EasyChair Preprint

№ 6596

Support System for the Determination of the Training Route in the Cybersecurity Area

Jalil Gerardo Espinoza Zepeda, Oscar Mario Rodríguez Elías,
Sonia Regina Meneses Mendoza and
Francisco Gabriel Ibarra Lemas

September 13, 2021

Sistema de Apoyo para la Determinación de Ruta de Capacitación en el Área de la Ciberseguridad

Jalil Gerardo Espinoza-Zepeda, Oscar Mario Rodríguez-Elías, Sonia Regina Meneses-Mendoza, Francisco Gabriel Ibarra-Lemas
Tecnológico Nacional de México/I.T. de Hermosillo, División de Estudios de Posgrado e Investigación
jgez.sys@gmail.com, omrodriguez@hermosillo.tecnm.mx, sonia.menesesm@hermosillo.tecnm.mx, ibarra@hermosillo.tecnm.mx

***Área de participación**: Sistemas Computacionales*

Resumen

El crecimiento de la penetración de los servicios basados en la nube en distintos ámbitos de los sectores público y privado, y la llegada de la industria 4.0, ha derivado en retos tecnológicos, entre los que se encuentra la ciberseguridad. La cada vez mayor dependencia de la digitalización y tecnologías que almacenan, gestionan, procesan datos privados, aumenta la complejidad de los problemas de ciberseguridad. Con el fin de atenuar dichos riesgos, es necesario realizar esfuerzos acelerados que fortalezcan la fuerza de trabajo especializada en el área de la ciberseguridad en nuestro país, para atender una demanda que crece con rapidez. En este trabajo, se presenta un sistema diseñado para apoyar en la definición de rutas de aprendizaje en ciberseguridad, mediante el uso del concepto de perfil de conocimiento y rol de trabajo, facilitando la selección de una serie de certificados adecuada a los intereses personales u organizacionales.

***Palabras clave**: ciberseguridad, perfil de conocimiento, rutas de capacitación, seguridad informática.*

Abstract

The growth in the penetration of cloud-based services in different areas of the public and private sectors, as well as the arrival of Industry 4.0, has led to different technological challenges, among which is cybersecurity. The increasing dependence on digitization and technologies that store, manage, process private data, increases the complexity of cybersecurity problems. In order to mitigate these risks, it is necessary to make accelerated efforts to strengthen the specialized workforce in the area of cybersecurity in our country, to meet a rapidly growing demand. In this work, a system designed to support the definition of learning paths in cybersecurity is presented, through the use of the concept of knowledge profile and work role, facilitating the selection of a series of certificates suitable for personal or organizational interests.

***Key words**: cybersecurity, knowledge profile, training routes, computer security.*

Introducción

La ciberseguridad en México y en el mundo es un tema de relevancia para todos, ya que tanto la sociedad como una gran mayoría de organizaciones hacen uso de tecnología digital, aprovechando la gran cantidad de beneficios que esta tiene. Como se observa en [1] ha existido un aumento constante de los dispositivos conectados al internet en los últimos años, con proyecciones que apuntan a que para el año 2050 existirán mil millones de dispositivitos conectados al internet en México. Se estima que en la actualidad existen aproximadamente 3 dispositivos por persona conectados a Internet en México [1]. Las organizaciones a nivel mundial declaran que entre los principales desafíos está la ciberseguridad, como lo ha informado en los últimos años el Foro Económico Mundial en ““The Global Risks Report” [2]–[4].

El panorama de riesgos del 2017 al 2021, incluye entre los principales riesgos económicos a nivel mundial aspectos de la seguridad en la tecnología [2]–[4]. Aunque los ciberataques no están entre los primeros 5 en 2021, el 75% de los encuestados considera que tendrán un aumento [4]. Para el 2021 los ciberataques se encuentran entre los primeros diez riesgos de la economía [4]. Los riesgos en ciberseguridad están presentes en todo el mundo, ya que pueden tener repercusiones indeseables en la infraestructura, la seguridad nacional y el desarrollo económico de cualquier país. Referente a México, 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 [5].

