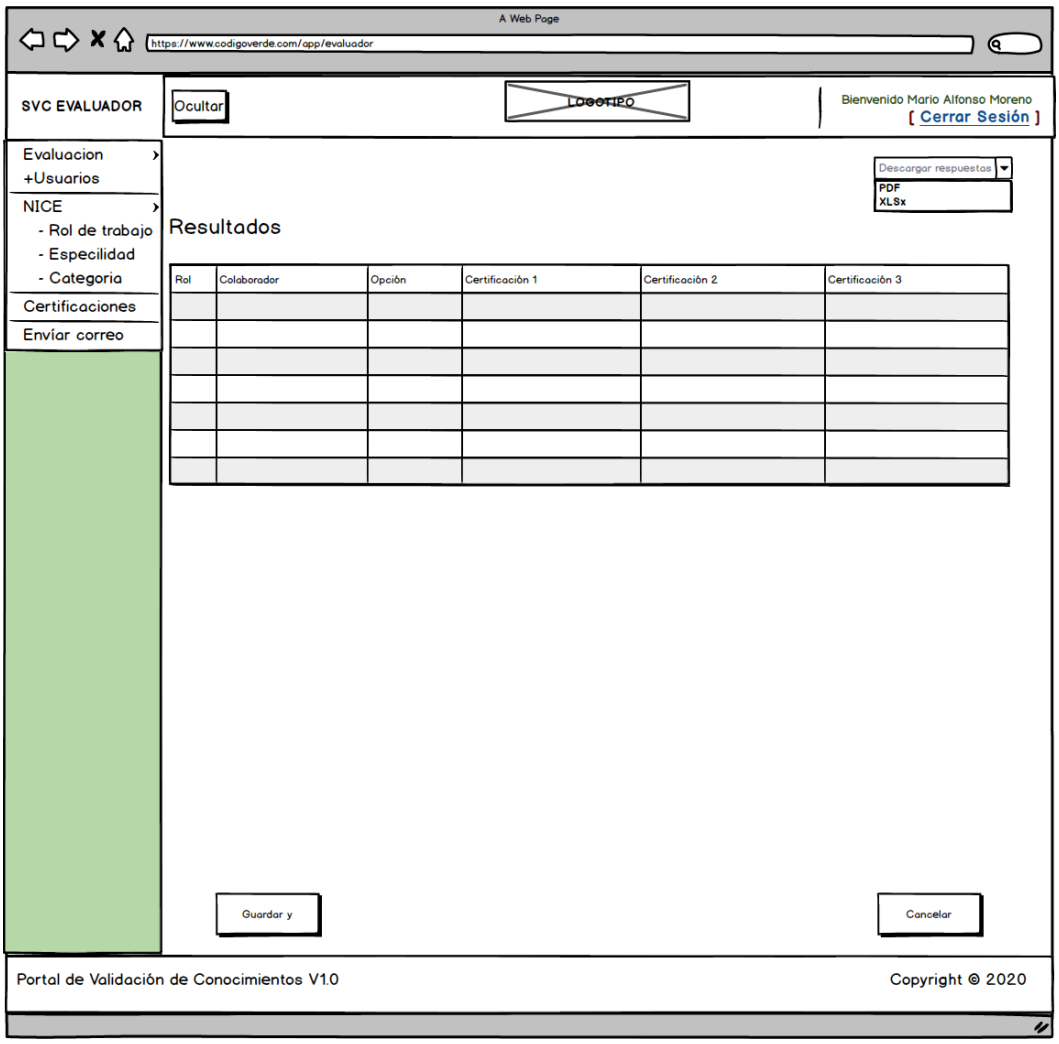

Ilustración 17. Ejemplo de la pantalla de resultados general de todos los colaboradores.

En la Ilustración 18 se muestra un ejemplo de la pantalla de evaluación de la app experto.

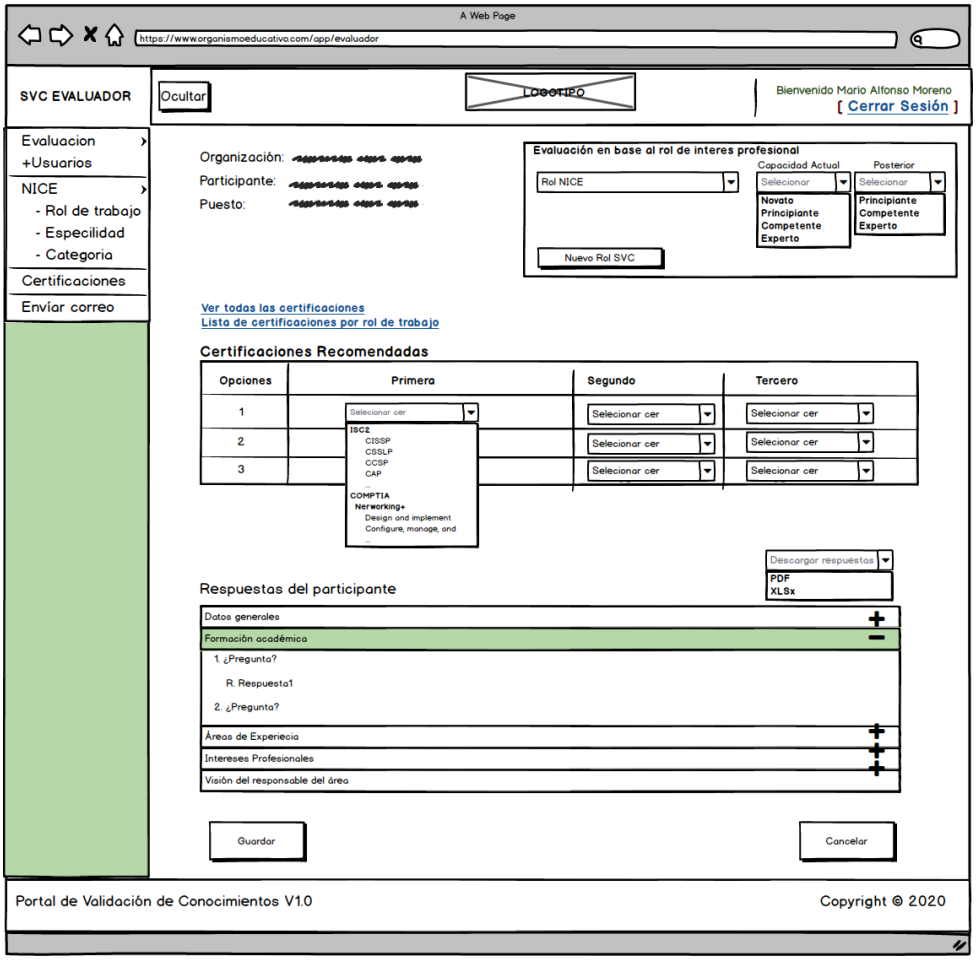

Ilustración 18. Ejemplo de la pantalla evaluación de la app experto.

5 Desarrollo del prototipo

La elaboración de prototipos de un sistema de información es una técnica valiosa para la recopilación rápida de información específica acerca de los requerimientos de los usuarios. Dentro de las características se debe especificar que este sea un prototipo que funcione, que permita probar las suposiciones formuladas por el analista y los usuarios y generalmente se debe desarrollar en un corto tiempo y sin la necesidad de invertir muchos recursos en su desarrollo [38].

Para fines del proyecto se entiende el desarrollo del prototipo como la ‘fase de programación o codificación del prototipo’ por medio de un lenguaje de programación para realizar un programa ejecutable y sin errores. El enfoque fue construir y entregar una o varias funcionalidades concisas. Al final de esta fase se obtuvo un PMV (Producto mínimo viable).

El Diagrama 34, especifica el proceso de trabajo desde el inicio del proyecto:

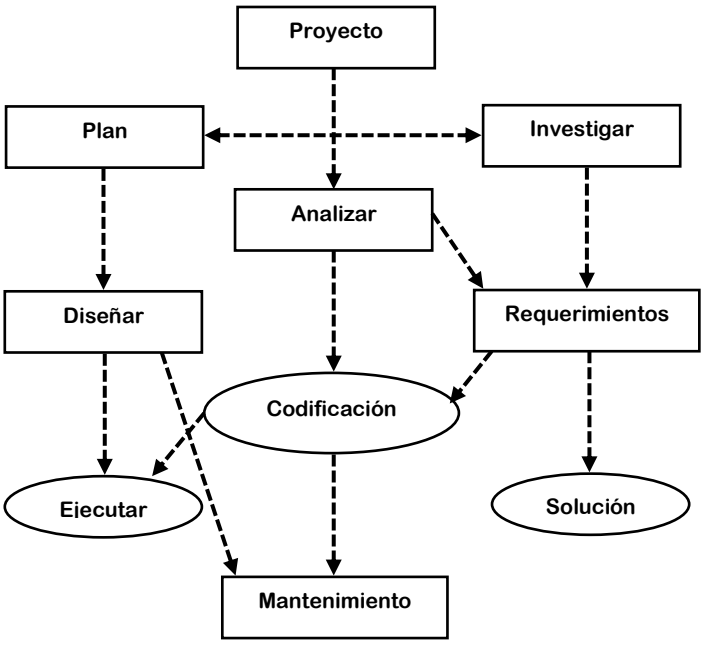

Diagrama 34. Ciclo del proyecto [36].

Llegado a este punto, ya se realizó un análisis previo del proyecto, se planteó un plan de trabajo, se especificaron directrices de investigación, se obtuvieron los requerimientos y se realizó un diseño arquitectónico del sistema, los cuales han sido un proceso iterativo entre los puntos mencionados, con el objetivo de obtener la primera versión del prototipo del sistema.

Lo que compete en este módulo es analizar más de cerca el proceso de codificación del prototipo y realización del sistema, generando el código de los componentes y procedimientos que se presentaron en el Capítulo 4, finalizando con un sistema funcional, el cual se muestra la validación del mismo en el Capítulo 6.

Nota importante: Las pantallas finales del sistema se pueden observar en el Anexo C.

5.1 Estructura del código

La estructura del código del sistema se definió respetando las responsabilidades de cada capa, establecidas en la arquitectura del sistema (véase Diagrama 23 página 92).

En la Ilustración 19 se muestran la estructura de componentes principales necesarios para el desarrollo del sistema. Para más información véase Ilustración 8, página 96)

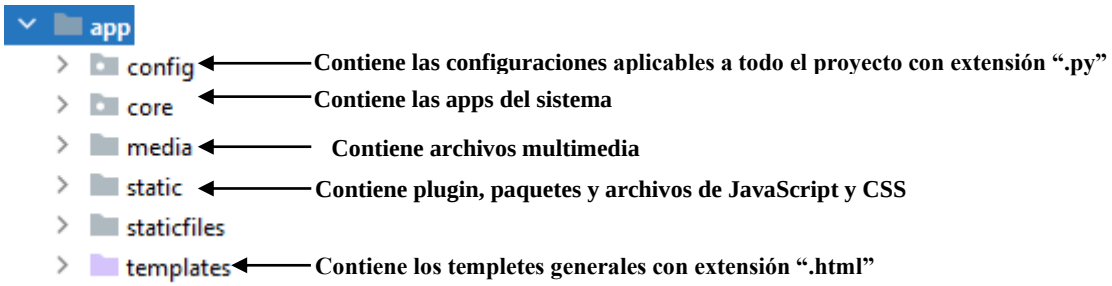

Ilustración 19. Estructura de componentes principales necesarios para el desarrollo del sistema. (Ver Ilustración 8. Pág 96.)

En la Ilustración 20 se muestra la estructura que contiene las configuraciones aplicables a todo el proyecto con extensión ".py". Para más información véase Tabla 17, página 92).

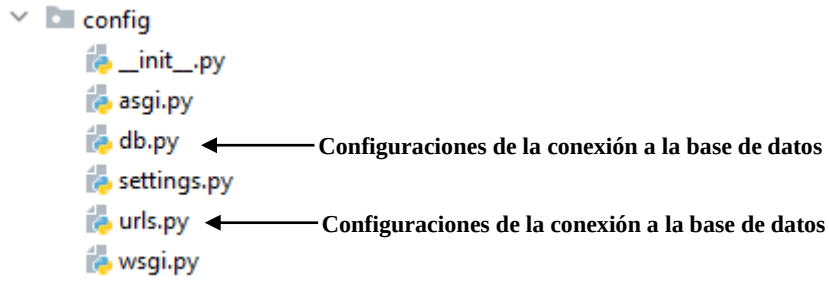

Ilustración 20. Estructura que contiene las configuraciones aplicables a todo el proyecto con extensión (véase Tabla 17, página 92).

En la Ilustración 22 se muestra la estructura de carpetas que contienen todos los recursos externos, como plugin, paquetes, archivos de JavaScript y CSS.

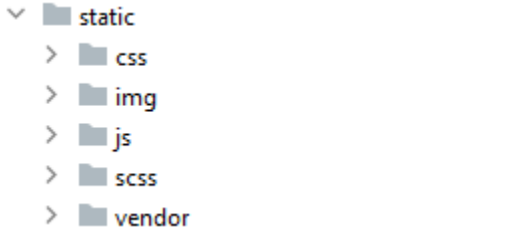

Ilustración 22. Estructura que contiene los plugin, paquetes y archivos de JavaScript y CSS.

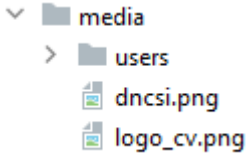

Ilustración 21. Estructura que contiene todos los archivos multimedia del sistema.

En la Ilustración 21 se muestra la estructura que contiene todos los recursos multimedia del sistema, como imágenes y videos.

La Ilustración 24 muestra la carpeta login, la cual contiene todos los archivos necesarios para el login del sistema.

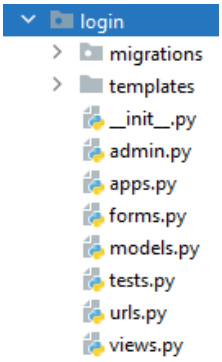

Ilustración 24. Estructura que contiene todo el código referente al login.

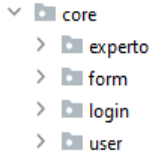

Ilustración 23. Estructura que contiene todas las aplicaciones del sistema.

La carpeta core (véase Ilustración 23) es uno de los principales archivos del sistema, ya que contiene todas las carpetas que representan una "app" o modulo del sistema.

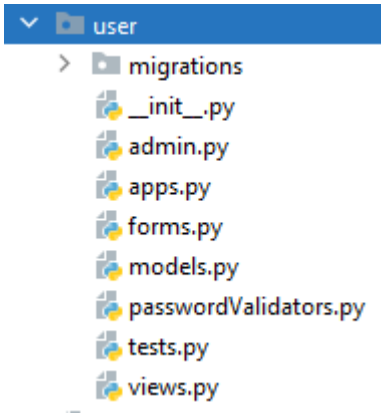

Ilustración 26. Estructura que contiene todo el código referente a los diferentes usuarios.

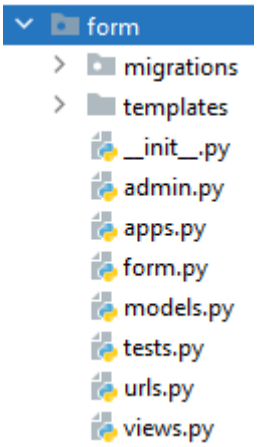

Ilustración 25. Estructura que contiene todo el código referente al formulario o cuestionario que contesta el colaborador.

La carpeta "user" (Ilustración 26) contiene todos los archivos de codificación referente al módulo de usuario. La carpeta "form" (Ilustración 25) contiene todos los archivos referentes al módulo del formulario o cuestionario, el cual contesta el colaborador.

La Ilustración 27 muestra la estructura que contiene los archivos y código referente a las actividades del experto en ciberseguridad.

