Universidad Metropolitana
Facultad de Ingeniería
Escuela de Ingeniería de Sistemas

Desarrollo de un sistema para la gestión de la certificación profesional en Seguridad de la Información en Venezuela

Fernando Baladi
Carnet: 20181110303
Gustavo Márquez
Carnet: 20181110043

Tutor: Vincenzo Mendillo

Caracas, 25 de febrero de 202

Objetivo(s) del Desarrollo Sustentable (ODS) al cual se orienta el trabajo de investigación

INSTRUCCIONES: *Coloque una "x" en las casillas "directo" o "indirecto" junto al o los Objetivos de Desarrollo Sostenible a los que la investigación contribuye y la forma; y describa brevemente (250 caracteres) de qué forma lo hace, en función de las metas del ODS, y el objetivo general de su trabajo.*

ODS	Descripción	Relación con los Objetivos de la Investigación	Directo	Indirecto
	Garantizar una educación inclusiva, equitativa y de calidad y promover oportunidades de aprendizaje durante toda la vida para todos.	*Con un sistema que permita la certificación profesional en Seguridad a la Información en Venezuela, se abrirán nuevas posibilidades para que los venezolanos tengan una mejor fuente de conocimiento relacionada a la Seguridad de la Información.*	*X*	
	Promover el crecimiento económico sostenido, inclusivo y sostenible, el empleo pleno y productivo y el trabajo decente para todos.	*Al certificar a cada vez más personas en el ámbito de la Seguridad de la Información, se permitirá que se obtengan mejores y más empleos en esta área, haciendo que las personas tengan trabajos más dignos.*	*X*	
	Lograr que las ciudades y los asentamientos humanos sean inclusivos, seguros, resilientes y sostenibles.	*Con profesionales en Seguridad de la Información certificados y trabajando en el área, se logrará que ciudadanos, así como entes públicos y privados, puedan planificar y mejorar los sistemas de seguridad.*	*X*	
	Promover sociedades justas, pacíficas e inclusivas.	*Al crear ambientes y sistemas más seguros, se estará a un paso más de entrar en una mayor paz y armonía, evitando conflictos internos y externos.*		*X*

Derecho del Autor

Quienes suscriben, en condición de autores del trabajo titulado “Desarrollo de un sistema para la gestión de la certificación profesional en Seguridad de la Información en Venezuela”, declaramos que: Cedemos a título gratuito, y en forma pura y simple, ilimitada e irrevocable a la Universidad Metropolitana, los derechos de autor de contenido patrimonial que nos corresponden sobre el presente trabajo. Conforme a lo anterior, esta cesión patrimonial sólo comprenderá el derecho para la Universidad de comunicar públicamente la obra, divulgar, publicar o reproducirla en la oportunidad que ella así lo estime conveniente, así como, la de salvaguardar nuestros intereses y derechos que nos corresponden como autores de la obra antes señalada. La Universidad en todo momento deberá indicar que la autoría o creación del trabajo corresponde a nuestra persona, salvo los créditos que se deban hacer al tutor o a cualquier tercero que haya colaborado o fuere hecho posible la realización de la presente obra.

_____	_____
Autor Fernando Baladi	Autor Gustavo Márquez
C.I. V-27.814.624	C.I. V-26.645.708

En la ciudad de Caracas, a los 25 días del mes de febrero de 2022.

Aprobación

Considero que el Trabajo Final titulado

Desarrollo de un sistema para la gestión de la certificación profesional en Seguridad de la Información en Venezuela

Elaborado por los ciudadanos

Fernando Baladi

Gustavo Márquez

Para optar al título de

Ingeniero de Sistemas

Reúne los requisitos exigidos por la Escuela de Ingeniería de Sistemas de la Universidad Metropolitana, y tiene méritos suficientes como para ser sometido a la presentación y evaluación exhaustiva por parte del jurado examinador que se designe.

En la ciudad de Caracas, a los 25 días del mes de febrero del año 2022

_____

Tutor: Ing. Vincenzo Mendillo

UNIVERSIDAD METROPOLITANA
RIF J-00065477-8

FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA DE SISTEMAS

ACTA DE VEREDICTO

Nosotros, los abajo firmantes, constituidos como jurado examinador y reunidos en Caracas, el día 15 de marzo de 2022, con el propósito de evaluar el Trabajo de Grado titulado:

"Desarrollo de un sistema para la gestión de la certificación profesional en Seguridad de la Información en Venezuela "

Presentado por: ***Baladi Tahan Fernando Michel***

Cédula de Identidad N°: ***27.814.624*** Carnet N°: ***20181110303***

Presentado por: ***Márquez Malave Gustavo Enrique***

Cédula de Identidad N°: ***26.645.708*** Carnet N°:***20181110043***

Para optar al título de:

INGENIERO DE SISTEMAS

Emitimos el siguiente veredicto:

Aprobado X Reprobado ____ Mención Honorífica ___ Sí/ No

OBSERVACIONES:_____

Luis Eduardo García	**Vincenzo Mendillo**	**María Carvajal**
Presidente	Tutor	Jurado

El Trabajo de Grado de Pregrado se rige por el Reglamento de Trabajo de Grado de Pregrado, aprobado por el Consejo Académico N° 450 del 14 de noviembre de 2013 y el Consejo Superior N° 303 del 18 de noviembre de 2013. La Evaluación del Trabajo de Grado corresponde a los artículos 29 al 42.

UNIVERSIDAD METROPOLITANA
Escuela de Sistemas
Sello de la Escuela

Agradecimientos

Primero que nada, quiero agradecer a la vida y el universo, por darme la suerte de estar aquí y ahora, por tener la dicha de lograr mis retos.

A mis padres, Mariela y Salvador, que incondicionalmente me han dado su amor, su vida y su apoyo en cada decisión que he tomado.