La seguridad de la información es una forma de aplicar conocimientos y tecnologías para defender, preservar y proteger los datos, asegurando implementar controles y procesos adecuados en las redes, programas, dispositivos y el actuar del recurso humano [6]. Lograrlo requiere el esfuerzo de múltiples áreas en una organización, ya que las especializaciones en seguridad de la información se dan en diversos ámbitos, incluidos los legales, tecnológicos, operativos y administrativos. Por lo tanto, la capacitación de profesionales de la ciberseguridad no es una tarea fácil, la alta diversidad en alternativas de áreas de especialización, así como de roles de trabajo a realizar, dificulta diseñar programas para capacitar a profesionales de diversas áreas de las TI, sobre todo si incluimos a otras disciplinas. Considerando lo anterior, en este artículo se propone un sistema que ayude a sistematizar la toma de decisiones para la asignación de rutas de capacitación en ciberseguridad considerando el perfil de conocimiento e intereses de los candidatos. Cabe resaltar que una descripción del planteamiento de este problema se presentó en [7], mientras que un primer acercamiento al diseño de una posible solución de este problema se propuso en [8].

El resto de este artículo está organizado de la siguiente manera: primeramente, se describe la metodología seguida para la realización del trabajo reportado en este artículo, que incluye los procesos de análisis y diseño de la arquitectura del sistema propuesto, empezando por los elementos base para la definición de requisitos y la aplicación de los conceptos base para el desarrollo del prototipo. Posteriormente, se presenta un prototipo del sistema resultante, para finalmente concluir este trabajo.

Metodología de trabajo

Este trabajo se realizó en dos fases generales. En la **Figura 1** se muestra la estructura completa. La primera fase se dividió en dos etapas, la primera consistió en determinar un mecanismo para que uno o varios expertos caractericen los roles de trabajos, no documentados, y perfiles de conocimiento, necesarios para cubrir cada rol en el área de la ciberseguridad en México, para posteriormente poder identificar las certificaciones más adecuadas, y así proponer planes de capacitación. Para establecer este mecanismo se utilizó el concepto de perfiles de conocimiento propuesto en [9], de lo cual, sus mismos autores definieron una ontología que ayuda a identificar los elementos básicos para definir perfiles de conocimiento de individuos y puestos o roles de trabajo [10]. Dentro de este contexto, para evaluar el grado al cual un perfil de conocimiento de un individuo se ajusta al rol de trabajo requerido y llevar ciertos planes de capacitación, se ha utilizado un modelo basado en lógica difusa propuesto en [11], permitiendo identificar las áreas que necesita fortalecer el individuo para cumplir en su totalidad con el rol de trabajo.

La segunda etapa de la primera fase se enfocó en identificar y analizar los perfiles de conocimiento ya conocidos en el área de la ciberseguridad para cada rol de trabajo, para lo que se trabajó con la guía para el marco de trabajo en ciberseguridad propuesto por la iniciativa nacional de educación en ciberseguridad del gobierno de los Estados Unidos (NICE), y que está dividida en siete categorías; cada una subdividida en treinta y tres áreas de especialidad. Cada área de especialidad está estructurada a su vez en roles de trabajo, contando actualmente con un total de cincuenta y dos; los cuales definen los conocimientos, habilidades y tareas necesarias para cumplir con el rol [12]. En esta misma etapa se identificaron algunas de las principales casas certificadoras en ciberseguridad y se estableció un formulario para obtener datos de los interesados.