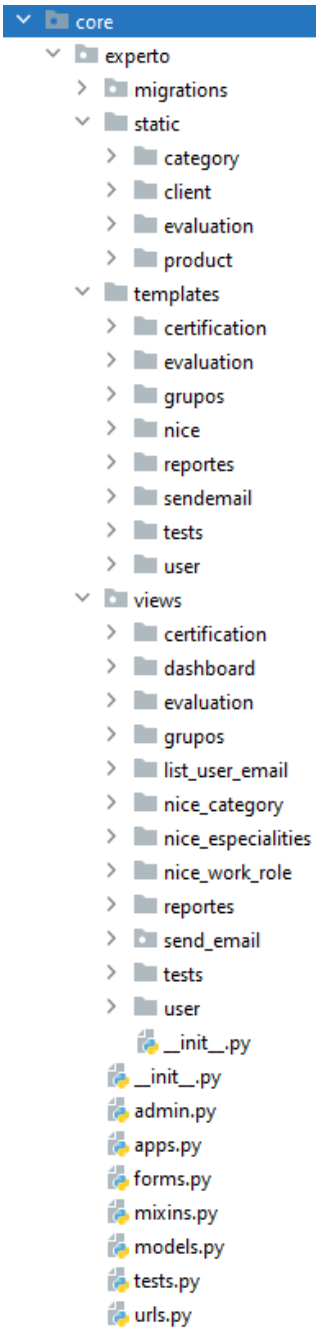

Ilustración 27. Estructura que contiene los componentes y código referente a las actividades del experto en ciberseguridad.

5.2 Las clases y métodos del sistema

En esta sección se muestran imágenes de la codificación de las clases y métodos de cada uno de los componentes del sistema. Se recuerda que los principales componentes son los Templates, Views y Models. Los códigos en las Ilustraciones 28 a 31 muestran un ejemplo de la codificación en el componente experto (véase Ilustración 11, página 99):

En la Ilustración *28* se muestra el archivo "views.py" del módulo del experto. En donde se puede observar el orden de la estructura de los componentes "views". El trayecto completo del archivo sería la siguiente app\core\experto\views\user\views.py. Cada una de las carpetas que contiene el componente "views" está estructurado de la misma forma.

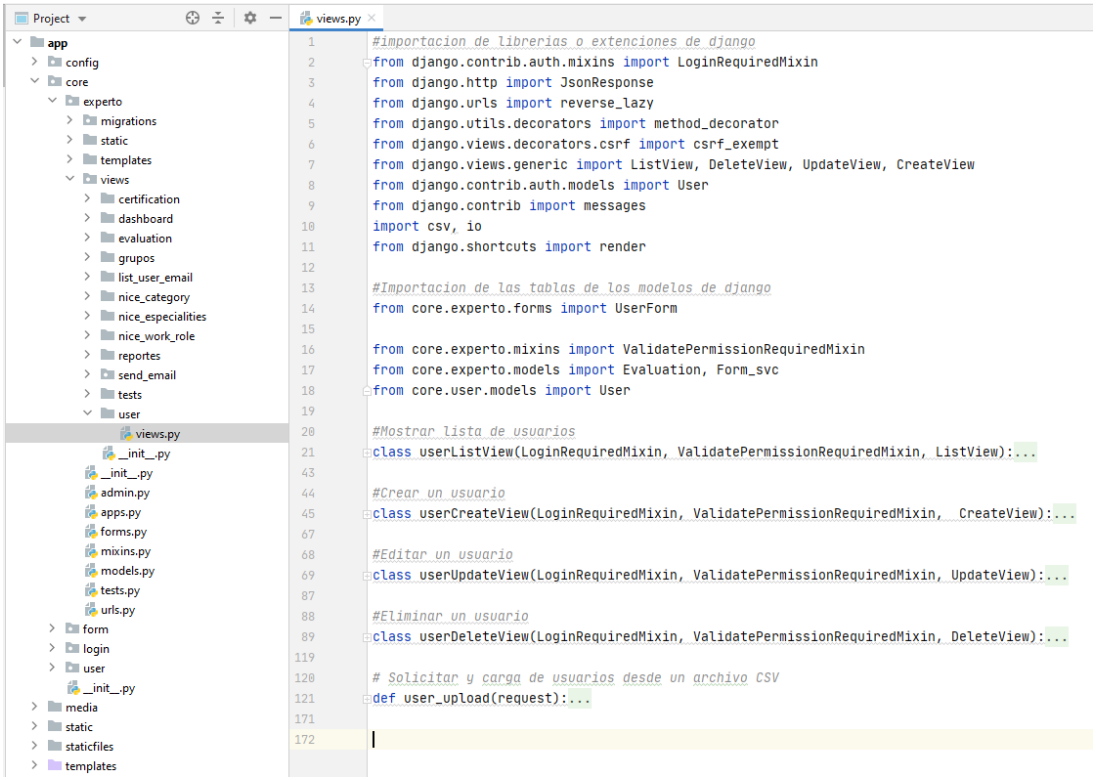

Ilustración 28. *Codificación de la vista user (views.py) perteneciente al componente experto.*

En la Ilustración 29 se puede observar un archivo con extensión “html” en la carpeta user de los templates del módulo experto, donde su ubicación exacta seria app\core\experto\templates\user. Este es un ejemplo de la estructura de los Templates.

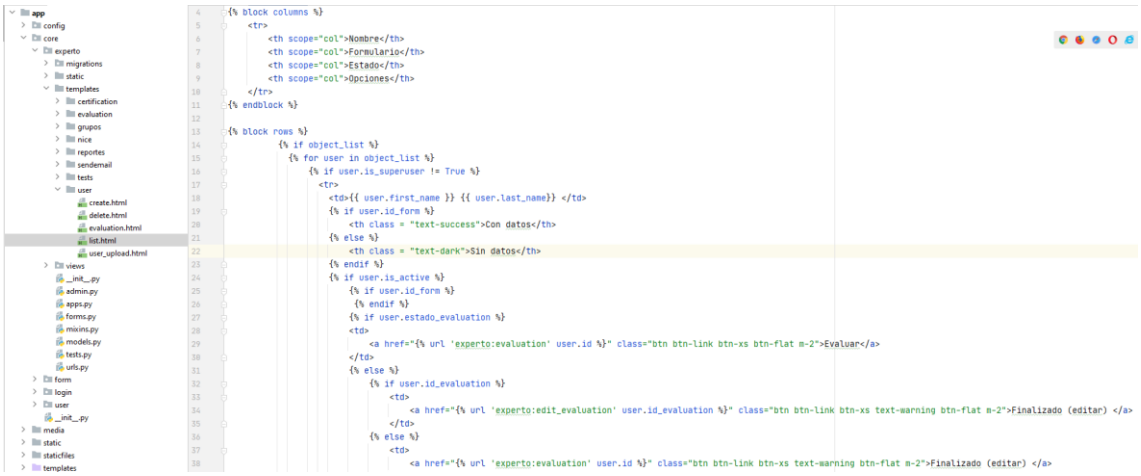

Ilustración 29. Codificación del template lista de usuarios (list.html) perteneciente al componente experto.

En la Ilustración 30 se puede observar un archivo con extensión “.py” en el módulo experto, donde su ubicación exacta seria app\core\experto\form. Este es un ejemplo de la estructura base del módulo experto. En el código se pueden ver las clases ordenadas y paqueterías importadas necesarias para su funcionamiento.

Ilustración 30. Codificación del forms del componente experto.

En la Ilustración 31 se puede observar el archivo “model.py”, el cual contiene todas las clases y atributos del modelado de los datos del sistema, que en fin y en cuenta son utilizados para crear las tablas en la base de datos.

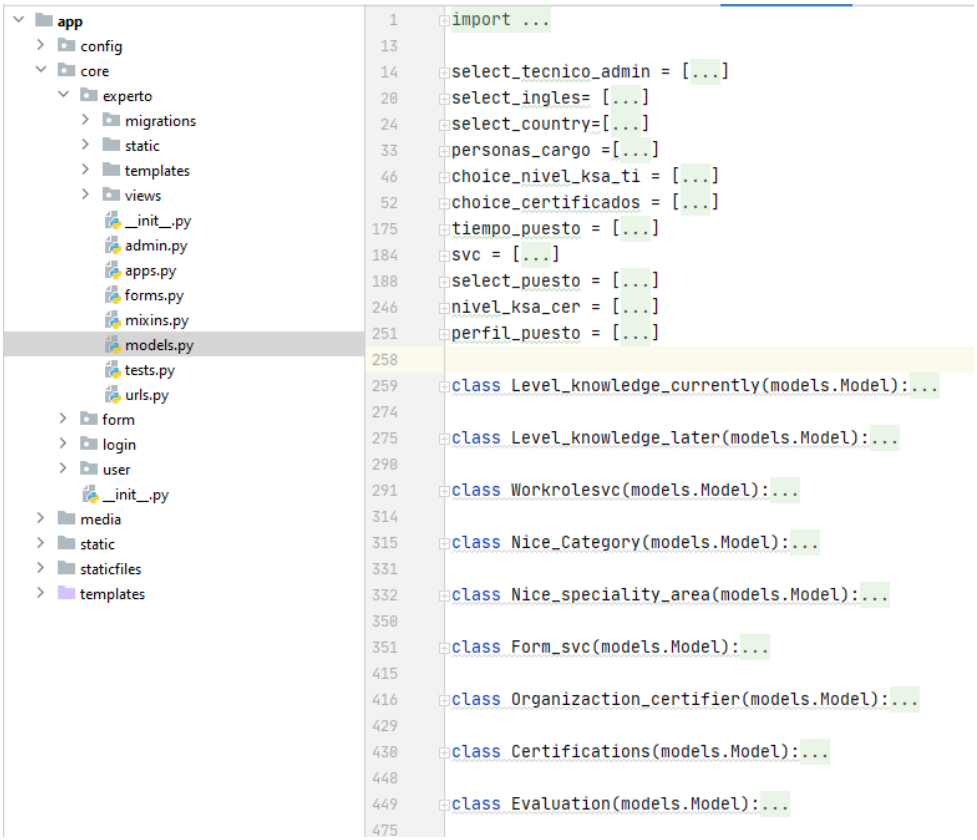

Ilustración 31. Codificación del models del componte experto.

Se recalca que en esta sección solo se muestra unos ejemplos del proyecto, por cuestión de tamaño de codificación lo cual ocuparía espació innecesario en el documento, pero si se desea ver el código completo puede solicitarlo al área de posgrado del instituto tecnológico de Hermosillo, Maestría en Ciencias de la Computación.

6 Validación del prototipo

El software desarrollado, hasta el momento, es un prototipo cuyo fin es demostrar las primeras cuatro especificaciones generales de la solución del proyecto (véase Diagrama 9, página 56), por lo que la codificación del mismo no evidencia necesariamente las técnicas adecuadas de programación, ya que se pueden detectar errores cuya presencia están justificados por la necesidad de complementación del código y la necesidad de una mejora en el modelado de la solución con respecto a la determinación de perfiles de conocimientos y rutas de capacitación. Aun así, en esta fase del proyecto se debe entregar un sistema funcional que servirá para obtener los requerimientos y retroalimentación de los usuarios o potenciales beneficiarios del mismo.

Esta validación se realizó para obtener requerimientos técnicos necesarios para avanzar en el desarrollo del sistema, siempre de cara a las necesidades del cliente; en esta fase de implementación y validación, el prototipo permitió demostrar cuáles son las ventajas y beneficios de las condiciones reales de operación; permitió detectar las deficiencias del sistema y obtener ideas que permiten mejorar el prototipo inicial, con menores fallas y mejorar la solución final del planteamiento del problema establecido en el proyecto (véase Sección 1.2, página 8); finalmente, continuando con la fase de consolidación del prototipo permitiendo medir el éxito del proyecto.

Es importante recalcar que el éxito de la validación del sistema está regido por el cliente (Código Verde S.A. de C.V.), ya que en este punto ellos son los que tienen la última palabra para que el proyecto continúe o se detenga.

Las validaciones realizadas en el prototipo son las siguientes:

1. Validación de usabilidad.
2. Validación de la propuesta de valor del sistema.

3. Validación por requerimientos funcionales y no funcionales.
4. Validación por restricciones del sistema.
5. Validación de los atributos de calidad.

Los colaboradores que participaron en el llenado del formulario del SVC y que validaron el sistema, son los mostrados en la Tabla 28**¡Error! No se encuentra el origen de la referencia.**:

Tabla 28. Número de colaboradores que apoyaron en la validación del sistema y observaciones recibidas.

Nombres	Estatus Estudiantil	Observaciones
Colaborador 1	Por egresar de la universidad	Se realizó la encuesta con supervisión, por medio de zoom meet (no realizó preguntas)
Colaborador 2	Por egresar de la universidad	Se realizó la encuesta con supervisión, por medio de zoom meet (no realizó preguntas)
Colaborador 3	Por egresar de la universidad	Se realizó la encuesta con supervisión, por medio de zoom meet (no realizó preguntas)
Colaborador 4	Por egresar de la universidad	Se realizó la encuesta con supervisión, por medio de zoom meet (no realizó preguntas)
Colaborador 5	Por egresar de la universidad	Se realizó la encuesta con supervisión, por medio de zoom meet (no realizó preguntas)
Colaborador 6	Por egresar de la universidad	Se realizó la encuesta con supervisión, por medio de zoom meet (no realizó preguntas)
Colaborador 7	Por egresar de la universidad	Sin supervisión (No hubo preguntas al contestar)
Colaborador 8	Profesional	Sin supervisión (No hubo preguntas al contestar)
Colaborador 9	Profesional	Sin supervisión (No hubo preguntas al contestar)
Colaborador 10	Profesional	Sin supervisión (No hubo preguntas al contestar)
Colaborador 11	Profesional	Sin supervisión (No hubo preguntas al contestar)
Colaborador 12	Profesional	Sin supervisión (No hubo preguntas al contestar)
Colaborador 13	Profesional	Sin supervisión (No hubo preguntas al contestar)

En la Tabla 28 se muestran la cantidad de colaboradores, el estatus educativo y las observaciones, también se muestra la forma de comunicación y como se supervisó el llenado del formulario detecciones de necesidades. En si no hubo preguntas al realizar el formulario. Por cuestiones de privacidad de los datos, no se muestran sus nombres originales,

6.1 Validación de usabilidad del sistema por parte de los colaboradores

En la Tabla 29 se muestra la escala de validación para realizar encuesta de usabilidad del SVC. Cada uno de las validaciones se encuentran enumeradas con el fin de facilitar las estadísticas de los resultados.

Tabla 29. Escala de evaluación de la usabilidad del sistema.

Escala de la evaluación				
1. Totalmente en desacuerdo	2. Algo en desacuerdo	3. Ni de acuerdo ni desacuerdo	4. Algo de acuerdo	5. Totalmente de acuerdo

Tabla 30. Resultados de la encuesta de usabilidad.

Pregunta	**No. de respuestas**	**1**		**2**		**3**		**4**		**5**	
El acceso a la página web me resulto fácil.	6									100.0%	**6**
Puedo entrar a la página web desde el primer intento, sin necesidad de insistir en más de una ocasión.	6									100.0%	**6**
Navegar dentro de la página web resulta una experiencia agradable.	6							33.3%	**2**	66.7%	**4**
El proceso de navegación dentro de ella ocurre de manera rápida y ágil.	6							33.33%	**2**	66.7%	**4**
La información publicada en la página web es de alta calidad y confiable.	6							33.33%	**2**	66.7%	**4**
El modo en que las informaciones estaban organizadas dentro de la Página Web resultó adecuado.	6					33.3%	**2**	33.33%	**2**	33.3%	**2**
Las preguntas me resultaron fáciles de comprender.	6							16.7%	**1**	83.3%	**5**
En las respuestas de selección me resulto fácil encontrar y responder la respuesta que buscaba.	6					33.3%	**2**			66.7%	**4**
En las respuestas de Casilla de verificación (checkbox) me resulto fácil encontrar y responder la respuesta que buscaba.	6							50.0%	**3**	50.0%	**3**
Me resultó muy sencillo contestar cada pregunta del cuestionario.	6							16.7%	**1**	83.3%	**5**
Promedio total por escala de evaluación						**6.62%**		**21.69%**		**71.69%**	

De los resultados mostrados en la Tabla 30, se determina que es muy fácil acceder a la página web; la navegación en la misma es buena, aunque se puede mejorar; las preguntas e información mostradas en la página web se debe mejorar, ya que solo el 33.3% indicaron

estar muy de acuerdo en el modo en que las informaciones estaban organizadas. Mejorar las opciones de verificación de casillas ya que solo el 50% está muy de acuerdo. La usabilidad del sistema es funcional y factible considerando los resultados totales de la validación y considerando que no hubo preguntas durante el llenado de los formularios (véase Tabla 31); pero también consideran que se puede mejorar y facilitar el llenado del mismo y la navegación, para ello se debe establecer como una meta de usabilidad para el sistema un promedio del 100% de respuestas en "de acuerdo" (escala 4), del total; o un 90% en muy de acuerdo (escala 5) del total de la validación del sistema.