A mi hermano, Angelo, por siempre estar conmigo, en las buenas y en las malas. *Sic parvis magna*.

A mi novia, Mafe, por siempre creer en mí y con su amor, inspirarme.

A mi compañero, Gustavo Márquez, por insistir tanto en lograr nuestra investigación, así como a nuestro tutor, Vincenzo Mendillo, por siempre estar atento y guiarnos en nuestra investigación.

A ASOVESINFO y a Luis Sandoval por su tiempo y apoyo en la realización del trabajo de grado.

A mis amigos y familiares, quienes me han guiado y aconsejado.

Finalmente, me agradezco por siempre ir más allá, por aceptar mis retos y mis locuras, por siempre decir "¡Sí puedo!", y esforzarme más.

Fernando Baladi

Quiero agradecer a mis padres, Gustavo y Marely, por haberme acompañado, apoyado y querido siempre, y por haberme traído hasta este punto, ayudándome a convertirme en la persona que soy. A mi hermana, Maria del Mar, por apoyarme siempre cuando más la necesito y por mostrarme siempre cómo seguir adelante.

A toda mi familia, por estar siempre pendientes y brindarme sus mejores deseos y energías.

A mi compañero, Fernando Baladi, por ser el mejor aliado que hubiese podido tener para una tarea tan ardua como ésta, y un gran amigo. A nuestro tutor, Ing. Vincenzo Mendillo, por poner a nuestra disposición toda su ayuda y sus herramientas, y guiarnos en este largo camino.

A todos mis amigos, por ser siempre la alegría que necesito y mi mejor motivación para ser mejor. A los que están lejos, sé que podré estar con ustedes muy pronto.

Gustavo Márquez

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Resumen

Desarrollo de un sistema para la gestión de la certificación profesional en Seguridad de la Información en Venezuela

Autor(es): Fernando Baladi y Gustavo Márquez

Tutor: Vincenzo Mendillo Caracas, febrero 2022

El objetivo de la presente investigación fue desarrollar una plataforma para la emisión y administración de certificaciones profesionales en seguridad de la información en Venezuela. Para ello, el primer paso fue evaluar la preparación universitaria en seguridad de la información ofrecida en el país y compararla con las certificaciones y demás cursos internacionales, de modo que la plataforma a desarrollar sirva como respuesta a la situación analizada en dicha comparación. Inicialmente se recopiló información sobre las certificaciones en seguridad de la información más prestigiosas a nivel mundial y sobre los planes de estudio de algunas de las universidades más importantes del país para efectuar dicha comparación. La investigación sobre las principales certificaciones sirvió de base para diseñar la certificación a implementar, incluyendo temas, subtemas y la forma de evaluación.

Posteriormente, se investigó sobre las distintas tecnologías de tipo LMS (Learning Management System), con el objetivo de seleccionar una de ellas como plataforma desde la que se gestionará dicha certificación. Una vez seleccionada dicha tecnología, se procedió a desarrollar la plataforma implementando las funcionalidades básicas y esenciales para la certificación profesional, es decir: Registro y acceso de usuarios, matriculación de aspirantes, creación de exámenes, administración de bancos de preguntas, otorgamiento de certificados e insignias, así como creación de certificaciones nuevas. Con respecto a la evaluación en línea (esto es los exámenes), se incorporó el requisito de Safe Exam Browser para su realización. Esta aplicación, de tipo navegador, evita que el usuario pueda efectuar capturas de pantalla, cambio de pestaña, entre otras cosas, con la finalidad de blindar las evaluaciones contra fraude o diversos tipos de trampa.

Palabras clave: Seguridad de la información, certificación, insignia, LMS, proctoring.

Introducción

Las certificaciones han sido una forma efectiva para demostrar que los profesionales poseen conocimientos avanzados en sus campos laborales. Estas certificaciones generan una mayor confianza desde el punto de vista de los reclutadores, porque así pueden constatar que el profesional posee buenos conocimientos en el área.

Considerando lo anterior y la falta de certificaciones en español sobre Seguridad de la Información, se analizaron y compararon distintas certificaciones internacionales el área, así como cursos que se imparten a nivel de pregrado y postgrado en universidades venezolanas y de otros países, todo esto con el fin de tener una base para diseñar una plataforma de certificación que sea en español y de costo razonable.

Para desarrollar la plataforma se buscaron alternativas de Sistemas de Gestión de Aprendizaje (o LMS por sus siglas en inglés). Se evaluaron LMS como Moodle, Chamilo o Efront, para así seleccionar el que mejor se adecuara a las necesidades de la certificación.

Esta certificación, una vez desarrollada, quedará bajo la administración de la Asociación Venezolana de la Seguridad de la Información (ASOVESINFO), la cual busca agremiar profesionales del área y contribuir a su desarrollo dentro del país. Mediante esta nueva Certificación Profesional en Seguridad de la Información, llamada PCSI, se podrán agremiar a más personas y generar una mayor confianza en los reclutadores que buscan personal calificado.

Este trabajo de grado está estructurado de la siguiente forma:

- Capítulo I: Tema de investigación. Aquí se presenta el tema a investigar, así como su justificación y los objetivos bajo los que se regirá la investigación.
- Capítulo II: Marco referencial. Aquí se desglosa y se plasma toda la información recopilada que servirá posteriormente durante el desarrollo de los objetivos.

- Capítulo III: Marco metodológico. Aquí se presenta la metodología utilizada para la elaboración del trabajo de grado y el correcto alcance y cumplimiento de los objetivos.
- Capítulo IV: Análisis de resultados. Aquí se analizan detalladamente los resultados obtenidos.
- Capítulo V: Conclusiones y recomendaciones. Aquí se exponen las conclusiones más importantes tras completar el trabajo de grado y las recomendaciones para el uso actual y futuro de la plataforma.