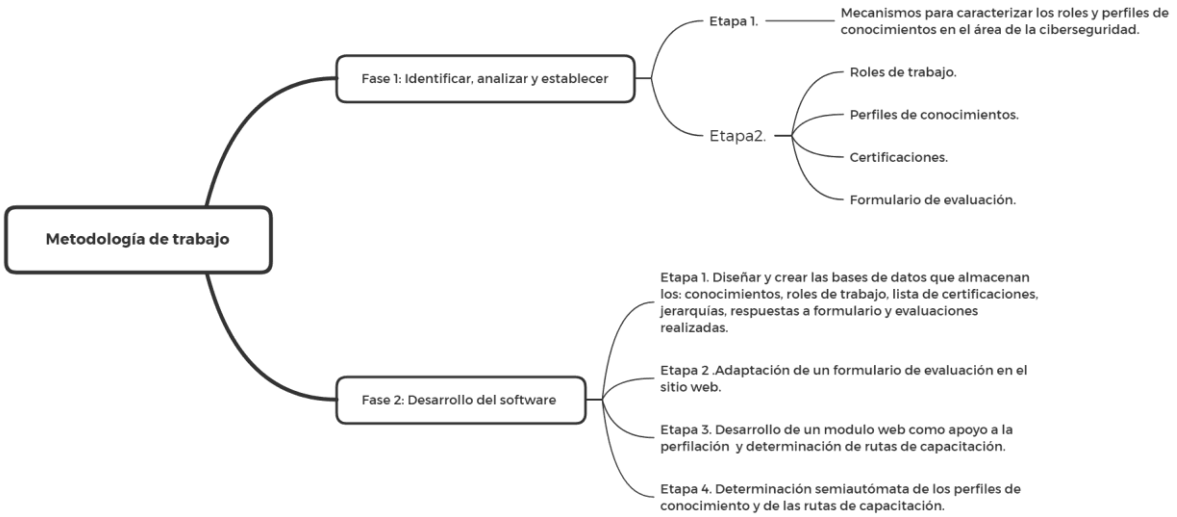

Figura 1. Metodología de trabajo usado en este proyecto.

En la segunda fase general del proyecto se aplicó un proceso de desarrollo de software dividido en cuatro etapas. (1) La primera consistió en diseñar la base de datos para contener la información recabada de los participantes y de las evaluaciones realizadas. (2) En la segunda se adaptó el formulario de evaluación a un sitio web, para la obtención de datos de los interesados en el estudio de la ciberseguridad. (3) En la tercera se desarrolló un módulo web como apoyo a la evaluación y determinación de rutas de capacitación por parte de los expertos en ciberseguridad. (4) Como última etapa se estableció una solución para que la aplicación, de manera semiautónoma, proporcione perfiles de conocimiento y rutas de capacitación como apoyo a los expertos.

Arquitectura del software

Para el diseño del sistema se tomaron en cuenta una serie de requisitos definidos con base en la consulta a expertos en ciberseguridad, cuya principal área de trabajo es la capacitación para la certificación en distintas áreas de la ciberseguridad. Como resultado se obtuvo un conjunto de requisitos base para el desarrollo del sistema, entre los que se encuentran los siguientes:

- Debe ser una aplicación web con una interfaz de usuario responsivo, fácil de usar.
- Recopilación y almacenamiento de los datos de los colaboradores y evaluaciones realizadas por los expertos.
- Garantizar la seguridad de los datos y administrar los permisos de los usuarios.
- Debe apoyar en la determinación de rutas de aprendizaje en el área de la ciberseguridad.
- Los expertos deberán poder: (1) evaluar el conocimiento de los participantes, (2) relacionar los resultados con un perfil que cumpla con un rol de trabajo y (3) determinar las mejores rutas de capacitación, tomando en cuenta los dos puntos anteriores.
- El sistema debe mostrar el o los planes de capacitación recomendados al participante.

De acuerdo a los requisitos mencionados anteriormente, se abstraen como componentes generales del sistema desarrollado: la seguridad, usabilidad, base de datos y funcionalidad.

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:

- **Colaborador o participante.** Profesional con interés de obtener conocimientos de algún rol de trabajo en el área de la ciberseguridad. Este usuario contesta cierto número de preguntas, para que el experto las analice.
- **Experto.** Usuario experto en el área de la ciberseguridad, quien realizará la evaluación de los conocimientos de los colaboradores y establece una o varias rutas de aprendizaje.