Tabla 31. Resultados generales de la facilidad de búsqueda de las preguntas de selección.

Pregunta	No. de respuestas	1. Muy complicado	2. Algo complicado	3. Regular	4. Algo fácil	5. Muy fácil
Díganos qué tan sencillo le resulta buscar una respuesta a cada pregunta.	6			16.7%	16.7%	66.7%

De los resultados mostrado en la Tabla 31, se concluye la facilidad en que los usuarios realizaron búsquedas en las preguntas de selección; concluyendo que el 66.7% se le hizo muy fácil encontrar las respuestas, en comparación con un 16.7% que fue regular, por lo que todavía hay trabajo por hacer para mejorar las búsquedas. Para cuestiones del proyecto, se debe considerar un porcentaje del 90% en la escala 5 de validación (muy fácil).

Tabla 32. Evaluación general de los usuarios de la Página Web.

Pregunta	No. de respuestas	Muy mala	Mala	3. Regular	4. Buena	5. Muy Buena
En sentido general, ¿Cómo evaluaría usted la Página Web del sistema de validación de conocimientos?	6			16.7%	50.0%	33.3%

Los resultados mostradores en la Tabla 32 muestran que el 50% de los encuestados consideran que la página es buena, pero en contra se tiene que un 16% considera que es

regular. Se concluye de los datos obtenidos, que la página web se debe mejorar, considerando un 90% para la escala 4 (buena) o un 80% para la escala 5 (muy buena).

6.2 Validación de la propuesta de valor del proyecto

En la Tabla 33 se muestra la cantidad de usuarios que están dispuestos a recomendar el sistema desarrollado.

Tabla 33. Usuarios dispuestos a recomendar la página web.

Pregunta	No. de respuestas	No	Si
Está dispuesto a recomendar esta Página Web a un relacionado suyo.	6		100.0%

Usando como base la escala de evaluación de la usabilidad del sistema de la Tabla 33, se obtuvieron los resultados de la Tabla 34, correspondientes a la propuesta de valor del proyecto:

Tabla 34. Evaluación de la propuesta de valor del proyecto.

Pregunta	No. de respuestas	1		2		3		4		5	
Considero que lo que plantea el proyecto de SVC es beneficioso para la comunidad.	6									100.0%	6
Considero que el proyecto planteado me puede beneficiar para mis intereses profesionales.	6					16.7%	1	16.7%	1	66.7%	4
Considero que el proyecto planteado me puede ayudar a decidir un plan de capacitación para reforzar las responsabilidades actuales en mi área laboral.	6					16.7%	1	16.7%	1	66.7%	4
Promedio total por escala de evaluación						11.10		11.10		77.8	

De los resultados mostrados en la Tabla 33 se obtiene que el 100% de los participantes están dispuestos a recomendar la página web y considerando los resultados mostrados en la Tabla

34, se considera que la información en la misma es de interés a los profesionales y los estudiantes que evaluaron, además de ser beneficioso para la comunidad: aunque no todos están seguros de que le pueda ser beneficio para ellos mismo. En sí la aceptación total de la propuesta del proyecto es de un 77.8%.

6.3 Validación por requerimientos funcionales del sistema.

Tabla 35. Validación de los requerimientos funcionales del sistema.

Id	Titulo	Tipo	Aprobado (Si, No)
RF-1	Loguin	Seguridad	Si
RF-2	Encriptar password	Seguridad	Si
RF-3	Longitud de password	Seguridad	Si
RF-4	Lista de usuarios	Funcionalidad	Si
RF-5	Estatus del usuario	Usabilidad	Si
RF-6	Existencia de las respuestas al cuestionario por parte del colaborador	Usabilidad	Si
RF-7	Colores de las referencias en lista de usuarios	Usabilidad	Si
RF-8	Usuario con autorización a contestar el cuestionario	Usabilidad	Si
RF-9	Número de veces que se puede contestar el cuestionario	Modificabilidad	Si
RF-10	Relleno automático de los inputs del formulario	Usabilidad	Si
RF-11	Resultados del colaborador	Usabilidad	Si
RF-12	Exportación de los resultados	Usabilidad	Si
RF-13	Generar reporte individual del colaborador	Usabilidad, Funcionalidad	Si
RF-14	Generar reporte general de todos los colaboradores	Usabilidad, Funcionalidad	Si
RF-15	Descarga de resultados individuales.	Usabilidad	Si
RF-16	Cuestionarios o formulario	Usabilidad	Si
RF-17	Correo para el colaborador con los datos de ingreso al SVC.	Usabilidad, Funcionalidad	No
RF-18	Correo de resultado de la evaluación.	Usabilidad, Funcionalidad	No
RF-19	Listas de los elementos que componen el marco de referencia NICE.	Usabilidad	Si
RF-20	Opciones del módulo del marco de referencia NICE	Usabilidad	Si
RF-21	Opciones del módulo de usuarios	Usabilidad	Si
RF-22	Alta de usuario	Usabilidad	Si
RF-23	Alta de varios usuarios desde un archivo CSV	Usabilidad	Si
RF-24	Quienes pueden agregar usuarios de tipo colaborador	Fiabilidad	Si
RF-25	Reporte general de las evaluaciones	Usabilidad, Funcionalidad	Si
RF-26	Módulo de evaluación	Usabilidad	Si
RF-27	Opciones de la evaluación	Usabilidad	Si
RF-28	Escala de evaluación	Funcionalidad	Si
RF-29	Numero de rutas de aprendizaje	Funcionalidad	Si
RF-30	Numero de certificaciones por ruta de aprendizaje	Funcionalidad	Si
RF-31	Input de las certificaciones	Funcionalidad	Si
RF-32	Nombre del colaborador en la evaluación.	Funcionalidad	Si
RF-33	Input del rol de trabajo	Funcionalidad	Si
RF-34	Mostrar respuestas del colaborador.	Funcionalidad	Si
RF-35	Mostrar rutas de aprendizaje de manera autómata	Funcionalidad	No

En la Tabla 35 se muestra la validación de los requerimientos funcionales del sistema, en la cual la mayoría son aprobados y quedaría pendiente por desarrollar el módulo de correos para enviar al colaborador con los datos de ingreso al SVC y envió de correos informándoles que ya pueden ver sus resultados. Uno de los requisitos funcionales principales, que es la de mostrar rutas de aprendizaje de manera autómata, quedaría pendiente para otra versión del sistema, ya que se necesitan más datos para poder avanzar con dicho módulo.

6.4 Validación de las restricciones del sistema

Tabla 36. Validación de las restricciones del sistema.

Id	Tipo	Descripción	Aprobado (Si/No)
Res-1	Tecnología	El sistema debe ser desarrollado con el framework django	Si
Res-2	Seguridad	El sistema debe asegurar los datos personales de las personas.	Si
Res-3	Calendarización	El tiempo límite de entrega del proyecto será a más tardar el 01 de marzo del 2021	No
Res-4	Éticos	Se deberá almacenar permanentemente la información que no comprometa al participante, para ello se crean tablas por separado en lo que los datos se almacenan con un identificador no relacionado al participante.	Si
Res-5	Negocio	Se desea que el proyecto aporte conocimientos para la realización de la tesis, por lo que se debe adaptar a las necesidades tanto personales como de la empresa a la que se le desarrolla el sistema.	Si

En la Tabla 36 se observa que la mayoría de las restricciones del sistema fueron cumplidas en el desarrollo del proyecto; aunque el tiempo de entrega no fue el acordado. El sistema se entregó con las tecnologías planteadas, métricas de seguridad, factores éticos con el almacenamiento de los datos personales y las restricciones de negocios ideales para este proyecto. Las restricciones del sistema, si no se respetan, pueden ocasionar problemas legales y/o pérdida del cliente.

6.5 Validación de atributos de calidad.

Tabla 37. Validación de los atributos de calidad.

Driver de Atributos de calidad			
Id	**Titulo**	**Tipo**	**Aprobado (Si/No)**
RNF-1	Seguridad entre el equipo cliente y el servidor	Seguridad	Si
RFN-2	Protección de datos a personas no autorizadas	Seguridad	Si
RFN-3	Permisos de exportación de reporte general de las evaluaciones	Fiabilidad	Si
RFN-4	Permisos de acceso al sistema admin	Fiabilidad	Si
RFN-7	Permisos de acceso al formulario	Fiabilidad	Si
RFN-8	Status de usuario colaborador	Permisos	Si
RFN-9	Tipo de aplicación: web.	Usabilidad	Si
RFN-10	Disponibilidad del sistema.	Disponibilidad	Si
RFN-11	Carga de trabajo por hora.	Distribución	Si
RFN-12	Cantidad de bases de datos necesarias.	Almacenamiento	Si
RFN-13	Escalabilidad del sistema	Escalabilidad	Si
RFN-14	Tiempo de respuesta de apertura	Rendimiento	Si
RFN-15	Interoperabilidad entre sistemas operativos	Interoperabilidad	Si
RFN-16	Aplicación responsiva	Interoperabilidad	No
RFN-17	Aspectos éticos en el almacenamiento de datos personales.	Confiabilidad	Si
RFN-18	Aspectos éticos en la vista de datos personales	Confiabilidad	Si
RFN-19	Facilidad de evaluación	Usabilidad	Si
RFN-20	Búsqueda de roles de trabajo y certificaciones	Usabilidad	Si
RFN-21	Referencia que facilite la selección de una ruta de capacitación	Usabilidad	Si
RFN-22	Reportes claros	Usabilidad	Si
RFN-23	Tasa de errores cometidos por los usuarios	Fiabilidad	Si
RFN-24	Tiempo para aprender a usar el sistema	Usabilidad	Si
RFN-25	Mensajes de error	Fidelidad	Si
RFN-26	Perdidas de mensajes	Confiabilidad	Si
RFN-27	Tiempo de ejecución.	Tiempo	Si
RFN-28	Compatibilidad en los navegadores	Compatibilidad	Si
RFN-29	Documentación	Estándares	Si
RFN-30	Leyes y reglamentos de protección de datos	Legales	Si
RFN-31	Tiempo de inactividad	Seguridad	No

Con referente a la Tabla 37, la mayoría de los atributos de calidad establecidas para el desarrollo del sistema, se realizaron sin ningún inconveniente, por lo que se dio una funcionalidad viable a los objetivos del proyecto; aunque hubo dos puntos que no se resolvieron al 100%, pero estos no afectan al proyecto directamente, ya que se encuentra en la fase de entrega del prototipo.

7 Conclusiones

En este capítulo se presentan las conclusiones relacionadas con la tesis. A partir de una síntesis del trabajo realizado (7.1), se procede a comentar las aportaciones (7.2) y finalmente se proponen algunas líneas futuras de acción (7.3).

7.1 Síntesis del trabajo realizado

A partir de la propuesta de un sistema que ayude a automatizar la toma de decisiones para la asignación de rutas de capacitación en ciberseguridad considerando el perfil de conocimiento de los candidatos, se ha llevado a cabo un trabajo que busca conseguir una comprensión más completa de los procesos y manera de lograrlo.

Se logró diseñar un sistema capaz de almacenar los conocimientos de un individuo en el área de la seguridad de la información, de forma que facilite ser evaluado y con ello establecer una ruta de capacitación adecuada, de acuerdo al rol de trabajo que desarrolla o desarrollará, además de que se califica el nivel de conocimiento.

El sistema favorece en la reducción de tiempo y esfuerzo en la realización de las actividades mencionadas anteriormente. Las personas beneficiadas son los expertos en ciberseguridad, que en sí son los que toman la decisión del plan de capacitación.

La base teórica fundamental es el conocimiento del NICE Framework (v2.0) que está dividido en siete categorías y cada una subdividida en treinta y tres áreas de especialidad. Cada área de especialidad está estructurada en roles de trabajo contando actualmente con un total de cincuenta y dos; a su vez cada una define los conocimientos, habilidades y tareas necesarias para cumplir con el perfil del rol. Los perfiles de puesto que se manejan en el proyecto son: no comprende, pre-junior, junior, semi-senior y senior. Para más información ver Capítulo 2.

Del análisis del sistema se obtuvo una forma de realizar el sistema propuesto, especificando lo siguiente: (1) Establecer las instituciones certificadoras, definición de los roles de trabajo, formulario de evaluación y escala en la que se evaluará. (2) Adaptar formulario de la empresa capacitadora a un formulario web, para la obtención de datos del colaborador. (3) diseñar base de datos de conocimientos, roles de trabajo, Certificaciones, jerarquías, respuestas a formulario y conclusiones de evaluaciones realizadas. (4) Desarrollo de una aplicación web como apoyo a determinación de rutas de capacitación y almacenamiento de datos. (5) Determinación autómata de los perfiles de conocimiento y de las rutas de capacitación. Para más información del análisis del sistema ver Capítulo 3.

En el contexto general del software que se desarrolló, garantiza la seguridad de los datos, como también administra las autorizaciones para ingresar al sistema en los diferentes módulos, dependiendo de los permisos de los usuarios; se puede implementar en el sistema operativo Windows y Linux. Los usuarios que ingresen a la aplicación lo podrán hacer por medio de un portal web, para hacer uso de las diferentes funciones del mismo. El sistema web es adaptable tanto para navegadores de equipos móvil como para equipos de escritorio. Para más información de la arquitectura del sistema ver Capítulo 4.

En el capítulo de desarrollo del prototipo (Capítulo 5) se analizó más de cerca el proceso de codificación del sistema, mostrando parte del código de los componentes y procedimientos que se presentaron en el Capítulo 4, finalizando con un sistema funcional, cuya validación se muestra en el Capítulo 6.

Las validaciones realizadas en el prototipo son las siguientes: (1) Validación de usabilidad. (2) Validación de la propuesta de valor del sistema; (3) Validación por requerimientos funcionales y no funcionales; (4) Validación por restricciones del sistema; Validación de los atributos de calidad. Para más información de la validación del sistema ver Capítulo 6.

7.2 Aportaciones

Los resultados que se obtienen del presente proyecto es una recopilación de conocimientos relacionado a la seguridad de la información, perfiles de conocimientos, categorías, áreas de especialidad, roles de trabajo y certificaciones en el área de la ciberseguridad. De esta recolección de conocimientos se obtiene una organización de los datos necesarios para realizar un sistema que ayude automatizar la toma de decisiones para la asignación de rutas de aprendizaje en el área de la ciberseguridad; considerando el rol de trabajo y el perfil de conocimiento de los candidatos.

El sistema desarrollado recopila información de una persona que trabaja en el área de las TI, por medio de un formulario web. Este formulario está dividido en las siguientes categorías: datos generales, responsabilidades, estudios, experiencia laboral, conocimientos técnicos, intereses profesionales; certificaciones disponibles. La información se almacena en una base de datos.

Ya que la información de la persona se tiene, los evaluadores ingresan al sistema para evaluar los datos para determinar rutas de aprendizaje a cada uno de los usuarios que llenaron el formulario web. El sistema está formado por un módulo de evaluación, el cual muestra de una manera ordenada los siguientes datos: el nombre del participante, el rol de trabajo, el perfil de conocimiento y la información obtenida del formulario web. El rol de trabajo es modificable al igual que el perfil de conocimiento. Teniendo los datos mencionados se deciden las rutas de aprendizaje; en el mismo módulo de evaluación se encuentra una sección para ingresar mínimo una ruta de aprendizaje que consta de tres certificaciones, ordenadas de primera opción hasta la última a ser tomada por el participante. Se pueden agregar máximo tres rutas de aprendizaje a recomendar. Finalizando, la evaluación se guarda en la base de datos.

Los resultados de las evaluaciones pueden consultarse por medio de reportes individuales y reportes generales en el módulo del sistema del experto en ciberseguridad. Estos reportes se pueden descargar en formato PDF. El participante puede ver los resultados de su evaluación usando su cuenta de sesión y descargarlo si lo desea.

La aportación más significativa de este sistema es el almacenamiento de los datos de los participantes y las evaluaciones correspondientes a cada uno, pero con la opción de eliminar los datos generales para proteger la identidad de los mismo.