CAPÍTULO I: Tema de Investigación

I.1 Planteamiento del problema

En el ámbito empresarial actual, la Seguridad de la Información se ha vuelto indispensable. Los constantes ataques cibernéticos a empresas se centran en robar información de los usuarios o de la estructura interna de la empresa, o incluso en sabotear sus operaciones. En Latinoamérica, se producen 45 ataques cibernéticos cada segundo, según Kaspersky, (Sánchez Dávila, 2019). Un ciberataque a una compañía puede implicar grandes pérdidas monetarias: “Se estima que las pérdidas económicas pueden alcanzar un trillón de dólares, con un promedio de USD $3,9 millones por cada brecha de seguridad” (Stranieri, 2021). Además de eso, se ve comprometida la reputación y el prestigio de la empresa. Un estudio realizado por PricewaterhouseCoopers (PwC) reveló que el 87% de los clientes encuestados afirma estar dispuesto a abandonar su compañía, si ésta es afectada por un ciberataque que exponga sus datos personales.

Debido a la gran importancia que ha cobrado la Seguridad de la Información, las organizaciones requieren de personal capacitado en esta área para proteger su infraestructura. Sin embargo, los conocimientos adquiridos en una carrera universitaria a menudo no son considerados suficientes y se suele exigir adicionalmente una certificación profesional.

El estudio “Information Security Breaches Survey” realizado en Reino Unido, y que contó con una base muestral de mil empresas de distintos sectores del mercado, muestra que, de las empresas encuestadas, el 75% no cuenta con personal certificado en Seguridad de la Información.

Según Datasec, para el año 2021 habría 147.591 profesionales en todo el mundo que cuentan con una certificación CISSP (Certified Information Systems Security Professional), la cual es una de las acreditaciones más prestigiosas a nivel mundial. Del total de profesionales certificados, el 63% se encuentra en los Estados Unidos, mientras que en Latinoamérica apenas hay 1.522, es decir el 1,03% del total. De esos profesionales certificados sólo 5 están en Venezuela,

país en el que, además, existen muy pocas posibilidades de certificarse sin viajar afuera.

En base a lo anteriormente descrito, en este trabajo especial de grado se plantea el desarrollo de un sistema para otorgar en Venezuela una certificación básica en Seguridad de la Información, la cual facilite a las empresas locales la tarea de seleccionar mejor sus recursos humanos.

I.2 Objetivos

I.2.1 Objetivo General

Desarrollar un sistema de certificación profesional en Seguridad de la Información en Venezuela, mediante el cual se evalúen los conocimientos de los candidatos y se otorgue el título PCSI (Profesional Certificado en Seguridad de la Información).

I.2.2 Objetivos Específicos

- Comparar los distintos tipos de certificación profesional en Seguridad de la Información con la preparación ofrecida en distintos títulos universitarios.
- Evaluar el interés de las empresas locales en una Certificación Profesional en Seguridad de la Información nacional, llamada PCSI, y administrada por ASOVESINFO (Asociación Venezolana de la Seguridad de la Información). https://asovesinfo.org/
- Definir los métodos de evaluación y requisitos para optar a la certificación.
- Identificar las características y las limitaciones del prototipo de plataforma web que fue montada hace muchos años en https://mendillo.info/PCSI/
- Implementar una moderna plataforma web con las tecnologías de gestión de aprendizaje más apropiadas.
- Realizar pruebas para determinar que el sistema funcione correctamente.

I.3 Justificación

En el marco de la Seguridad de la Información es necesario contar, en muchos casos, con certificaciones que permitan corroborar la experticia en el área, mediante exámenes realizados por el profesional, siendo a menudo un

complemento al título universitario. En Venezuela no existe ninguna certificación local en esta área, para que así los profesionales puedan mostrar sus destrezas y en donde los reclutadores puedan apoyarse para definir el perfil que buscan. Es por esto que muchas personas deben recurrir a certificaciones internacionales, teniendo que invertir grandes sumas de dinero, al no contar con plataformas o instituciones nacionales para adquirir esta certificación. En este Trabajo Especial de Grado se busca desarrollar una plataforma de que los profesionales de la Seguridad de la Información puedan certificarse en Venezuela, sin gastar tanto dinero, y permitiendo a las compañías definir mejor las cualidades que se buscan en los profesionales de esa área.

CAPÍTULO II: Marco Referencial

II.1 Seguridad de la información y ciberseguridad

"La seguridad de la información es conjunto de técnicas y medidas para controlar todos los datos que se manejan dentro de una institución y asegurar que no salgan de ese sistema establecido por la empresa" (Anna Pérez, 2017). Es común referirse a ella cómo seguridad informática, pero ésta sólo se refiere a proteger la información en un sistema informático, mientras que la seguridad de la información engloba medidas de protección, protocolos de seguridad, entre otros aspectos. Tampoco debe confundirse con ciberseguridad y, según Kaspersky, la ciberseguridad es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos llevados a cabo por cibercriminales.

En términos más simples, la seguridad de la información busca garantizar tres objetivos principales: confidencialidad, disponibilidad e integridad.

II.1.1 Confidencialidad

La confidencialidad es el principio de la seguridad de la información que garantiza que los datos sólo puedan ser accedidos por personas autorizadas, por lo que no deben ser divulgados a entidades o personas sin autorización.

II.1.2 Disponibilidad

La disponibilidad es uno de los principios fundamentales de la seguridad de la información, que garantiza que a los datos y recursos puedan tener acceso solamente los individuos autorizados.

II.1.3 Integridad

La integridad es el principio de la seguridad de la información que asegura que la información almacenada en dispositivos, o que está siendo transmitida a través de canales de comunicación, no sea manipulada con fines maliciosos por terceras personas.

Así vemos como estos tres objetivos principales son la piedra angular para evaluar la seguridad de cualquier sistema. Estos objetivos deben ser evaluados y cuidadosamente estudiados para minimizar el riesgo de un ataque informático,

y si éste llegase a suceder, minimizar también el daño que podría ocasionar en los sistemas de información.