- **Admin (administrador del sistema).** Usuario con todos los permisos del colaborador y experto, además de crear, eliminar y modificar usuario experto.

Operación general del sistema

Para proteger la privacidad de los usuarios, no se almacenan permanentemente datos personales que los identifique, como: nombre, apellido, región, país, correo, username, password. 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. Por seguridad el colaborador no carga ningún tipo de archivo en el cuestionario proporcionado, se establece la eliminación por usuario y no por grupos, como opción de recuperación se crea una base de datos extra de la principal para respaldar. Los datos obtenidos de la encuesta realizada por el colaborador serán utilizados para hacer investigaciones futuras, así que cuando se elimina un usuario, sus datos personales se remplazan por referencias genéricas, sin relación al colaborador.

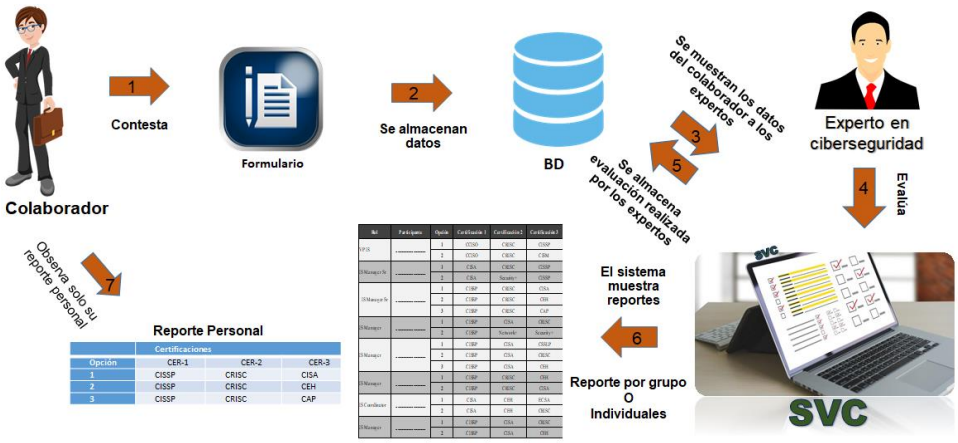

Figura 2. Flujo del proceso de negocio del sistema desarrollado.

En la **Figura 2** se observa el flujo del proceso de negocio del sistema, empezando con el cuestionario por parte del colaborador, hasta finalizar con un reporte con las rutas de aprendizaje recomendados. Antes de contestar el cuestionario el colaborador recibirá los datos de ingreso al sistema, con un enlace para crear una contraseña. El proceso a seguir es el siguiente: (1) El colaborador contesta el formulario y presiona el botón submit para que las respuestas se (2) almacenen en la base de datos; (3) Los datos del colaborador son mostrados en el módulo de evaluación; (4) El experto analiza los datos, evalúa (establece un perfil de conocimiento e indica el rol de trabajo) y determina una o varias de rutas de aprendizaje recomendadas, al finalizar realiza el submit para que la (5) evaluación se almacene en la base de datos; (6) El sistema crea reportes de las evaluaciones, que pueden ser observados por el experto evaluador en cualquier momento. (7) El experto debe notificar a los colaboradores las rutas de aprendizaje obtenida por medio de un archivo PDF y también el colaborador puede revisar sus evaluaciones en el mismo sistema. Este es el proceso para que el colaborador reciba una o varias propuestas de rutas de aprendizaje por medio de certificaciones recomendadas, de acuerdo a sus intereses y necesidades.

La **Figura 3** muestra el esquema general del sistema desarrollado. El componente experto incluye los módulos principales para cumplir con la capa de negocio en el proceso de evaluación y control de reportes. El sistema está constituido de seis módulos principales: evaluación, reportes, usuarios, formularios, correo, nice (NICE Framework (v2.0)); estructurado con tres bases de datos para el almacenamiento lógico: datos estáticos, datos dinámicos y respaldo de las respuestas de los usuarios sin datos personales que lo identifique.