Los conocimientos teóricos recopilados en este proyecto, además del sistema desarrollado ayudan a establecer limitaciones e investigaciones futuras en el área de perfilado, definición de roles y certificaciones adecuados para los trabajadores de las TI.

7.3 Limitaciones e investigaciones futuras

A partir de la información y los resultados de las evaluaciones obtenidas por medio del sistema, es posible sugerir algunas líneas futuras de investigación:

- Extender los estudios de perfilación de conocimientos en el área de la ciberseguridad, incluyendo los roles de trabajo y especificaciones de los certificados recomendados para los trabajadores de las TI.
- Ampliar y enriquecer las aportaciones obtenidas por medio de nuevas características y/o diagramas. Esto se puede conseguir por medio de encuestas y/u observaciones que permitan ampliar el contenido de las aportaciones y los resultados.
- Recopilar datos para ser analizados, con el objetivo de mejoras en el sistema de validación de conocimientos en el área de la ciberseguridad. Como ejemplo se puede implementar algoritmos de aprendizaje automático, para la determinación de perfiles de conocimientos, roles de trabajo y rutas de aprendizaje.

Las líneas de investigación están limitadas de una u otra manera, a la participación de los expertos en el área de la ciberseguridad y a la información proporcionada por los participantes, que son los que llenan las encuestas. Es importante que los datos obtenidos de los participantes sean verídicos y que los expertos estén disponibles para la validación de los resultados obtenidos.

Para la definición de perfiles de conocimientos y de expertos o evaluadores, se recomienda utilizar el modelo de Rosas Daniel, J. A. (2014), Construcción de un Modelo de Lógica Difusa para Validación de Perfiles de Conocimiento de Personal [23]. El cual será de gran ayuda para definir jerarquías entre los evaluadores y definición de las rutas de aprendizaje.

El prototipo desarrollado en este proyecto es un punto de partida para el desarrollo de un sistema sólido y el desarrollo de un modelado viable en la definición de un algoritmo de IA, a partir de la retroalimentación obtenida de la determinación de perfiles de conocimientos y rutas de capacitación en el área de la ciberseguridad. Por lo que el siguiente paso recomendado como parte de la propuesta de solución en la determinación de rutas de capacitación en el área de la ciberseguridad, es el desarrollo de la aplicación web que obtenga y muestre los datos de manera clara y filtrada, utilizando un algoritmo inteligente que realice el proceso de selección de manera autómata, siguiendo con la implementación y validación del sistema resultante mediante su aplicación en casos reales.

Referencias bibliográficas

[1]. (ISC)2. (2019). Strategies for Building and Growing Strong Cybersecurity Teams. In *(ISC)2 Cybersecurity Workforce Study* (Vol. 2019). https://www.isc2.org/Research/2019-Cybersecurity-Workforce-Study

[2]. Aulbur, W., CJ, A., & Bigghe, R. (2016). Skill Development for Industry 4.0. *Roland Berger, BRICS Skill Development Working Group, India Section*, 1–50.

[3]. Cámara Nacional de la Industria Electrónica de telecomunicaciones y tecnologías de la información. (2017). Evaluación de la Ciberseguridad en México: brechas y recomendaciones en un mundo híper-conectado. https://docplayer.es/65552142-Evaluacion-de-la-ciberseguridad-en-mexico-brechas-y-recomendaciones-en-un-mundo-hiper-conectado.html

[4]. Cisco. (2018). *VNI Complete Forecast Highlights*. https://www.cisco.com/c/dam/m/en_us/solutions/service-provider/vni-forecast-highlights/pdf/South_Africa_2022_Forecast_Highlights.pdf

[5]. Código Verde. (n.d.). *Nosotros - código verde | respiramos seguridad informática*. Retrieved July 14, 2020, from https://codigoverde.com/contacto/nosotros/

[6]. *CompTIA y la Iniciativa Nacional de Educación en Ciberseguridad (NICE)*. (n.d.). Retrieved April 28, 2020, from https://certification.comptia.org/es/por-qué-certificarse/gobierno/comptia-y-la-iniciativa-nacional-de-educación-en-ciberseguridad-(nice)

[7]. Dan Shoemaker, Anne Kohnke, and K. S. (2016). *A Guide to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2.0)*. https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework

[8]. Fundación Telefónica. (2016). *Ciberseguridad, la protección de la información en un mundo digital* (Ariel S.A. (ed.)). https://www.fundaciontelefonica.com/cultura-digital/publicaciones/531/

[9]. GUZMÁN, K. (2019). *México, país con más ciberataques en el mundo*. https://www.milenio.com/negocios/mexico-pais-con-mas-ciberataques-en-el-mundo

[10]. Hypponen, M., & Nyman, L. (2017). The Internet of (Vulnerable) Things: On Hypponen's Law, Security Engineering, and IoT Legislation. *Technology Innovation Management Review*, *7*(4), 5–11. https://doi.org/10.22215/timreview1066

[11]. INEGI. (2019a). Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2018. Comunicado de prensa. In *Instituto Nacional de Estadística y Geografía (INEGI)*. https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2019/OtrTemEcon/ENDUTIH_2018.pdf

[12]. INEGI. (2019b). *Estadísticas a Propósito de las Ocupaciones Relacionadas con las Tecnologías de la Información y de la Comunicación Datos Nacionales*. *29*, 12. https://www.inegi.org.mx/contenidos/saladeprensa/aproposito/2019/OcupaTIC2019

_Nal.pdf
[13]. International Telecommunication Union. (2020). Global Cybersecurity Index (GCI) 2017. In *ITU-D Global*. https://www.itu.int/myitu/-/media/Publications/2021-Publications/Global-Cybersecurity-Index-2020.pdf
[14]. ITU News MAGAZINE. (2018). Inteligencia artificial para el bien en el mundo. *ITU News MAGAZINE*, *6*, 46. https://www.itu.int/en/itunews/Documents/2018/2018-01/2018_ITUNews01-es.pdf
[15]. Manpower, G. (2018). *Resolviendo la Escasez de Talento Resolviendo la escasez*. 4–12. www.manpowergroup.pe
[16]. Martelo, R. J., Villabona, N., & Jiménez-Pitre, I. (2017). Guía metodológica para definir el perfil profesional de programas académicos mediante la herramienta ábaco de régnier. *Formacion Universitaria*, *10*(1), 15–24. https://doi.org/10.4067/S0718-50062017000100003
[17]. Martínez, M. del P. (2019). México tendrá la demanda de 2 millones de especialistas en Ciberseguridad. *El Economista*. https://www.eleconomista.com.mx/empresas/Mexico-tendra-la-demanda-de-2-millones-de-especialistas-en-Ciberseguridad-20190607-0054.html
[18]. McKinsey&Company. (2018). *Perspectiva de ciberseguridad en México*. https://consejomexicano.org/multimedia/1528987628-817.pdf
[19]. Meushaw, R. (2012). *Developing a blueprint for a science of cybersecurity Globe at a Glance | According to the Experts | Pointers Editor ' s column* (Vol. 19, Issue 2).
[20]. Ministerio de Educación Nacional. (2013). *Lineamientos para solicitud, otorgamiento y renovación de registro calificado programas de pregrado y posgrado* (Issue 57). www.mineducacion.gov.cowww.mineducacion.gov.co/cvnewww.colombiaaprende.edu.coCalle93BNo17-49Oficina402PBX:
[21]. *Misión, visión, competencias básicas y valores fundamentales del NIST | NIST*. (n.d.). Retrieved April 28, 2020, from https://www.nist.gov/about-nist/our-organization/mission-vision-values
[22]. Organización de Estados Americanos, & Comisión Nacional Bancaria y de Valores. (2019). *Estado de la Ciberseguridad en el Sistema Financiero Mexicano*. http://www.oas.org/es/sms/cicte/documents/informes/Estado-de-la-Ciberseguridad-en-el-Sistema-Financiero-Mexicano.pdf
[23]. Rosas Daniel, J. A. (2014). *Construcción de un Modelo de Lógica Difusa para Validación de Perfiles de Conocimiento de Personal. Tesis de Maestría en Sistemas Industriales*.
[24]. Secretaria del Trabajo y Provisión social, C. N. de los S. M. (2018). *Salarios Mínimos 2018*. https://www.gob.mx/cms/uploads/attachment/file/285013/TablaSalariosMinimos-01ene2018.pdf

[25]. UIT, U. I. de T. (2008). Uit-T X.1205 Aspectos generales de la ciberseguridad. In *Sector De Normalización De Las Telecomunicaciones De La Uit* (Vol. 1205).
[26]. Wilbanks, L. (2007). Cybersecurity: Welcome to my world. *IT Professional*, *9*(2), 61–64. https://doi.org/10.1109/MITP.2007.31
[27]. World Economic Forum. (2019). *The Global Risks Report*. 1–114. http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf
[28]. L. Bass, P. Clements, R. Kazman (2003), Software Architecture in Practice, 2nd Edition, Addison Wesley
[29]. Cervantes, D. H. (n.d.). Arquitectura de Software | SG Buzz. https://sg.com.mx/revista/27/arquitectura-software
[30]. Estratégicos, I. E. de E. (2010). Líneas De Acción De La Estrategia Nacional De Ciberseguridad. In Ciberseguridad. Retos y amenazas a la Seguridad Nacional en el ciberespacio- cuaderno de estudios estrategicos. http://www.ieee.es/publicaciones-new/cuadernos-de-estrategia/2011/Cuaderno_149.html
[31]. Unión Internacional de Telecomunicaciones. (2010). Ciberseguridad definiciones y terminología relativas a la creación de confianza y seguridad. https://www.itu.int/net/itunews/issues/2010/09/pdf/201009_20-es.pdf
[32]. McKinsey Global Institute. (2015). The Internet of Things: Mapping the Value beyond the Hype EXECUTIVE SUMMARY. McKinsey & Company, June, 1–18. www.mckinsey.com/mgi.]
[33]. A. McGettrick, "Toward Effective Cybersecurity Education," IEEE Secur. Priv., vol. 11, no. 6, pp. 66–68, Nov. 2013 [Online]. Available: http://ieeexplore.ieee.org/document/6682988/
[34]. Ledo, María & Pérez, Ana. (2012). Gestión de la información y el conocimiento. Educación Médica Superior. 26. 474-484.
[35]. Carnegie Mellon University (2021). Software Engineering Institute. https://www.sei.cmu.edu/
[36]. Gutiérrez de Mesa, J. A. (2009). Planificación y gestión de proyectos informáticos. España: Servicio de Publicaciones. Universidad de Alcalá.
[37]. Silkelopez. (1 de mayo de 2013). Primera fase del ciclo de vida de los sistemas de informacion. Obtenido de https://silkeguabylopez20.wordpress.com/2013/05/01/desarrollo-de-prototipos/
[38]. Sarraipa, J., Artífcie (2019), Metodología De Evaluación De Prototipo Innovador. https://acacia.red/wp-content/uploads/2019/07/Gu%C3%ADa-Metodologi%CC%81a-de-evaluaci%C3%B3n-de-prototipo-innovador.pdf
[39]. Maigua, G. G., & López, E. F. (2012). *Buenas prácticas en la dirección y gestión de proyectos informáticos*.
[40]. Django Software Foundation. (2021). Django. https://www.djangoproject.com
[41]. Integratec (2021). Perfiles de Puesto: ¿qué son, cómo hacerlos?. https://www.integratec.com/blog/perfiles-de-puesto.html

[42]. Kambrica (2021). Niveles de seniority UX. https://www.kambrica.com/niveles-de-seniority-ux
[43]. Fundación Gustavo Bueno (2020). Conocimiento. https://www.filosofia.org/enc/ros/conoc.htm
[44]. World Economic Forum. (2020). *The Global Risks Report 2020* (Vol. 15). http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf
[45]. World Economic Forum. (2021). *The Global Risks Report 2021* (Vol. 16). http://www3.weforum.org/docs/WEF_Global_Risk_Report_2021.pdf
[46]. Martínez, M. del P. (2020). 12 hackeos o incidentes de seguridad en México. *El Economista*. https://www.eleconomista.com.mx/tecnologia/2020-en-12-hackeos-o-incidentes-de-seguridad-en-Mexico-20210102-0007.html
[47]. Martínez, M. del P. (2019). Hackeo a Pemex puede considerarse como un delito de extorsión. *El Economista*. https://www.eleconomista.com.mx/tecnologia/Hackeo-a-Pemex-puede-considerarse-como-un-delito-de-extorsion-20191113-0095.html
[48]. Banco de Mexico (2018). Información sobre los Ataques a Participantes del Sistema de Pagos Electrónicos Interbancarios (SPEI). https://www.banxico.org.mx/publicaciones-y-prensa/informes-trimestrales/recuadros/%7B86A498AE-5F8A-57CE-2C11-B5059AB9EB20%7D.pdf
[49]. Asociación de especialistas certificados en delitos finanancieros. (2017). Corea del norte y los ataques cibernéticos a instituciones financieras. https://www.delitosfinancieros.org/corea-del-norte-y-los-ataques-ciberneticos-a-instituciones-financieras/
[50]. Nehouse, W., Keith, S., Scribner, B., & Witte, G. (2017). NIST 2017 National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. *National Institute of Standards and Technology (NIST)*, *November*, 144. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf
[51]. National Initiative For Cybersecurity Careers And Studies (2021). NICCS Education and Training Catalog. https://niccs.cisa.gov/training/search
[52]. Mendoza, M. de J. V. (2013). *Construcción de un modelo para el diseño de perfiles de conocimiento*.
[53]. Instituto Nacional de Estadística y Geografía. INEGI. (2018). Sistema nacional de clasificación de ocupaciones SINCO. *Sinco*, 180. https://www.snieg.mx/DocumentacionPortal/Normatividad/vigente/sinco_2019.pdf

Anexo A. Tablas de Workforce framework for cybersecurity

Tabla 38. Categorías, áreas de especialidad y roles de trabajo propuesto por NICE Framework. [50]

	Categorías	Área de especialización NICE		Code	Roles de trabajo
1	Analyze	1	Threat Analysis (TWA)	141	Threat Warning Analyst (AN-TWA-001)
		2	Exploitation Analysis (EXP)	121	Exploitation Analyst (AN-EXP-001)
		3	All-Source Analysis (ASA)	111	All-Source Analyst (AN-ASA-001)
				112	Mission Assessment Specialist (AN-ASA-002)
		4	Targets (TGT)	131	Target Developer (AN-TGT-001)
				132	Target Network Analyst (AN-TGT-002)
		5	Language Analysis (LNG)	151	Multi-Disciplined Language Analyst (AN-LNG-001)
2	Investigate		Cyber Investigation (INV)	221	Cyber Crime Investigator (IN-INV-001)
		6	Digital Forensics (FOR)	211	Law / Counterintel Forensics Analyst (IN-FOR-001)
				212	Cyber Defense Forensics Analyst (IN-FOR-002)
3	Collect and Operate	7	Collection Operations (CLO)	311	All Source-Collection Manager (CO-CLO-001)
				312	All Source-Collection Requirements Manager (CO-CLO-002)
		8	Cyber Operational Planning (OPL)	331	Cyber Intel Planner (CO-OPL-001)
				332	Cyber Ops Planner (CO-OPL-002)
				333	Partner Integration Planner (CO-OPL-003)
		9	Cyber Operations (OPS)	321	Cyber Operator (CO-OPS-001)
4	Operate and Maintain	10	Data Administration (DTA)	421	Database Administrator (OM-DTA-001)
				422	Data Analyst (OM-DTA-002)
		11	Knowledge Management (KMG)	431	Knowledge Manager (OM-KMG-001)
		12	Customer Service and Technical Support (STS)	411	Technical Support Specialist (OM-STS-001)
		13	Network Services (NET)	441	Network Operations Specialist (OM-NET-001)
		14	Systems Administration (ADM)	451	System Administrator (OM-ADM-001)
		15	Systems Analysis (ANA)	461	Systems Security Analyst (OM-ANA-001)
5	Protect and Defend	16	Cybersecurity Defense Analysis (CDA)	511	Cyber Defense Analyst (PR-CDA-001)

		17	Cybersecurity Defense Infrastructure Support (INF)	521	Cyber Defense Infrastructure Support Specialist (PR-INF-001)
		18	Incident Response (CIR)	531	Cyber Defense Incident Responder (PR-CIR-001)
		19	Vulnerability Assessment and Management (VAM)	541	Vulnerability Assessment Analyst (PR-VAM-001)
6	Securely Provision	20	Risk Management (RSK)	611	Authorizing Official/Designating Representative (SP-RSK-001)
				612	Security Control Assessor (SP-RSK-002)
		21	Software Development (DEV)	621	Software Developer (SP-DEV-001)
				622	Secure Software Assessor (SP-DEV-002)
		22	Systems Architecture (ARC)	651	Enterprise Architect (SP-ARC-001)
				652	Security Architect (SP-ARC-002)
		23	Technology R&D (TRD)	661	Research & Development Specialist (SP-TRD-001)
		24	Systems Requirements Planning (SRP)	641	Systems Requirements Planner (SP-SRP-001)
		25	Test and Evaluation (TST)	671	System Testing and Evaluation Specialist (SP-TST-001)
		26	Systems Development (SYS)	631	Information Systems Security Developer (SP-SYS-001)
				632	Systems Developer (SP-SYS-002)
7	Oversee and Govern	27	Legal Advice and Advocacy (LGA)	731	Cyber Legal Advisor (OV-LGA-001)
				732	Privacy Compliance Manager (OV-LGA-002)
		28	Training, Education, and Awareness (TED)	711	Cyber Instructional Curriculum Developer (OV-TEA-001)
				712	Cyber Instructor (OV-TEA-002)
		29	Cybersecurity Management (MGT)	722	Information Systems Security Manager (OV-MGT-001)
				723	COMSEC Manager (OV-MGT-002)
		30	Strategic Planning and Policy (SPP)	751	Cyber Workforce Developer and Manager (OV-SPP-001)
				752	Cyber Policy and Strategy Planner (OV-SPP-002)
		31	Acquisition and Program/Project Management (PMA)	801	Program Manager (OV-PMA-001)
				802	IT Project Manager (OV-PMA-002)
				803	Product Support Manager (OV-PMA-003)
				804	IT Investment/Portfolio Manager (OV-PMA-004)
				805	IT Program Auditor (OV-PMA-005)
		32	Executive Cybersecurity Leadership (EXL)	901	Executive Cyber Leadership (OV-EXL-001)

Tabla 39. Colección de certificaciones más conocidas [51].