II.1.4 Ataques Informáticos

> “Un ataque informático consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático, a fin de obtener un beneficio, por lo general de índole económico, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización” (Jorge Mieres, 2009).

Un ciberataque a una compañía puede implicar grandes pérdidas monetarias: “Se estima que las pérdidas económicas pueden alcanzar un trillón de dólares, con un promedio de USD $3,9 millones por cada brecha de seguridad” (Stranieri, 2021). Además de eso, se ve comprometida la reputación y el prestigio de la empresa. Un estudio realizado por PricewaterhouseCoopers (PwC) reveló que el 87% de los clientes encuestados afirma estar dispuesto a abandonar su compañía, si ésta es afectada por un ciberataque que exponga sus datos personales.

II.1.5 Sistemas de redes

“Se denomina sistema de red al conjunto formado por los equipos y los medios físicos y lógicos que permiten la comunicación de información entre diferentes usuarios a cualquier distancia que se encuentren” (Escuela Técnica Superior de Edificación). Esto también implica que si dichas computadoras se encuentran en un mismo lugar, puede ser llamado como red local o por sus siglas en inglés LAN, o si se encuentran en diversas localidades, se les llama red de área extendida o WAN, por sus siglas en inglés.

Esta interconexión tan amplia con casi todas las computadoras y servidores del mundo permite que los atacantes puedan intentar vulnerar cualquier dispositivo que esté dentro de la interconexión en estos grandes sistemas de redes.

Para la interconexión de esta gran cantidad de equipos es necesario una variedad de protocolos que actúan en las distintas capas del modelo OSI. De

esta manera, los equipos pueden intercambiar información de manera satisfactoria.

II.1.6 Principales áreas de la seguridad de la información

La Seguridad de la Información tiene en su haber temas tan diversos y a la vez tan conectados como la criptografía y los sistemas de redes, los riesgos y los ataques de penetración. Es por esta variedad que la Seguridad de la Información tiene muchos puntos que deben ser estudiados y evaluados por separado.

Por tal razón se decidió desglosar y explicar con mayor detenimiento algunas de estas áreas, que también se buscan evaluar dentro de la certificación.

II.1.6.1 Seguridad y gestión de riesgos

"La gestión de riesgos de seguridad de la información es el proceso de identificar, comprender, evaluar y mitigar los riesgos –y sus vulnerabilidades subyacentes– y el impacto en la información" (Sullivan, 2016). El riesgo puede definirse como la probabilidad de que se produzca un daño o una pérdida, y a su vez, el riesgo tiene componentes: La amenaza, vulnerabilidad, resultados e impacto. La amenaza es la entidad humana o no humana que puede explotar una vulnerabilidad y finalmente el impacto es la consecuencia de dicha eventualidad. Otro componente muy importante del riesgo es el activo, la información, tecnología o elemento que puede ser afectado.

Por ello, uno de los objetivos fundamentales de la gestión de riesgos es detectar y tratar de eliminar las vulnerabilidades, y si no pueden ser eliminadas, entonces reducir la probabilidad de explotación y reducir la gravedad del impacto, hasta que el riesgo se considere aceptable.

II.1.6.2 Seguridad de activos

"En una organización los activos en materia de seguridad de la información son: Los datos creados o utilizados por un proceso de la organización en medio digital, el hardware y el software utilizado para el procesamiento, transporte o almacenamiento de información, los servicios utilizados para la transmisión, recepción y control de la información y las

personas que manejan datos, o un conocimiento específico muy importante para la organización" (Cárdenas Varela, 2021).

Es así como The International Information System Security Certification Consortium (ISC)² concuerda con Cárdenas Valera enunciando lo siguiente: la seguridad de activos abarca los siguientes puntos clave: Identificar y clasificar información y activos, determinar y mantener la información y la propiedad de activos, proteger la privacidad, asegurar la retención adecuada de activos, determinar los controles de seguridad de datos y establecer requisitos de gestión de activos e información.

Se puede ver entonces que la seguridad de los activos tiene una gran relevancia para las empresas, siendo ellos estratégicos y de mucho valor, por lo que su protección es fundamental. Por esto, muchas organizaciones buscan tener expertos en Seguridad de la Información y afianzarse en las certificaciones que posean.

II.1.6.3 Arquitectura de seguridad

"La arquitectura de seguridad es un marco que especifica la estructura organizativa, los estándares, las políticas y el comportamiento funcional de una red informática junto a sus características y seguridad" (DocuSign, 2021). Es decir, la arquitectura de seguridad comprende el diseño y planificación de los elementos, políticas y procedimientos que componen la seguridad. Por lo que escoger o desarrollar una arquitectura de seguridad involucra diseñar, planificar y ejecutar las soluciones de dicha arquitectura, así como evaluar y mitigar sus posibles vulnerabilidades.

II.1.6.4 Comunicación y seguridad de red

"La seguridad de red es cualquier actividad diseñada para proteger el acceso, el uso y la integridad de la red y los datos corporativos" (Cisco, 2020). Como se explicó anteriormente, los sistemas de redes involucran una gran cantidad de hardware y software para su funcionamiento. Por ello, la seguridad en sistemas de redes involucra dichos elementos en sus soluciones, por lo que se vuelve imprescindible conocerlos y entender detalladamente su

funcionamiento. Por este motivo, la seguridad en sistemas de redes se convierte en un término bastante amplio que abarca distintos tipos: Firewalls, redes privadas virtuales (VPN), control de acceso, software antivirus y antimalware, seguridad inalámbrica, prevención de pérdida de datos y sistemas de detección/prevención de intrusiones (IDS/IPS). También, basándose en los protocolos de red y herramientas de software y hardware, la seguridad de red permite el diseño e implementación de medios y canales de comunicación seguros.