En el módulo formulario se estructura la interface gráfica para el cuestionario a ser contestado por el colaborador o candidato. En el módulo de evaluación se estructura las interfaces gráficas que contiene el nombre del colaborador, un input para ingresar el rol o puesto de trabajo a capacitarse,

opciones para establecer un perfil de conocimiento (ver Tabla 1) del colaborador antes de realizar las certificaciones; también se establece un perfil de conocimiento, el cual se obtiene u obtendrá después de la capacitación; en este módulo también se determinan las mejores rutas de aprendizaje, considerando el análisis obtenido de las respuestas de los colaboradores.

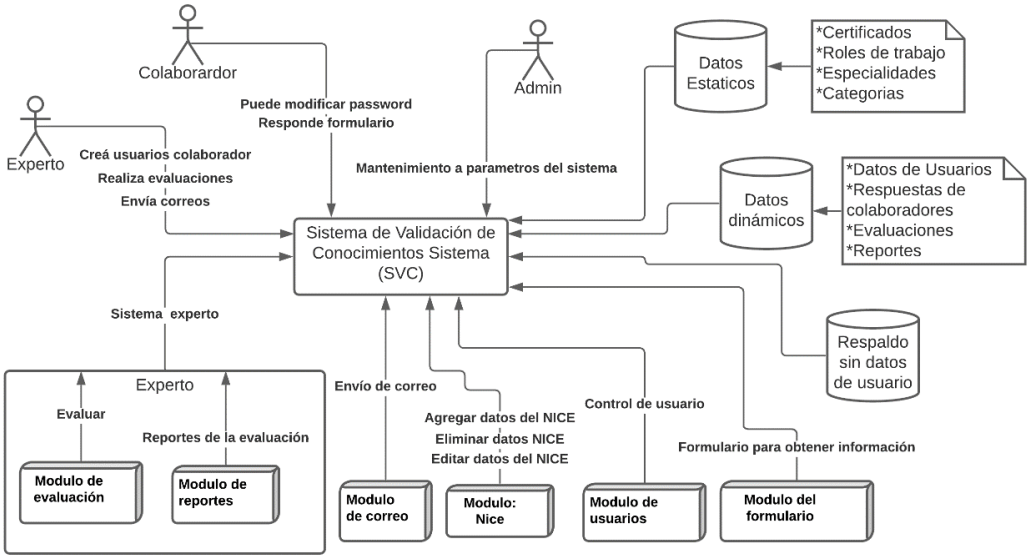

Figura 3. Estructura general del sistema desarrollado.

Validación de los perfiles de conocimientos

El perfil de conocimiento, en este proyecto, es el nivel de competencia del colaborador en el área de la ciberseguridad. Por lo que el módulo de evaluación por parte de los expertos, se realizó con la siguiente propuesta de cuestionario para validar el perfil de conocimientos de los colaboradores, estos son: (1) Cuestionario de nivel de conocimientos por habilidades técnicas, (2) Cuestionario de nivel de conocimientos por experiencia y estudios realizados. Es importante destacar que la determinación de puntajes a cada perfil de conocimiento, y que estos puntos sean establecidos por los expertos, se basó en [11], y los perfiles base en [6]. Los perfiles de conocimientos que se implementaron en el sistema son los de la Tabla 1.

Tabla 1. 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

Resultados

El sistema se desarrolló siguiendo el Framework django (www.djangoproject.com), que se basa en el patrón arquitectónico Modelo-Vista-Template. En la **Figura 4** se muestra la pantalla del módulo de evaluación, donde se establece el rol de trabajo, los perfiles de conocimiento y las rutas de aprendizaje.

En la **Figura 5** se muestra un ejemplo del reporte de recomendación de rutas de capacitación que arroja el sistema. Se puede observar que se ofrecen tres opciones, cada una con tres posibles

cursos o certificaciones, ordenadas de acuerdo a cómo deberían llevarse para lograr el rol de trabajo deseado. Dichas rutas se definen al analizar el rol de conocimiento del candidato a la capacitación.