Id	Name	Abbreviation
1	Certified in Information Assurance (CIA)	CIA
2	Intelligence Analyst Certified (IAC)	IAC
3	Sensitive Security Information Certified (SSI)	SSI
4	American Society for Quality (ASQ) - Software Quality Engineer (CSQE)	CSAE
5	Certified Wireless Network Administrator (CWNA)	CWNA
6	Certified Wireless Network Expert (CWNE)	CWNE
7	Certified Wireless Security Professional (CWSP)	CWSP
8	Certified Wireless Technology Specialist (CWTS)	CWTS
9	Certified Wireless Analysis Professional (CWAP)	CWAP
11	CCNA-Security	CCNA-Security
12	CCNP-Security	CCNP-Security
13	SCyber	SCyper
14	A+	A+
15	Advanced Security Practitioner (CASP)	CASP
16	Certified Technical Trainer+ (CTT+)	CTT+
17	Cloud Essentials	Cloud Essentials
18	Cloud+	Cloud+
19	IT Fundamentals	IT Fundamentals
20	Linux+	Linux+
21	Mobility+	Mobility+
22	Network+	Network+
23	Project+	Project+
24	Security+	Security+
25	Server+	Server+
26	Social Media Security	Social Media Security
27	CySA+	CySA+
28	Certified Data Management Professional	CDMP
29	Department of Defense Cyber Crime Center (DC3) Certifications	DC3 Certifications
30	Defense Acquisition Workforce Improvement Act (DAWIA) Information Technology (IT) - Level I	DAWIAN-IT Level I
31	Defense Acquisition Workforce Improvement Act (DAWIA) Information Technology (IT) - Level II	DAWIAN-IT Level II
32	Defense Acquisition Workforce Improvement Act (DAWIA) Information Technology (IT) - Level III	DAWIAN-IT Level III
33	Defense Acquisition Workforce Improvement Act (DAWIA) Program Management (PM) - Level I	DAWIAN-PM Level I
34	Defense Acquisition Workforce Improvement Act nac(DAWIA) Program Management (PM) - Level II	DAWIAN-PM Level II

35	Defense Acquisition Workforce Improvement Act (DAWIA) Program Management (PM) - Level III	DAWIAN-PM Level III
36	Certified Chief Information Security Officer (CCISO)	CCISO
37	EC-Council Certified Encryption Specialist (ECES)	ECES
38	EC-Council Certified Incident Handler (ECIH)	ECIH
39	EC-Council Certified Network Defense Architect (CNDA)	CNDA
40	EC-Council Certified Secure Computer User (CSCU)	CSCU
41	EC-Council Certified Secure Programmer (ECSP)	ECSP
42	EC-Council Certified Security Analyst (ECSA)	ECSA
43	Certified Network Defender (CND)	CND
44	Certified EC Council Instructor (CEI)	CEI
45	EC-Council Certified Security Specialist (ECSS)	ECSS
46	EC-Council Certified VoIP Professional (ECVP)	ECVP
47	EC-Council Disaster Recovery Professional (EDRP)	EDRP
48	EC-Council Licensed Penetration Tester (LPT)	LPT
49	EC-Council Certified Ethical Hacker (CEH)	CEH
50	EC-Council Computer Hacking Forensic Investigator (CHFI)	CHFI
51	Licensed penetration Tester (LPT)	LPT
52	Certified Enterprise Architect (CEA)	CEA
53	FAC - Program and Project Management (FAC - P/PM) - Entry/Apprentice	(FAC -P/PM)-Entry/Apprentice
54	FAC - Program and Project Management (FAC - P/PM) - Mid-Level/Journeyman	(FAC - P/PM) - Mid-Level/Journeyman
55	FAC - Program and Project Management (FAC - P/PM) - Senior/Expert	(FAC - P/PM) - Senior/Expert
56	FAI - Certification in Program and Project Management (FAC-P/PM)	(FAC-P/PM) (entry, mid, senior, and IT core-plus)
57	Certified FISMA Compliance Practitioner (CFCP)	CFCP
58	GASF: GIAC Advanced Smartphone Forensics	GASF
59	GIAC Assessing Wireless Networks (GAWN)	GAWN
60	GIAC Certified Enterprise Defender (GCED)	GCED
61	GIAC Certified Forensic Analyst (GCFA)	GCFA
62	GIAC Certified Forensic Examiner (GCFE)	GCFE
63	GIAC Certified Firewall Analyst (GCFW)	GCFW
64	GIAC Certified Incident Handler (GCIH)	GCIH
65	GIAC Certified Intrusion Analyst (GCIA)	GCIA
66	GIAC Certified Project Manager (GCPM)	GCPM
67	GIAC Certified Penetration Tester (GPEN)	GPEN
68	GIAC Certified Perimeter Protection Analyst (GPPA)	GPPA
69	GIAC Certified UNIX Security Administrator (GCUX)	GWEB
70	GIAC Certified Web Application Defender (GWEB)	GWEB
71	GIAC Certified Windows Security Administrator (GCWN)	GCWN
72	GIAC Continuous Monitoring Certification (GMON)	GMON
73	GIAC Critical Controls Certification (GCCC)	GCCC
74	GIAC Exploit Research and Advanced Penetration Tester (GXPN)	GXPN
75	GIAC Information Security Fundamentals (GISF)	GISF
76	GIAC Information Security Professional (GISP)	GISP

77	GIAC Law of Data Security & Investigations (GLEG)	GLEG
78	GIAC Mobile Device Security Analyst (GMOB)	GMOB
79	GIAC Network Forensic Analyst (GNFA)	GNFA
80	GIAC Reverse Engineering Malware (GREM)	GREM
81	GIAC Secure Software Programmer- .NET (GSSP-.NET)	GSSP-.NET
82	GIAC Secure Software Programmer-Java (GSSP-JAVA)	GSSP-JAVA
83	GIAC Security Essentials Certification (GSEC)	GSEC
84	GIAC Security Expert (GSE)	GSE
85	GIAC Security Leadership Certification (GSLC)	GSLC
86	GIAC Systems and Network Auditor (GSNA)	GSNA
87	GIAC Web Application Penetration Tester (GWAPT)	GWAPT
88	Global Cybersecurity Program Manager (GCPM)	GCPM
89	Global Industrial Cyber Security Professional (GICSP)	GICSP
90	Information Technology Infrastructure Library (ITIL)	ITIL
91	Information Technology Infrastructure Library (ITIL) - V2 Foundations Certification	ITIL-V2 Foundations
92	ITIL v3 Foundations	ITIL v3 Foundations
93	IEEE Software Quality Engineer Certification	IEEE Software Quality Engineer Certification
94	Certified in Risk and Information Systems Control (CRISC)	CRISC
95	Certified in the Governance of Enterprise IT (CGEIT)	CGEIT
96	Certified Information Security Manager (CISM)	CISM
97	Certified Information Systems Auditor (CISA)	CISA
98	Cybersecurity Nexus CSX Certificate and CSX-P Certification	Cybersecurity Nexus CSX Certificate and CSX-P Certification
99	Certified Authorization Professional (CAP)	CAP
100	Certified Cloud Security Professional (CCSP)	CCSP
101	Certified Cyber Forensics Professional (CCFP)	CCFP
102	Certified Information Systems Security Professional (CISSP)	CISSP
103	Certified Secure Software Lifecycle Professional (CSSLP)	CSSLP
104	Information Systems Security Architecture Professional (CISSP-ISSAP)	CISSP-ISSAP
105	Information Systems Security Engineering Professional (CISSP-ISSEP)	CISSP-ISSEP
106	Information Systems Security Management Professional (CISSP-ISSMP)	CISSP-ISSMP
107	HealthCare Information Security and Privacy Practitioner (HCISPP)	HCISPP
108	Systems Security Certified Practitioner (SSCP)	SSCP
109	International Society of Forensic Computer Examiners (ISFCE) Certified Computer	ISFCE

110	CyberSec First Responder (CFR)	CFR
111	Certified Healthcare IS Security Practitioner (C)HISSP)	CHISSP
112	Certified Information Systems Risk Manager (C)ISRM)	CISRM
113	Certified Information Systems Security Auditor (C)ISSA)	CISSA
114	Certified Secure Web Applications Engineer (C)SWAE)	CSWAE
115	Certified Vulnerability Assessor (C)VA)	CVA
116	Certified Wireless Security Engineer (C)WSE)	CWSE
117	Information Systems Certification and Accreditation Professional (ISCAP)	ISCAP
118	ISO 27001	ISO 27001
119	ISO 22301	ISO 22301
120	ISO 20000	ISO 20000
121	ISO 31000	ISO 31000
122	CBCP	CBCP
123	CFCP	CFCP
124	MBCP	MBCP
125	CRMP	CRMP

Anexo B. Ejemplo de la propuesta de definición de perfiles de conocimiento.

Definición del perfil considerando los conocimientos técnicos.

Cada una de las siguientes preguntan ayudan a la determinan de nivel de conocimientos técnicos que requiere un colaborador para ser considerado en uno de los siguientes perfiles del área de la ciberseguridad: básico (Junior), Intermedio (Semi - senior), avanzado (Senior), utilizar la Tabla 40 como referencia para los puntajes.

Tabla 40. Definición de las respuestas con su equivalencia en puntos.

Respuesta	Valor
No lo conoce	0
Lo utilizo alguna vez	1
Lo utiliza regularmente	2
Lo domina	3

A partir de la siguiente página se muestran los cuestionarios y los resultados para la determinación de puntos necesarios en los perfiles.

A. Contestar en la columna agregando el valor mínimo de conocimiento técnico para cada una de las cuestiones, para obtener el puntaje para el perfil “junior”.

Tabla 41. Determinación de puntos necesarios en el perfil Junior, considerando los conocimientos técnicos.

Intermedio (Junior)	
Conocimiento valorado	**Valor**
Comandos básicos de Linux / Unix	1
Switches de red	2
Ruteadores de red	2
Firewalls	1
Modelo OSI de ISO	2
Conceptos de seguridad como: confidencialidad, integridad y disponibilidad.	1
OWASP top 10	0
Parches de seguridad	2
SIEM, IDS, IPS	0
Ping	3
Burp, ZAP	0
Nmap	0
SQLmap	0
Wireshark	1
Secure Software Development Lifecycle	0
Gestión de Riesgos de TI	2
Total, mínimo de puntos considerados para perfil “junior” (Intermedio): 17 puntos	**17**

El total indica el puntaje técnico mínimo que debe tener un usuario para ser considerado en el perfil de conocimiento “Junior”.

B. Contestar en la columna agregando el valor mínimo de conocimiento técnico para cada una de las cuestiones, para obtener el puntaje para el perfil “semi - senior”, utilizando los valores de la Tabla 40.

Tabla 42. Determinación de puntos necesarios en el perfil Semi - senior, considerando los conocimientos técnicos.

Avanzado (Semi - senior)	
Conocimiento valorado	**Valor**
Comandos básicos de Linux / Unix	2
Switches de red	2
Ruteadores de red	2
Firewalls	2
Modelo OSI de ISO	2
Conceptos de seguridad como: confidencialidad, integridad y disponibilidad.	2
OWASP top 10	1
Parches de seguridad	2
SIEM, IDS, IPS	1
Ping	3
Burp, ZAP	1
Nmap	2
SQLmap	1
Wireshark	2
Secure Software Development Lifecycle	1
Gestión de Riesgos de TI	2
Total, mínimo de puntos considerados para perfil “Semi - senior” (Avanzado): 28 puntos	28

El total indica el puntaje técnico mínimo que debe tener un usuario para ser considerado en el perfil de conocimiento “Semi - senior”.

C. Contestar en la columna agregando el valor mínimo de conocimiento técnico para cada una de las cuestiones, para obtener el puntaje para “senior”, utilizando los valores de la Tabla 40.

Tabla 43.. Determinación de puntos necesarios en el perfil Senior, considerando los conocimientos técnicos.

Experto (Senior)	
Conocimiento valorado	**Valor**
Comandos básicos de Linux / Unix	3
Switches de red	3
Ruteadores de red	3
Firewalls	3
Modelo OSI de ISO	3
Conceptos de seguridad como: confidencialidad, integridad y disponibilidad.	3
OWASP top 10	1
Parches de seguridad	3
SIEM, IDS, IPS	1
Ping	3
Burp, ZAP	1
Nmap	2
SQLmap	1
Wireshark	2
Secure Software Development Lifecycle	1
Gestión de Riesgos de TI	3
Total, mínimo de puntos considerados para perfil “junior” (Experto): 36 puntos	36

El total indica el puntaje técnico mínimo que debe tener un usuario para ser considerado en el perfil de conocimiento “Senior”.

Definición del perfil considerando los conocimientos por experiencia y capacitación

Cada una de las siguientes preguntas determinan el nivel de conocimientos que requiere un colaborador para ser considerado en uno de los siguientes perfiles del área de la ciberseguridad: básico (Junior), Intermedio (Semi - senior), avanzado (Senior).

Contestar en la columna agregando el valor mínimo a cada una de las cuestiones, para obtener el puntaje para "junior", "Semi - senior" y "Senior".

Tabla 44. Determinación de puntos necesarios en el perfil Junior, considerando los conocimientos por experiencia y capacitación.

Intermedio (Junior)	
Conocimiento valorado	**Valor**
Requiere comprensión de inglés para el perfil de junior. (Si: tres puntos, No: cero puntos)	Si: _____ No: __X__
Cuanto tiempo en el puesto actual requiere para el perfil de junior: 1 años: 0 puntos. 2 años: 1 punto. 3 a 4 años: 2 puntos. 5 a 6 años: 3 puntos.	Años: _2___
Cuanto tiempo en el puesto anterior en algunas de las áreas de ciberseguridad requiere para el perfil de junior. **1 años:** 0 puntos. **2 años:** 1 punto. **3 a 4 años:** 2 puntos. **5 a 6 años:** 3 puntos.	Años: _0__
Se requiere estudios profesionales a nivel licenciatura: Si: tres puntos. No: cero puntos	Si: _____ No: ___X__
Se requiere estudios a nivel de posgrado: Si: tres puntos. No: cero puntos.	Si: _____ No: __X___
Se requiere alguna certificación: Si: tres puntos por cada certificación. No: cero puntos.	Si: _____ No: _X___
Se requiere algún curso en el área de la ciberseguridad: Si: un punto por cada curso. No: cero puntos.	Si: ___X___ No: _____
Total, de puntos mínimo considerados para perfil "junior" (intermedio): 2 puntos	2

Tabla 45. Determinación de puntos necesarios en el perfil Semi - senior, considerando los conocimientos por experiencia y capacitación.