II.1.6.5 Gestión de identidad y acceso (IAM: Identity and Access Management)

"La Gestión de Identidad y Acceso es un framework diseñado para procesos de negocios que asegura un mayor control para el registro y la seguridad de identidades digitales o electrónicas" (Synnex Westcon-Comstor, 2021). El IAM es el conjunto de políticas y soluciones tecnológicas que se toman para proteger los activos de la empresa.

El IAM comprende distintos campos de acción, como control de acceso físico y lógico a los sistemas e instalaciones, diseño e implementación de sistemas de autenticación que incluyen elementos como login único y autenticación de varios factores que involucre distintos roles dentro de una misma organización, junto con un restrictivo sistema de administración de datos.

II.1.6.6 Evaluación de seguridad y pruebas de penetración

La evaluación de seguridad se refiere a una inspección técnica y detallada de los sistemas, con la intención de detectar posibles vulnerabilidades que pudieran ser explotadas, lo cual conlleva ejecutar pruebas en las cuales se intenta penetrar el sistema para encontrar y explotar vulnerabilidades, determinando que tan seguros son los mecanismos implementados. Este tipo de pruebas también se conoce como pruebas de penetración (pentesting). "Las pruebas de penetración se refieren al proceso de identificación y explotación de vulnerabilidades en seguridad que pueda tener una organización en su infraestructura tecnológica ya sea a nivel de servicios o software implementado" (B-Secure, 2017).

II.1.6.7 Operaciones de seguridad

> “Las operaciones de seguridad se ocupan del acceso diario y la seguridad de los recursos del sistema. Esto significa que debería existir un Centro de Operaciones de Seguridad (Security Operations Center, SOC) que consta de las políticas, estándares, procedimientos y directrices adecuados para los servicios básicos y de apoyo de una organización” (Infosec Institute, 2019).

El SOC se encarga del monitoreo, detección, análisis y resolución de incidentes en materia de seguridad que pudiesen surgir, por lo que su principal objetivo es proteger los datos y hacer cumplir las regulaciones dentro de la organización. Las operaciones de seguridad están muy relacionadas con el monitoreo y gestión de eventos. En este contexto, los eventos son los sucesos que se registran en una red o sistema.

II.1.6.8 Seguridad de desarrollo de software

La seguridad del desarrollo de software son los controles y buenas prácticas que deben tomarse en cuenta durante el proceso de desarrollo para evitar crear vulnerabilidades de seguridad. “Las aplicaciones pueden tener vulnerabilidades de seguridad que los desarrolladores pueden haber introducido de forma intencionada o no. Esta es la razón por la que se requieren controles de software y hardware” (Infosec Institute, 2017). Tales controles de software incluyen validar todas las entradas de datos, implementar controles de acceso apropiados, entre otros.

II.1.6.9 Informática Forense

“La informática forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional” (López, Amaya, León, 2001). La informática forense tiene el principal objetivo de perseguir y procesar a quienes cometen actos ilícitos o criminales. Esta ciencia tiene fundamentos en las leyes de la física, por ejemplo, sabiendo aprovechar las propiedades del magnetismo, es posible recuperar datos que ya han sido borrados en un disco duro.

II.2 Puestos de trabajo en la seguridad de la información

La importancia de proteger la información ha crecido. Como lo indica Stranieri (2021), en el año 2020 los ataques informáticos aumentaron más de un 400% con pérdidas de más de un trillón de dólares, es por este tipo de casos que muchas empresas deciden contratar y tomar en cuenta cada vez más a profesionales en ciberseguridad. Es así como para proteger al ciudadano y a la empresa, la Unión Europea promulgó una nueva directiva donde el rol del Chief Information Security Officer (CISO) es obligatorio para muchas empresas (Martínez, 2021), demostrando que las redes e Internet son áreas que las empresas y los gobiernos buscan asegurar.

Sin embargo, es complicado saber en qué lugar del organigrama debe estar el CISO, ya que él solamente representa la cúspide de la ciberseguridad en la empresa; sin embargo, muchas veces existen otros roles que trabajan de la mano con el CISO, albergando su propio Departamento de Seguridad de la Información, el cual buscará salvaguardar y proteger la infraestructura, la información, y la red de la empresa, mediante la creación y diseño de protocolos basados en las políticas y el negocio de la empresa, sin dejar a un lado los estándares internacionales como el ISO 27001, así como realizar pruebas y auditorías para velar en que todos los departamentos estén siguiendo los lineamientos (Tiwari, 2018).

II.2.1 CISO

Como indican Hooper y McKissack (2016), en muchas el CISO es Gerente de Seguridad de la Información, quien se encarga de proteger los activos en forma de información, controlar los riesgos y asegurar la continuidad del funcionamiento de la empresa, elaborando políticas y protegiendo la integridad de los datos. Entre los requerimientos que muchas empresas buscan para un CISO es que tengan al menos 10 años de experiencia en el área de Tecnologías de la Información, entre 5 y 10 años de experiencia en seguridad y manejo de riesgos, teniendo que contar con una gran cantidad de certificaciones como CISSP, CSSLP, CCFP, CISA y CISM, que son certificaciones relacionadas a la seguridad de la información.

Es así como vemos que el CISO debe tener muchas cualidades y una gran experiencia trabajando en el manejo de riesgos y evaluando vulnerabilidades. El CISO también debe tener habilidades para poder liderar el equipo y explicarle a sus superiores o demás directivos cómo se van a aplicar las medidas de seguridad y las distintas políticas y cuáles serán sus beneficios (Hooper & McKissack, 2016, 4).

Como ya se explicó, el CISO sería comúnmente el Gerente de Seguridad de la Información, por lo que no siempre actuará solo, teniendo bajo su jerarquía otros varios expertos en distintas áreas que a continuación se describen.