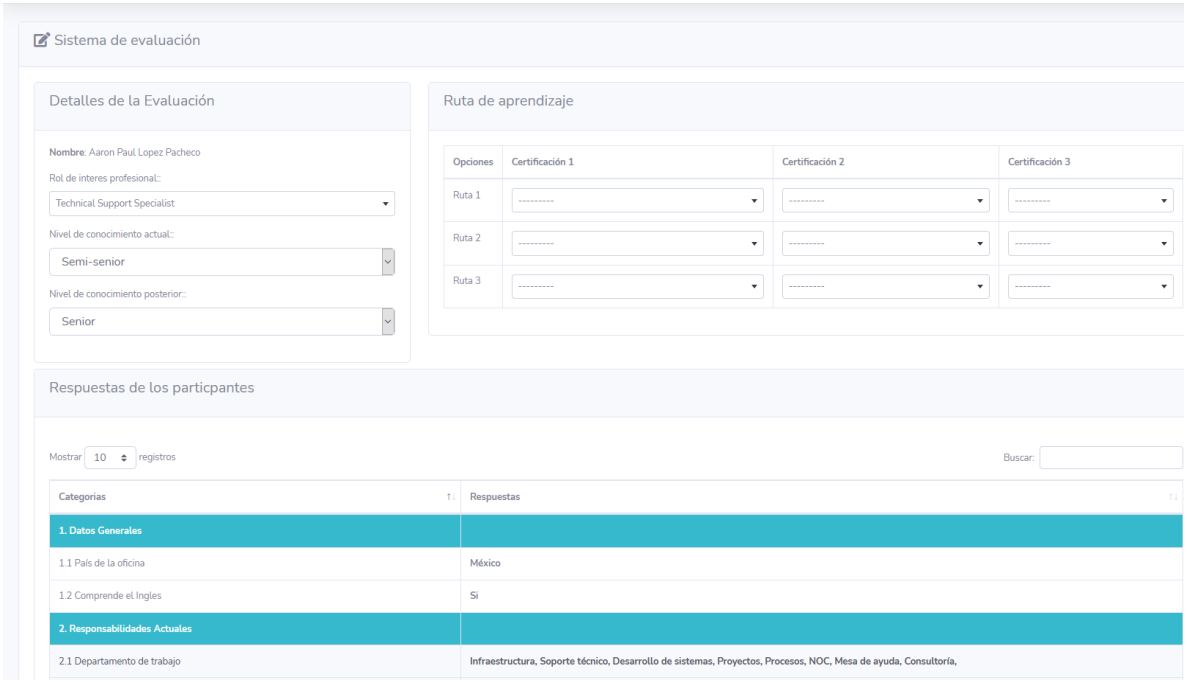

Figura 4. Pantalla de evaluación del colaborador o participante.