Avanzado (Semi - senior)	
Conocimiento valorado	**Valor**
Requiere comprensión de inglés para el perfil de Semi - senior. (Si: tres puntos, No: cero puntos)	Si: ___X____ No: _____
Cuanto tiempo en el puesto actual requiere para el perfil de Semi - senior: **1 años:** 0 puntos. **2 años:** 1 punto. **3 a 4 años:** 2 puntos. **5 a 6 años:** 3 puntos.	Años: ___4_____
Cuanto tiempo en el puesto anterior en algunas de las áreas de ciberseguridad requiere para el perfil de Semi - senior. **1 años:** 0 puntos. **2 años:** 1 punto. **3 a 4 años:** 2 puntos. **5 a 6 años:** 3 puntos.	Años: ___2_____
Se requiere estudios profesionales a nivel licenciatura: Si: tres puntos. No: cero puntos	Si: ___X_____ No: _____
Se requiere estudios a nivel de posgrado: Si: tres puntos. No: cero puntos.	Si: _____ No: __X____
Se requiere alguna certificación: Si: tres puntos por cada certificación. No: cero puntos.	Si: _____ No: ___X_____
Se requiere algún curso en el área de la ciberseguridad: Si: un punto por cada curso. No: cero puntos.	Si: __X_____ No: _____
Total, de puntos considerados para perfil "Semi - senior" (Avanzado): 10 puntos	10

Tabla 46. Determinación de puntos necesarios en el perfil Senior, considerando los conocimientos por experiencia y capacitación.

Experto (Senior)	
Conocimiento valorado	**Valor**
Requiere comprensión de inglés para el perfil de Senior. (Si: tres puntos, No: cero puntos)	Si: ___X_____ No: _____
Cuanto tiempo en el puesto actual requiere para el perfil de Senior: **1 años:** 0 puntos. **2 años:** 1 punto. **3 a 4 años:** 2 puntos. **5 a 6 años:** 3 puntos.	Años: ___6_____
Cuanto tiempo en el puesto anterior en algunas de las áreas de ciberseguridad requiere para el perfil de Senior. **1 años:** 0 puntos. **2 años:** 1 punto. **3 a 4 años:** 2 puntos. **5 a 6 años:** 3 puntos.	Años: ____2_____
Se requiere estudios profesionales a nivel licenciatura: Si: tres puntos. No: cero puntos	Si: ____X_____ No: _____
Se requiere estudios a nivel de posgrado: Si: tres puntos. No: cero puntos.	Si: ____X_____ No: _____
Se requiere alguna certificación: Si: tres puntos por cada certificación. No: cero puntos.	Si: ___X_____ No: _____
Se requiere algún curso en el área de la ciberseguridad: Si: un punto por cada curso. No: cero puntos.	Si: _____ No: __X_____
Total, de puntos considerados para perfil "Senior" (Experto): 16 puntos	16

Anexo C. Pantallas del sistema de validación de conocimientos en ciberseguridad

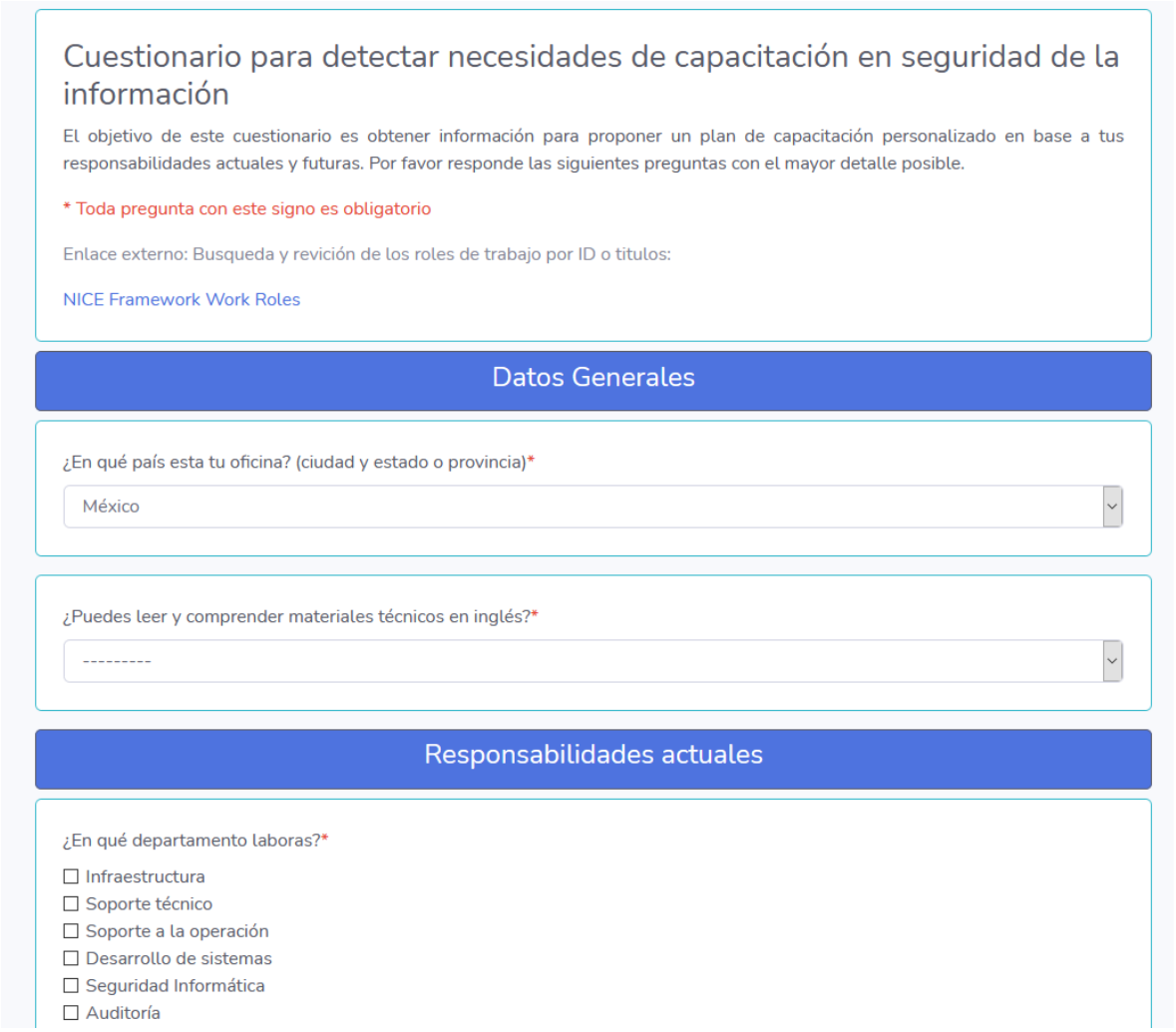

Ilustración 32. Formulario para detectar necesidades de capacitación en el área de la seguridad de la información.

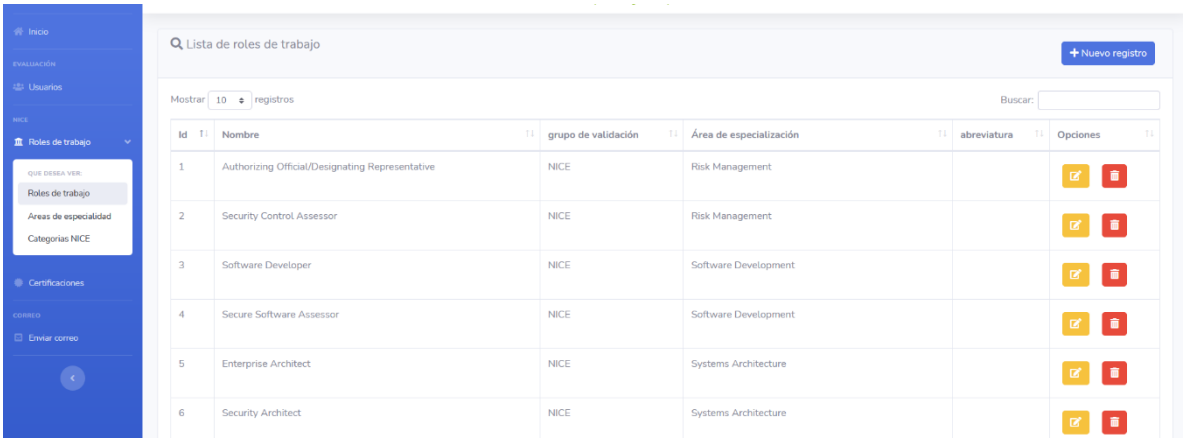

Ilustración 33. Pantalla de la lista de roles de trabajo de validación de conocimientos

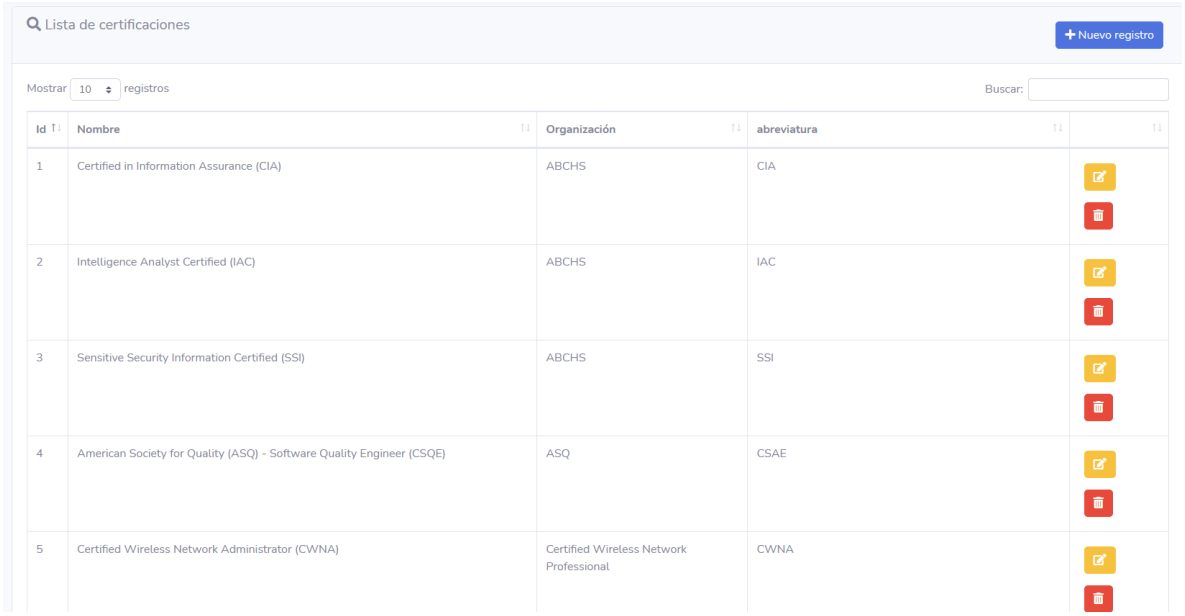

Ilustración 34. Pantalla de la lista de certificaciones.

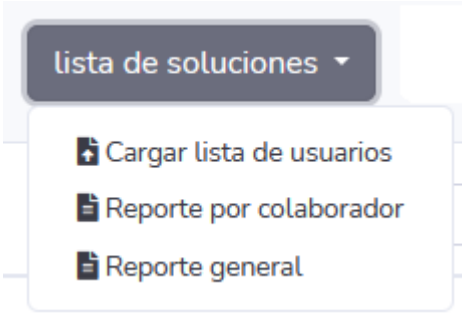

Ilustración 36. Menú de la lista de soluciones

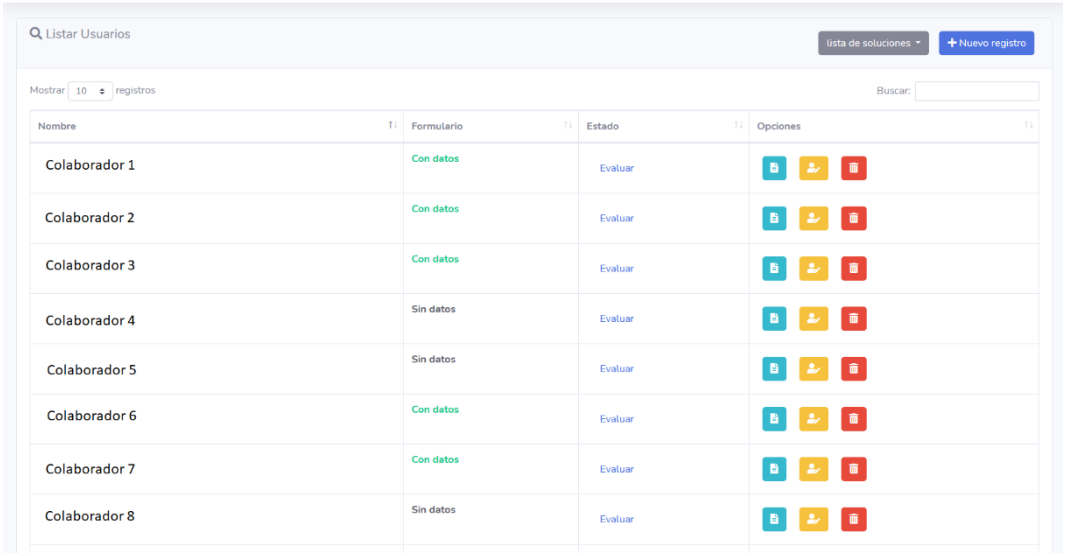

Ilustración 35. Pantalla de la lista de usuarios del sistema.

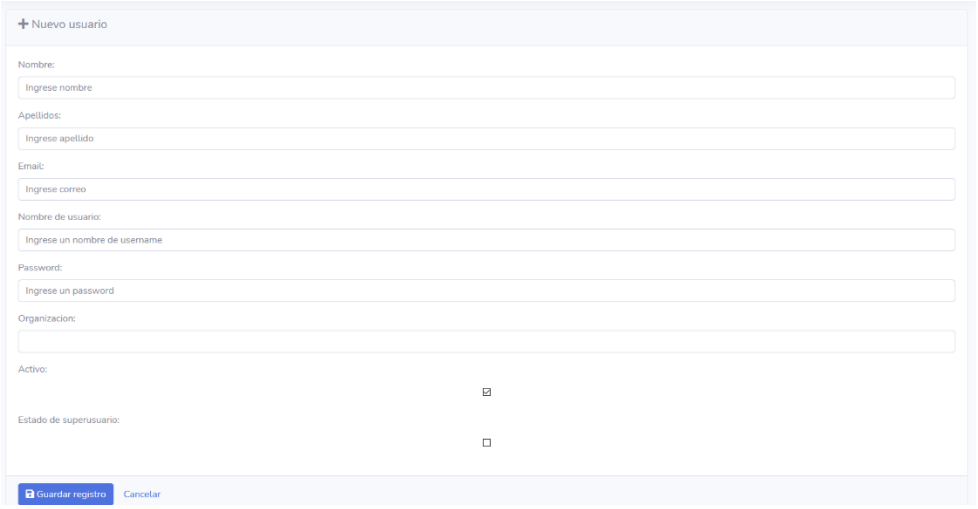

Ilustración 37. Pantalla de la creación de nuevos usuarios.

Ilustración 38. Pantalla del Loguin del sistema de validación de conocimientos.