II.2.2 CIO

CIO viene de las siglas Chief Information Officer y ha sido un rol fundamental en la inteligencia de negocio de la empresa, ocupando un cargo más bien creativo e innovando con ideas, siendo el responsable de utilizar las nuevas tecnologías para manejar la información de la empresa y mejorar su desempeño (McLaughlin, 2020).

Es por esto que la mayoría de los CIOs no son exactamente expertos en seguridad, y es así que nace el rol del CISO, siendo necesariamente independiente del CIO para poder desprenderse un poco de la inteligencia del negocio y centrarse a cumplir los protocolos completos de los estándares internacionales (Brousell, 2014).

II.2.3 CTO

Por otro lado está el CTO, siglas en inglés para el Director Ejecutivo de Tecnología, quien sería el responsable de toda el área tecnológica dentro de la empresa. Anteriormente este rol era ocupado por el mismo CIO, sin embargo, el CTO debe encargarse de buscar las mejores tecnologías que se utilizan en la empresa y buscar que todos las utilicen para agilizar los trabajos que se necesiten en los demás departamentos. Junto con el CISO, debe buscar las mejores soluciones para cerrar las brechas de seguridad y apuntar a tener un mayor control contra las amenazas (Pérez, 2019).

II.2.4 CSO

A diferencia de las siglas CISO, CSO viene del inglés para Jefe de Seguridad (Chief Security Officer), teniendo un rol fundamental para las empresas de hoy en día, trabajando de la mano con el CISO para poder resguardar de manera eficiente la organización, tanto su infraestructura como sus tecnologías y recursos, centrándose en que todas las actividades sean planificadas y ejecutadas de forma en que puedan seguir los objetivos de la empresa. (IT Digital Security, 2018)

II.2.5 Delegado de Protección de Datos (DPD)

El delegado de Protección de Datos o en inglés Data Protection Officer (DPO), como lo define la European Data Protection Supervisor (2018), se encarga de informar y asesorar al responsable y encargado del tratamiento y la protección de los datos para el correcto uso de los mismos, buscando que se cumplan todas las legislaciones correspondientes en la organización, así como también ser el punto de contacto para las solicitudes del usuario en el uso que se le da a sus datos.

II.2.6 Responsable del tratamiento

El responsable del tratamiento es quien determina el uso y los medios por los cuales los datos personales serán manejados (Comisión Europea, 2016), teniendo en cuenta que es un rol muy importante para las organizaciones por ser el personal que trabajará directamente con los datos personales de la empresa. El responsable del tratamiento también debe estar sincronizado con el DPO para poder hacer cumplir las regulaciones sobre los datos.

II.2.7 Ingeniero en Seguridad de DevSecOps

Los Ingenieros en Seguridad de DevSecOps (o simplemente Ingenieros DevSecOps), se encargan de asesorar al grupo de trabajo de un proyecto de software desde el inicio, durante su construcción y hasta el mantenimiento del mismo, integrando la componente de seguridad en un proyecto de DevOps. Así como también de encontrar vulnerabilidades que puedan ser explotadas (Cobb, 2019).

Es por esto que el Ingeniero en DevSecOps debe estar al día con distintos lenguajes de programación de uso frecuente, como Python, Java, PHP o Javascript y herramientas como Github, así como proveedores de alojamiento en la nube como AWS o Azure.

II.2.8 Threat hunter

Como indica IBM (n.d.), el 20% de las amenazas pueden ser más sofisticadas y traspasar las barreras de ciberseguridad automatizadas, lo que implica una gran cantidad de brechas que están latentes, pudiendo ocasionar grandes pérdidas. Es ahí cuando el thread hunter o cazador de amenazas actúa, buscando de forma proactiva posibles ataques a la red, mitigando estas amenazas incluso antes de que logran actuar (CSO España, 2020).

En este ámbito, CSO España (2020) entrevistó a representantes de 575 empresas con equipos de Cacería de Amenazas, de los cuales el 61% afirmaron ver una mejoría en seguridad de IT de un 11%.

II.3 Certificaciones en seguridad de la información

Las certificaciones en seguridad de la información son títulos emitidos por instituciones que gozan de prestigio y reconocimiento en el área. Dichas certificaciones son obtenidas mediante un examen, luego de que el candidato haya culminado con éxito un curso o carrera corta en la materia, de modo que estas certificaciones se convierten en una garantía, respaldada por la institución que las emite, de que el titular domina y es capaz de desempeñarse en el área. Usualmente, para optar por puestos de trabajo en seguridad de la información, los conocimientos adquiridos en una carrera universitaria no son considerados suficientes y se suele exigir adicionalmente una certificación profesional.

II.3.1 Certificaciones más populares

Según un estudio realizado por el Consorcio internacional de Certificación de Seguridad de Sistemas de Información (ISC)², en el 2019, las certificaciones de seguridad que más profesionales tienen en la actualidad son:

- CISSP (Certified Information Systems Security Professional): Certificación ofrecida por el (ISC)² (International Information Systems Security Certification Consortium, Inc). Consta de los siguientes dominios:

    1. Security and Risk Management
    2. Asset Security
    3. Security Architecture and Engineering
    4. Communications and Network Security
    5. Identity and Access Management
    6. Security Assessment and Testing
    7. Security Operations
    8. Software Development Security

- CCNA Security (Cisco's Certified Network Associate): Certificación ofrecida por CISCO, garantiza que el titular de la certificación es competente y está calificado para manejar una variedad de tareas de seguridad de la red. Consta de los siguientes temas:

    1. Security Concepts
    2. Secure Access
    3. Virtual Private Network
    4. Secure Routing and Switching
    5. Cisco Firewall Technologies
    6. Intrusion Prevention System
    7. Content and Endpoint Security