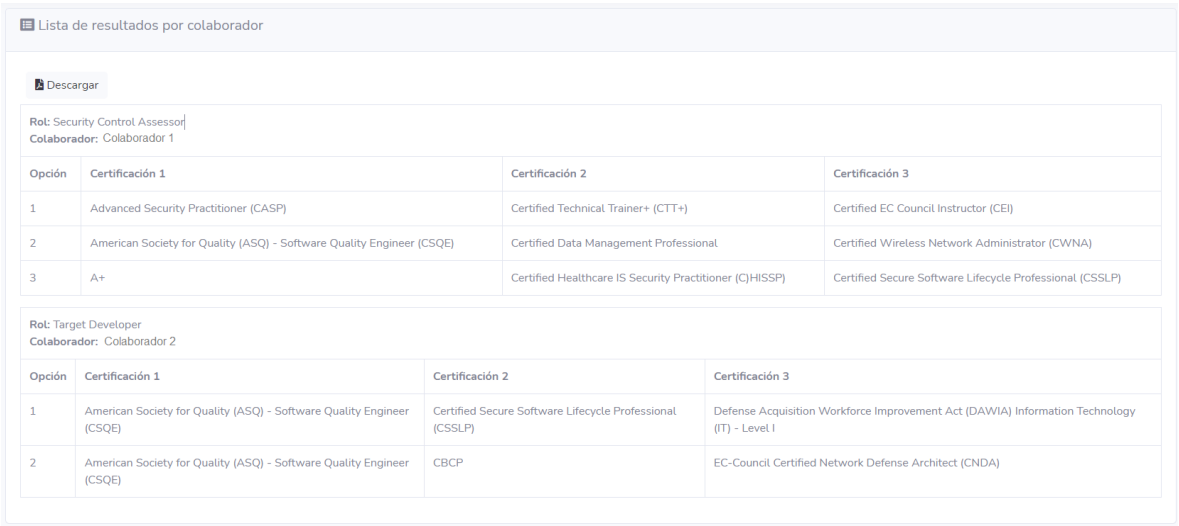

Figura 5. Ejemplo de reporte de recomendación de rutas de capacitación.

Para validar el cumplimiento de los requisitos del sistema, se realizaron varios tipos de pruebas, entre algunas de las preguntas principales se muestran en la **Tabla 2**. Las validaciones realizadas fueron 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 resultados más relevantes obtenidos de estas validaciones son los siguientes:

- Se concluyó que todavía hay trabajo por hacer, para mejorar la usabilidad, ya que los usuarios, al realizar una búsqueda en las preguntas de selección, mencionaron que fue muy fácil encontrar las respuestas, en comparación con un 16.7% que fue regular, por lo que no se alcanza un 90% de usabilidad.
- El 100% de los participantes están dispuestos a recomendar el sistema, y se considera que la información en este es de interés a los profesionales, además de ser beneficioso para la comunidad: aunque no todos están seguros de que les pueda ser de beneficio para ellos mismo. En sí, la aceptación total de la propuesta del proyecto fue de un 77.8% (se considera solo el promedio de las tres primeras preguntas).

Tabla 2. Principales preguntas de validación del sistema. Valor: R: regular, B: Bueno, MB: Muy bueno.

Pregunta	3 (R)	4 (B)	5 (MB)
Considero que lo que plantea el proyecto de SVC es beneficioso para la comunidad.			100%
Considero que el proyecto planteado me puede beneficiar para mis intereses profesionales.	16.7%	16.7%	66.7%
Díganos qué tan sencillo le resulta buscar una respuesta a cada pregunta.	16.7%	16.7%	66.7%
En sentido general, ¿Cómo evaluaría usted la Página Web del sistema de validación de conocimientos?	16%	50%	33.3%
Está dispuesto a recomendar esta Página Web a un relacionado suyo.			100%
Promedio total por escala de evaluación	16.47%	27.80%	66.68%

Conclusión

Acelerar la formación de personal especializado en ciberseguridad es una necesidad creciente, por lo que proveer mecanismos que abonen en este sentido podría tener un impacto significativo en diversos ámbitos, tanto en sectores privados como públicos. Por los resultados obtenidos en este proyecto, se considera que el sistema propuesto favorece en la reducción de tiempo y esfuerzo en la realización de la toma de decisión de las rutas de capacitación en el área de la ciberseguridad, lo que pudiera contribuir en un aumento en la cantidad de personas que pudieran atenderse por parte de empresas e instituciones especializadas en la capacitación de profesionales en el área de la ciberseguridad. Las personas principalmente beneficiadas serían los expertos en ciberseguridad, que en sí son los que toman la decisión de plan de capacitación; pero también organizaciones y otros interesados podrían beneficiarse al contar con un sistema web seguro y validado, que apoye en las recomendaciones de capacitación para la obtención de trabajadores mejor preparados para un rol de trabajo en el área de la seguridad de la información.

Como parte del proceso de análisis del sistema, se logró también especificar 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 cuestionarios de empresa/s capacitadora/s a un formulario web, para la obtención de datos de candidatos a capacitación. (3) Diseñar base de datos de conocimientos, roles de trabajo, Certificaciones, jerarquías, respuestas a formulario y conclusiones de evaluaciones realizadas. (4) Desarrollar una aplicación web como apoyo para la determinación de rutas de capacitación. (5) Determinación automática de los perfiles de conocimiento y de las rutas de capacitación.