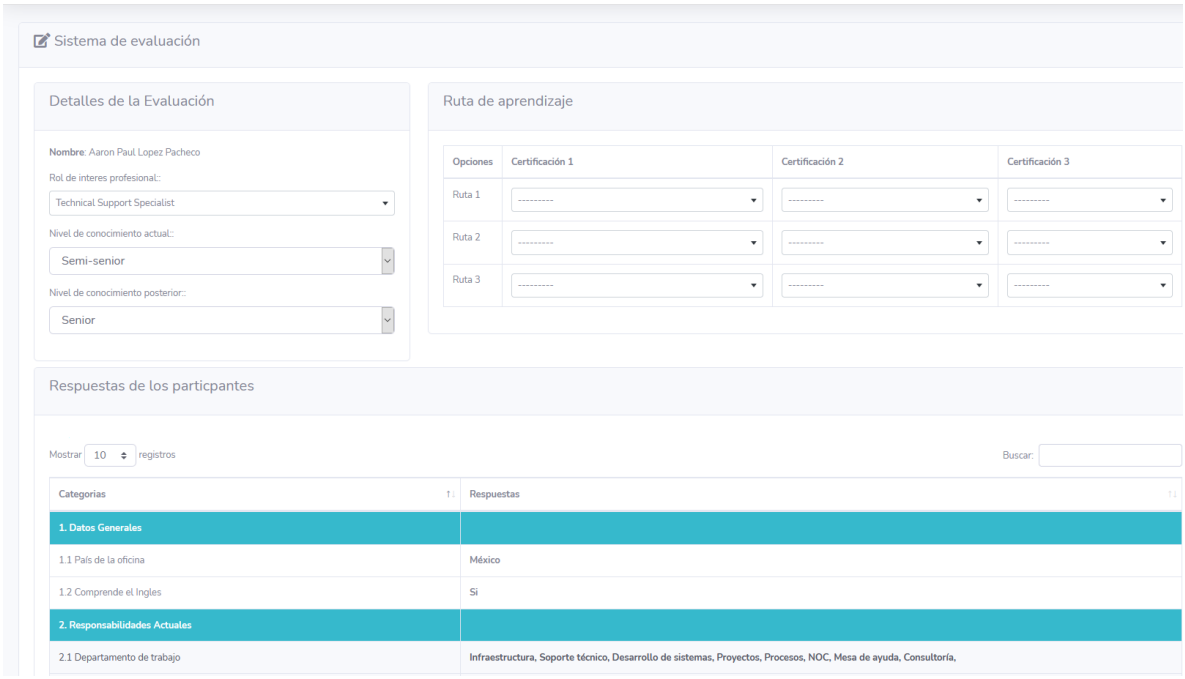

Ilustración 39. Pantalla de evaluación de los colaboradores o participantes

Anexo D. Pantallas que muestran el formulario que llena el colaborador

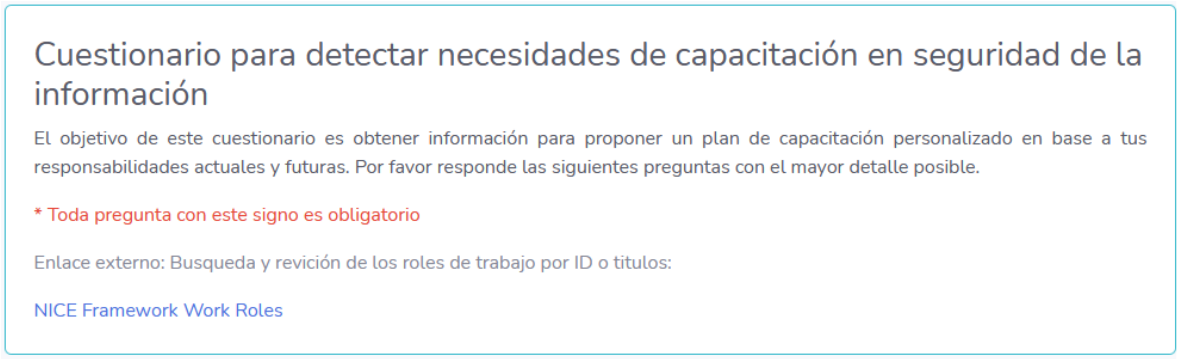

Ilustración 41. Título del formulario.

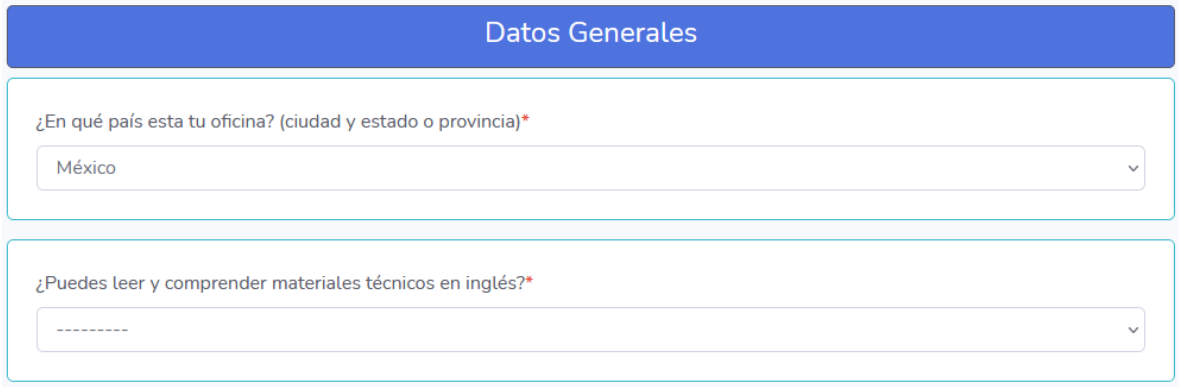

Ilustración 40. Sección de preguntas de datos generales.

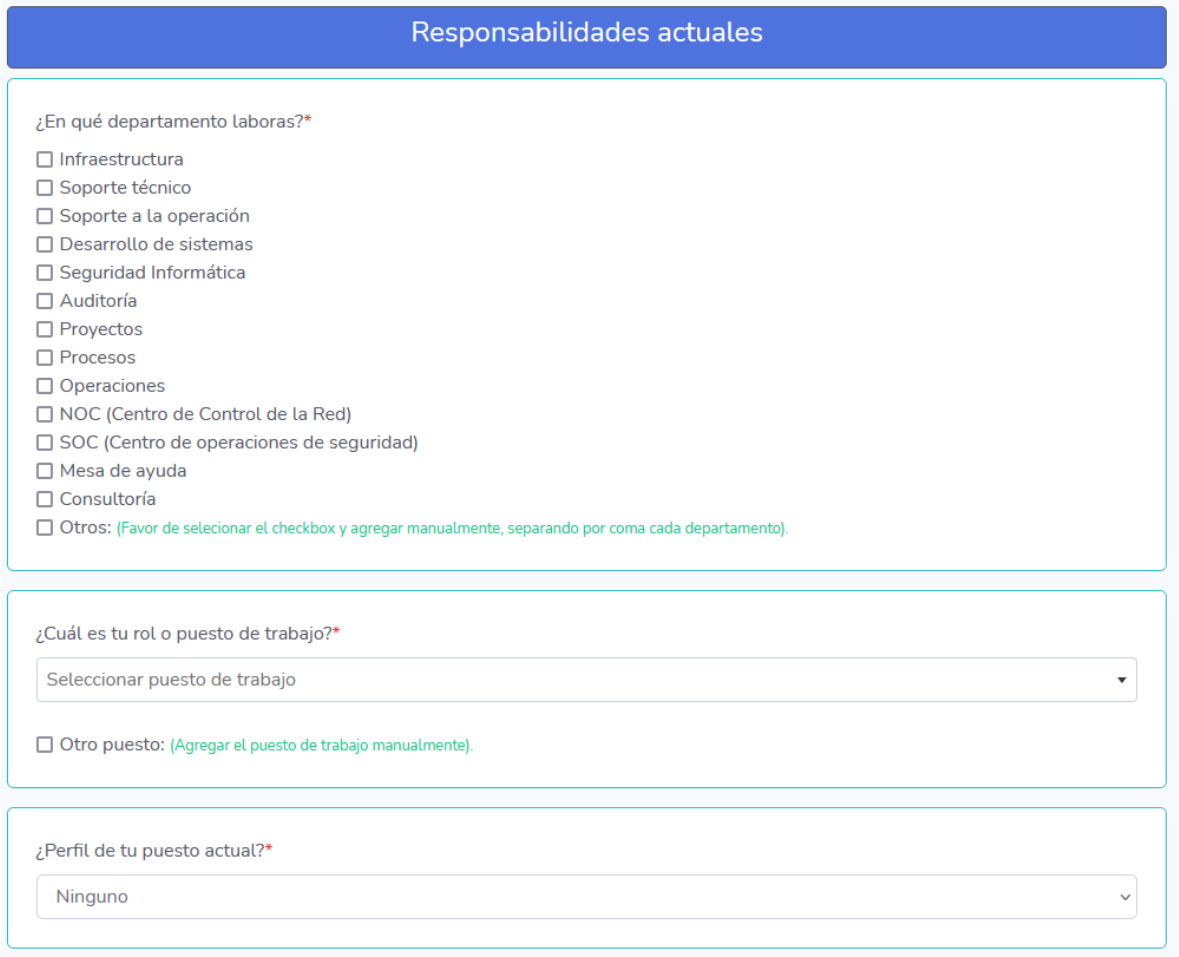

Ilustración 42. Parte 1 de la sección de responsabilidades actuales.

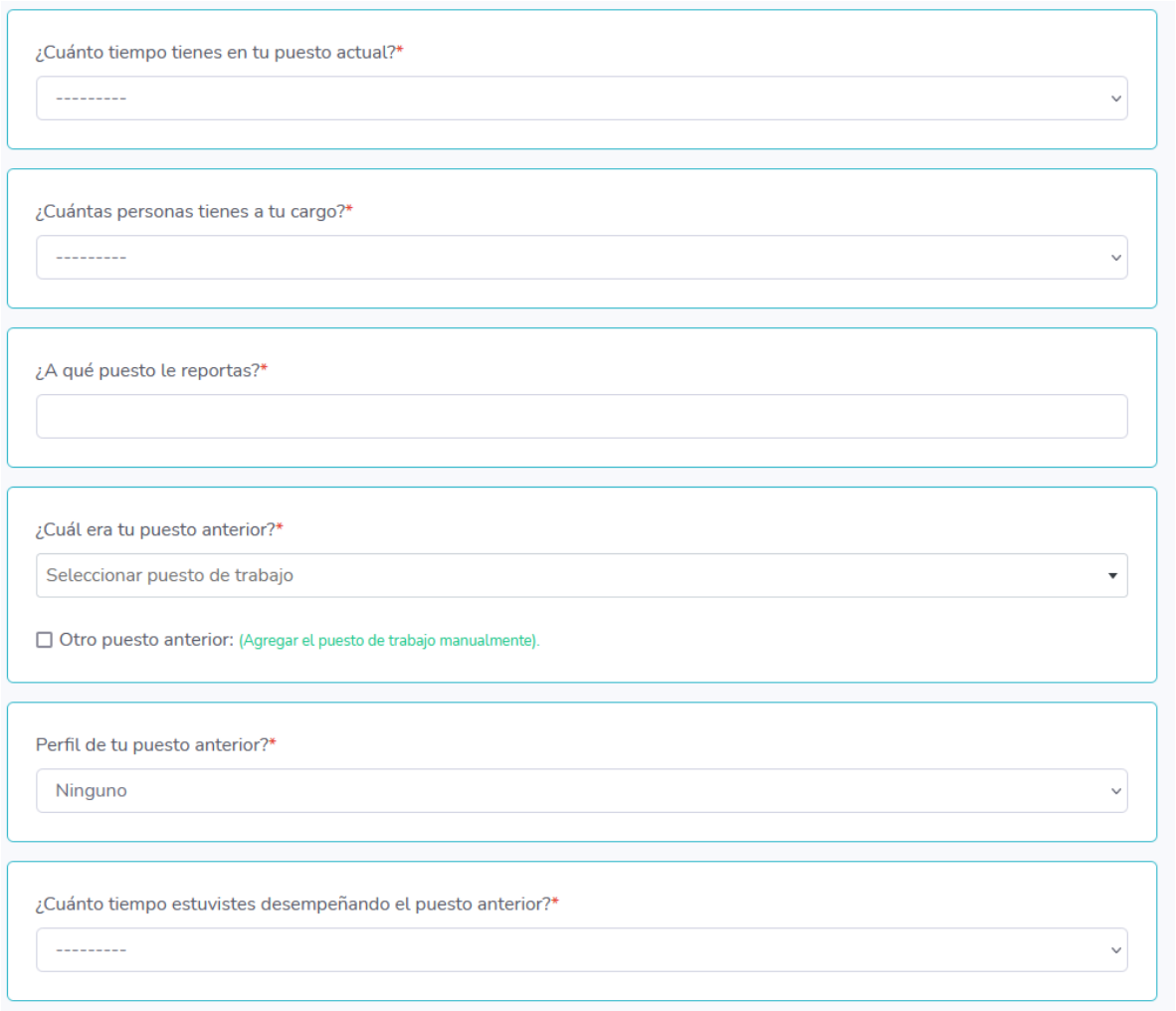

Ilustración 43. Parte 2 de la sección de responsabilidades actuales.

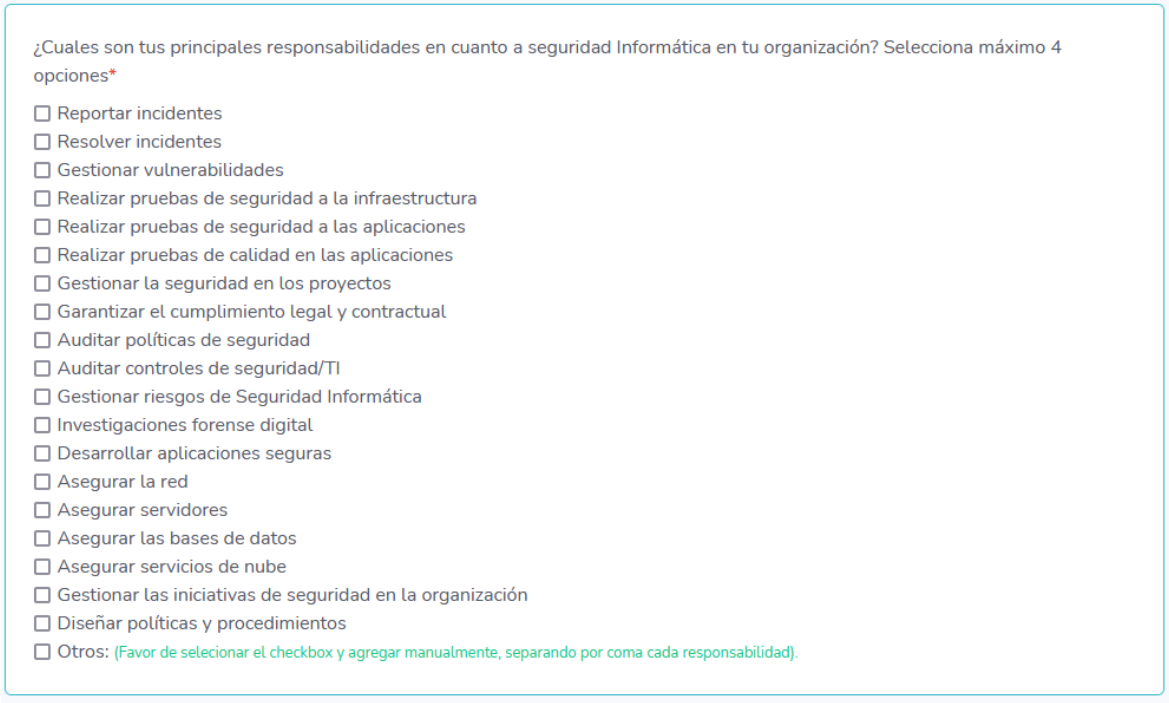

Ilustración 44. Parte 3 de la sección de responsabilidades actuales.