- CCSP (Certified Cloud Security Professional): Certificación ofrecida por el (ISC)², garantiza que se tienen las habilidades técnicas y conocimientos avanzados para diseñar, administrar y asegurar datos, aplicaciones e infraestructura en la nube utilizando las mejores prácticas, políticas y procedimientos. Consta de los siguientes dominios:

    1. Cloud Concepts, Architecture and Design
    2. Cloud Data Security
    3. Cloud Platform & Infrastructure Security
    4. Cloud Application Security

5. Cloud Security Operations
6. Legal, Risk and Compliance

- CCNP Security (Cisco Certified Network Professional Security): Certificación ofrecida por CISCO, garantiza que el titular de la certificación tiene las habilidades requeridas de los ingenieros de seguridad de redes de nivel profesional para elegir, implementar, brindar soporte y solucionar problemas de firewalls, VPN y soluciones IPS para entornos de redes. Consta de los siguientes temas:

    1. Network security
    2. Cloud security
    3. Securing content in enterprise settings
    4. Endpoints
    5. Network resources access
    6. Policy enforcement

- CIW (Certified Internet Web Professional): Certificación ofrecida por Certifications Partners. CIW consta de un grupo de certificaciones en distintas áreas, entre ellas, CIW: Web Security Associate (1D0-671), la cual consta de los siguientes temas:

    1. What Is Security?
    2. Security Threats
    3. Elements of Security
    4. Applied Encryptions
    5. Types of Attacks
    6. General Security Principles
    7. Protocol Layers and Security
    8. Securing Resources
    9. Firewalls and Virtual Private Networks
    10. Levels of Firewall Protection
    11. Detecting and Distracting Hackers
    12. Incident Response

- CCSK (Certificate of Cloud Security Knowledge): Certificación ofrecida por la CSA (Cloud Security Alliance), garantiza que el titular pueda desarrollar de forma eficaz un programa holístico de seguridad en la nube en relación con los estándares aceptados a nivel mundial. Consta de los siguientes temas:

    1. Cloud Computing Concepts and Architectures
    2. Governance and Enterprise Risk Management
    3. Legal Issues, Contracts, and Electronic Discovery
    4. Compliance and Audit Management
    5. Information Governance
    6. Management Plane and Business Continuity
    7. Infrastructure Security
    8. Virtualization and Containers
    9. Incident Response
    10. Application Security
    11. Data Security and Encryption
    12. Identity, Entitlement, and Access Management
    13. Security as a Service
    14. Related Technologies
    15. ENISA Cloud Computing: Benefits, Risks, and Recommendations for Information Security

- CASP+ (CompTIA Advanced Security Practitioner): Certificación ofrecida por CompTIA (Computing Technology Industry Association). Consta de los siguientes temas:
    1. Enterprise security
    2. Risk management and incident response
    3. Research and analysis
    4. Integration of computing
    5. Communications and business disciplines
    6. Technical integration of enterprise components

- Security+ : Certificación ofrecida por CompTIA. Consta de los siguientes temas:

1. Attacks, Threats and Vulnerabilities
2. Architecture and Design
3. Implementation
4. Operations and Incident Response
5. Governance, Risk, and Compliance

- CISM (Certified Information Security Manager): Certificación ofrecida por ISACA (Information Systems Audit and Control Association). Consta de los siguientes temas:
    1. Information Security Governance
    2. Information Risk Management
    3. Information Security Program Development and Management
    4. Information Security Incident Management

- CISA (Certified Information Systems Auditor): Certificación ofrecida por ISACA. Consta de los siguientes temas:
    1. Information Systems Auditing Process
    2. Governance and Management of IT
    3. Information Systems Acquisition, Development and Implementation
    4. Information Systems Operations And Business Resilience
    5. Protection of Information Assets

- GSEC (GIAC Security Essentials): Certificación ofrecida por GIAC (Global Information Assurance Certification). Consta de los siguientes temas:
    1. Active defense
    2. Cryptography
    3. Defensible network architecture
    4. Incident handling and response
    5. Linux security
    6. Security policy
    7. Windows: access controls, automation, auditing, forensics, security infrastructure, and securing network services

- GPEN (GIAC Penetration Tester): Certificación ofrecida por SANS (SysAdmin Audit, Networking and Security Institute) a través de GIAC. Consta de los siguientes temas:
    1. Comprehensive Pen Test Planning, Scoping, and Recon
    2. In-Depth Scanning
    3. Exploitation
    4. Password Attacks and Merciless Pivoting
    5. Domain Domination and Azure Annihilation
    6. Penetration Test and Capture-the-Flag Workshop

- GWAPT (GIAC Web Application Penetration Tester): Certificación ofrecida por SANS a través de GIAC. Consta de los siguientes temas:
    1. Introduction and Information Gathering
    2. Content Discovery, Authentication, and Session Testing
    3. Injection and XXE
    4. XXE
    5. CSRF, Logic Flaws and Advanced Tools
    6. Capture the Flag

II.4 Educación

"La educación es la transmisión de conocimientos a una persona para que ésta adquiera una determinada formación" (Oxford Languages). Durante la última década las modalidades de educación han cambiado de una forma bastante acelerada gracias a los avances tecnológicos, trayendo al mundo la educación en línea, hasta el punto de ser sumamente popular y utilizada en la actualidad.

> "La era digital revolucionó muchos aspectos de la vida cotidiana y el sector educativo no fue ajeno a ello, puesto que años atrás los estudiantes solamente podían acceder a la educación de forma presencial. En la actualidad, gracias a los avances tecnológicos e implementación de las TIC (Tecnologías de la Información y Comunicación), las personas pueden tener acceso a la educación en línea desde sus propias casas" (Universidad Internacional de La Rioja, 2020).