En el contexto general del software que se desarrolló se garantiza la seguridad de los datos, como también se administran las autorizaciones para ingresar al sistema en los diferentes módulos, dependiendo de los permisos de los usuarios. Los usuarios que ingresen a la aplicación lo hacen 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.

Limitaciones y trabajos a futuros

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, incluyendo los roles de trabajo y especificaciones de los certificados recomendados en el área de la ciberseguridad.
- Ampliar y enriquecer las aportaciones obtenidas por medio de nuevas características y/o diagramas. Esto se puede conseguir por medio de encuestas 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 pueden implementar algoritmos de aprendizaje automático, para la determinación de perfiles de conocimientos, roles de trabajo y 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 que utilice un algoritmo inteligente para realizar el proceso de selección de rutas de capacitación de manera automática reduciendo la intervención de personal experto, siguiendo con la implementación y validación del sistema resultante mediante su aplicación en casos reales.

Agradecimientos

Se agradece el apoyo del CONACYT con la beca número 744901 otorgada al segundo autor. Así mismo, agradecemos todo el apoyo otorgado por la empresa Código Verde, y en particular a su director general. Ing. David Taboada.

Referencias

[1] D. Abusaid, A. Cristofori, R. Fernández MacGregor, and S. Waisser, “Perspectiva de ciberseguridad en México,” 2018.
[2] FEM (Foro Económico Mundial), “Informe de riesgos mundiales 2019: 14.ª edición,” Ginebra, Suiza, 2020.
[3] FEM (Foro Económico Mundial), “The Global Risks Report 2020,” 2020.
[4] FEM (Foro Económico Mundial), “The Global Risks Report 2021,” 2021.
[5] International Telecommunication Union (ITU), “Global Cybersecurity Index 2020,” 2021.
[6] National Initiative for Cybersecurity Careers and Studies (NICCS), “The Cyber Career Pathways Tool User Guide,” 2021.
[7] Jalil Gerardo Espinoza Zepeda, Oscar Mario Rodríguez Elías, Propuesta para abordar la necesidad de profesionales en ciberseguridad, Espacio ITH: *un lenguaje natural tecnológico*, Año 9, No. 2, pp. 46-54, 2019.
[8] Jalil Gerardo Espinoza-Zepeda, Oscar Mario Rodríguez-Elías, Sonia Regina Meneses-Mendoza, Francisco Gabriel Ibarra-Lemas, Diseño de un Sistema de Apoyo en la Determinación de Rutas de Aprendizaje en Seguridad de la Información, *Avances de Investigación en Ingeniería en el Estado de Sonora*, Año 6, No. 1, pp. 10-17, 2020.
[9] M. J. Velázquez Mendoza, O. M. Rodriguez-Elias, C. E. Rose Gómez, and S. R. Meneses Mendoza, “Perfiles de Conocimiento en la Gestión del Recurso Humano de las Organizaciones,” *Congr. Int. Investig. Acad. JOURNALS*, vol. 4, no. 3, pp. 3209–3214, 2012.
[10] O. M. Rodríguez-Elias, M. de J. Velázquez-Mendoza, and C. E. Rose-Gómez, “An Ontology Based System for Knowledge Profile Management,” in *Current Trends on Knowledge-Based Systems*, vol. 120, G. Alor-Hernández and R. Valencia-García, Eds. Cham: Springer, 2017, pp. 49–72.
[11] J. A. Rosas Daniel, O. M. Rodríguez-Elias, M. de J. Velazquez-Mendoza, and C. E. Rose-Gómez, “Diseño de un sistema para valoración de perfiles de recursos humanos,” *Rev. Coloq. Investig. Multidiscip.*, vol. 3, no. 1, pp. 403–414, 2015.
[12] D. Shoemaker, A. Kohnke, and K. Sigler, *A Guide to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2.0)*, 1rst ed. Auerbach Publications, 2016.