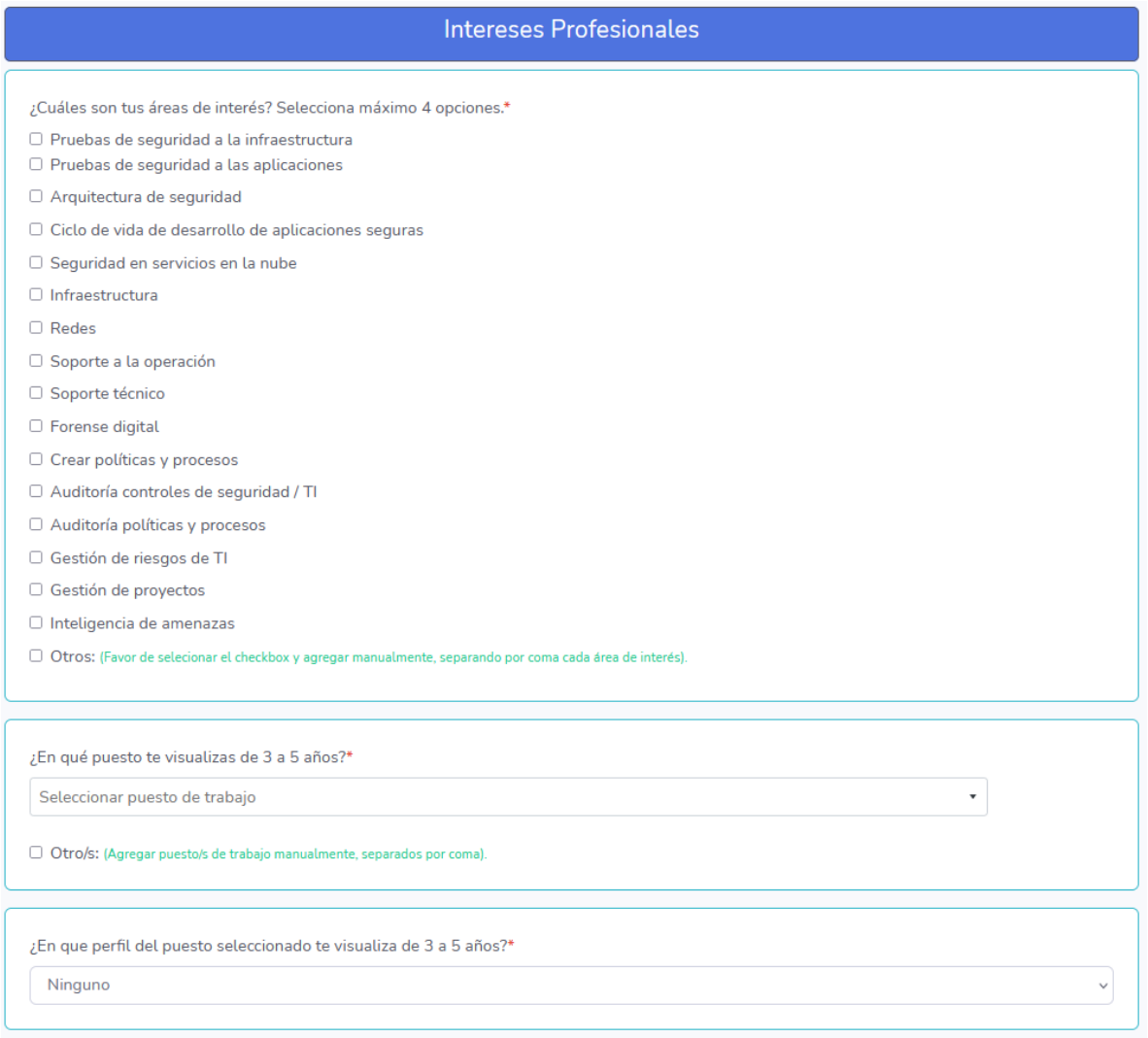

Ilustración 45. Sección de Intereses profesionales

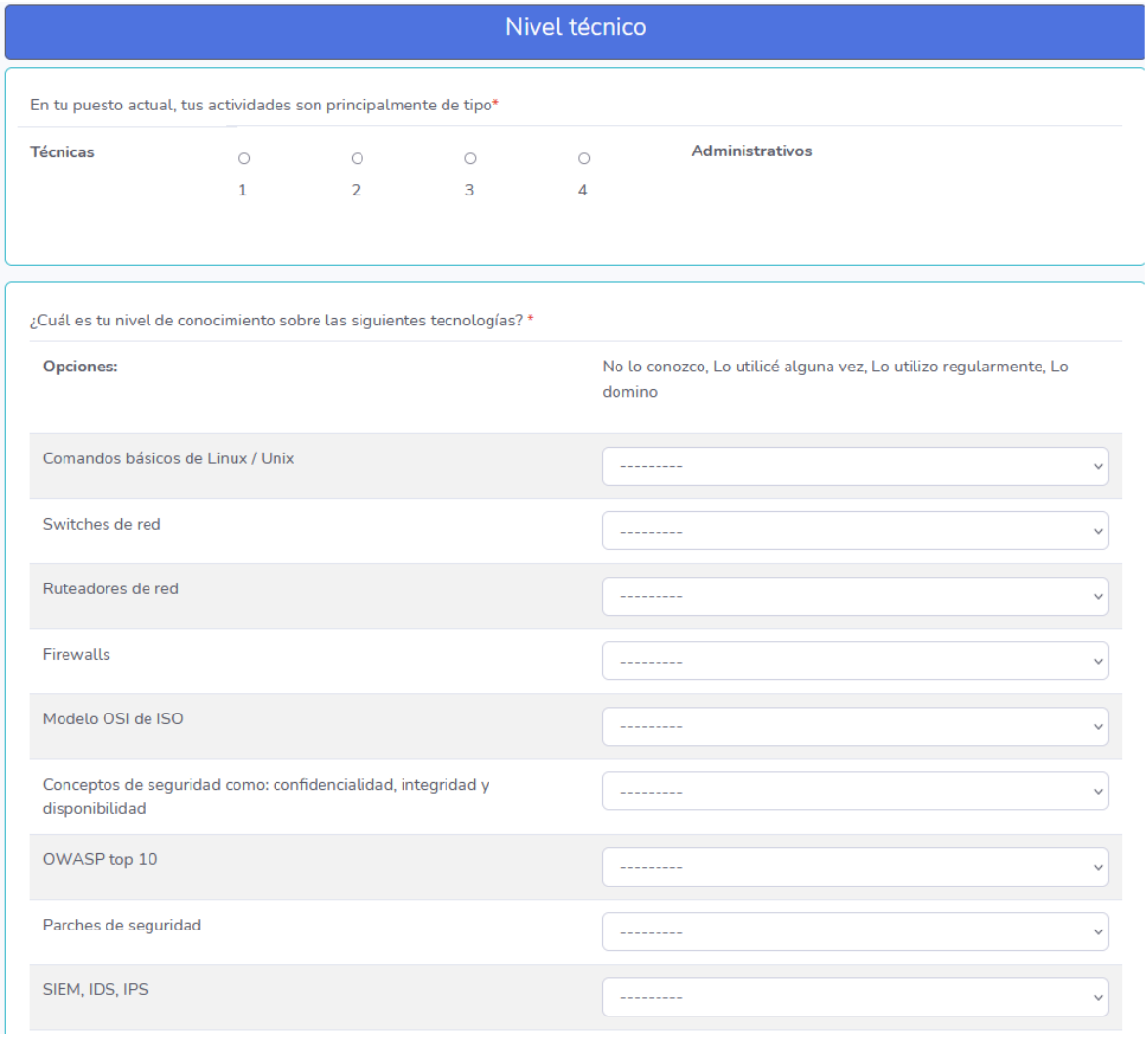

Ilustración 46. Parte 1 de nivel técnico.

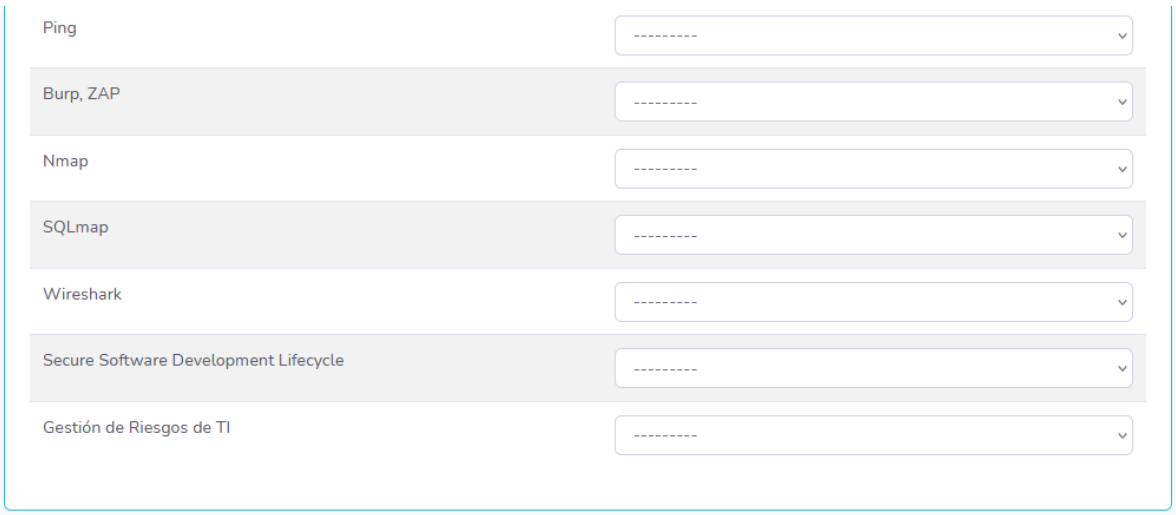

Ilustración 47. Parte 2 de nivel técnico.

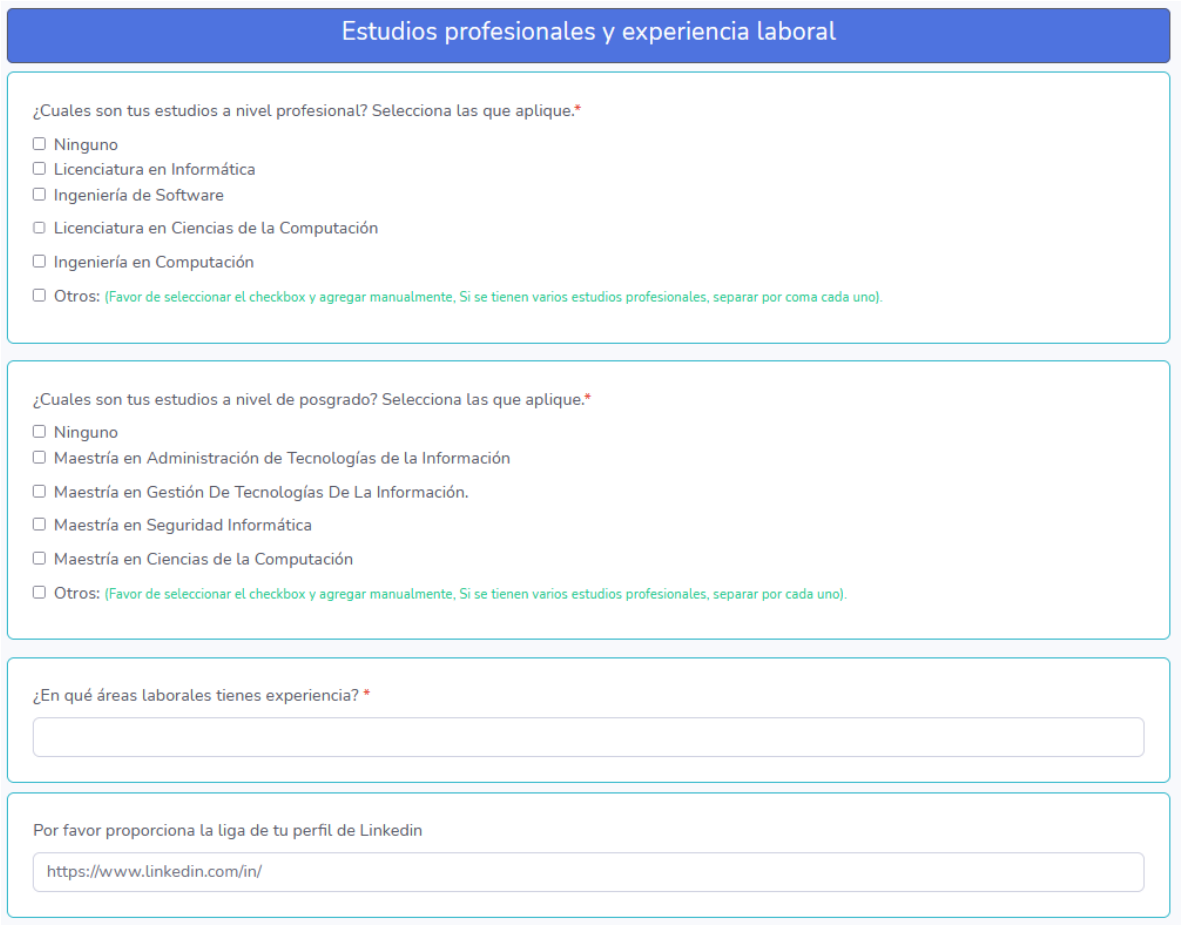

Ilustración 48. Sección de estudios profesionales y experiencia laboral.

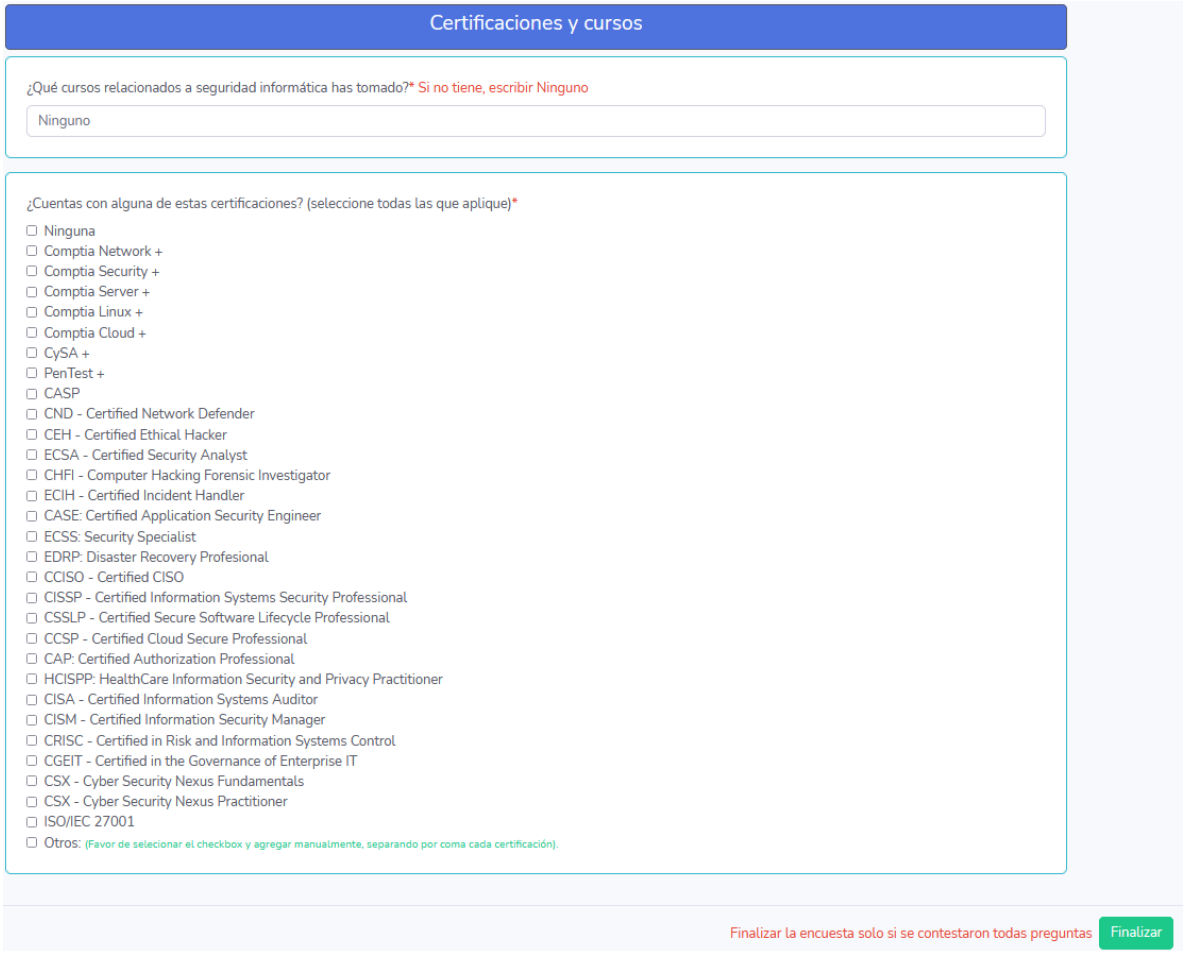

Ilustración 49. Sección de certificaciones y cursos.