II.4.1 Educación en línea

"La educación en línea —o también conocida como educación a distancia— es una forma innovadora de aprender y enseñar que se adapta a diferentes niveles y estudios" (Universidad Internacional de la Rioja, 2020). La educación en línea se ha vuelto extremadamente popular en los últimos años, para muchos se vuelve una opción complementaria a la educación tradicional, mientras que otros recurren a medios de educación en línea con el objetivo de hacer de ellos la principal fuente para su formación profesional. Con el avance de la tecnología y el desarrollo de nuevos modelos de negocios, han surgido nuevas herramientas y modalidades en el marco de la educación en línea, tales como los Sistemas de gestión de aprendizaje, los Cursos Abiertos Masivos Online (MOOC), las universidades virtuales y las insignias (badges).

II.4.1.1 Sistemas de gestión de aprendizaje (Learning Management System LMS)

Según Muñoz Arteaga, Álvarez Rodríguez, Osorio Urrutia y Cardona Sala, "Un sistema de gestión de aprendizaje es una aplicación residente en un servidor de páginas web en la que se desarrollan las acciones formativas". Los LMS cumplen el propósito de facilitar la educación en línea, a través de la estandarización y estructuración del modelo educativo. Los LMS aportan funciones de mucha utilidad, como por ejemplo: Permiten crear y almacenar en una base de datos los módulos de aprendizaje del programa a seguir, almacenar el material didáctico según su módulo correspondiente para que los estudiantes puedan revisarlo y organizar y programar evaluaciones con preguntas de tipo selección simple y selección múltiple, hasta de tipo de desarrollo.

II.4.1.2 Cursos Abiertos Masivos Online (MOOC)

Un Curso Abierto Masivo Online (Massive Online Open Course, MOOC) es una modalidad de curso de educación en línea en la que los estudiantes se inscriben, usualmente por un precio de inscripción, y consiguen acceso a material didáctico y actividades que les permiten formar los conocimientos por los que se inscribieron y obtener un certificado al completar el material. Según la Universidad Autónoma de Barcelona, un Curso Abierto Masivo Online "se trata

de un curso a distancia, accesible por internet, al que se puede apuntar cualquier persona y no tiene límite de participantes".

II.4.1.2.1 Coursera

Coursera es una plataforma de enseñanza online que fue fundada en 2012 por dos profesores de la Universidad de Stanford, que cuenta con más de dos mil cursos de distintas temáticas, impartidos en 29 países y por 147 instituciones. El sitio cuenta con una amplia oferta de cursos en seguridad de la información, dictados por distintas organizaciones, desde empresas reconocidas como IBM o Google, hasta prestigiosas instituciones universitarias.

II.4.1.3 Insignias (Badges)

Una insignia (badge) es un indicativo que señala una específica área o herramienta de conocimiento en una certificación digital. Según Google Cloud Certification "Una insignia de habilidad mide el conocimiento de un individuo sobre un producto o servicio específico y prueba su capacidad para aplicar ese conocimiento en un entorno práctico interactivo". Los portadores de certificaciones de cursos suelen colocarlas en su currículum o en sus perfiles en plataformas digitales. Estas insignias ayudan a identificar puntualmente las competencias desarrolladas durante dicha certificación.

II.4.1.4 Proctoring

Es una técnica que permite hacer exámenes de forma remota y monitorearlos de modo que pueda evitarse el fraude. Según Martínez López et al (2018), "el *proctoring* permite la realización de las pruebas en lugar donde el estudiante se encuentre y que se pueden monitorizar desde sitios diferentes". Con el auge de la educación en línea, este tipo de prácticas se ha vuelto más común y necesaria en la realización de evaluaciones virtuales. Además, el *proctoring* no sólo se limita a la vigilancia a través de recursos telemáticos y "existen navegadores de Internet específicos para el *proctoring* que evitan que el alumno salga de la pantalla del examen y debe hacer la prueba sin poder consultar ninguna otra aplicación o programa en el ordenador" (Alonso, 2020).

II.4.2 Formación en seguridad de la información

La formación en seguridad de la información es la formación que un profesional adquiere en distintas áreas, desde gestión de riesgos hasta operaciones de seguridad. Dicha formación puede adquirirse en varias fuentes, como carreras universitarias, diplomados, certificaciones y cursos de tipo MOOC en línea.

II.4.2.1 Formación en Seguridad de la Información en Venezuela

II.4.2.1.1 Formación universitaria en Venezuela

En Venezuela hay universidades que ofrecen cierto nivel de preparación en seguridad de la información, algunas como parte del pensum de carreras relacionadas con la informática, y otras como un diplomado o maestría.

II.4.2.1.1.1 Universidad Metropolitana (UNIMET)

En la Universidad Metropolitana (UNIMET), la Facultad de Ingeniería ofrece la carrera de Ingeniería de Sistemas bajo la dirección de la Escuela de Sistemas. Dentro del plan de estudio de la carrera de Ingeniería de Sistemas, está la materia Seguridad de la Información. Tiene como objetivo que el estudiante no sólo conozca de seguridad informática, sino de la Seguridad de la Información, diferenciándose porque busca que el estudiante conozca todas las formas de salvaguardar la información desde el punto físico, técnico y administrativo, preparándose para posibles ataques y planificando métodos de acción. La asignatura contiene 16 temas a elegir, de los cuales el estudiante sólo tiene que revisar 8 de estos y realizar el examen correspondiente por cada tema. Estos son:

1. Fundamentos de Seguridad de la Información
2. Amenazas, vulnerabilidades y riesgos.
3. Ataques y delitos informáticos.
4. Inseguridad en redes y aplicaciones web.
5. Gestión de Seguridad de la Información.
6. Auditoría de seguridad, hacking ético y pruebas de penetración.
7. Forénsica digital, ley y ética.
8. Seguridad física y ambiental.

9. Defensa contra fallas, accidentes y desastres.
10. Defensa contra intrusos y barreras de protección.
11. Criptografía y protección de la confidencialidad.
12. Integridad y autenticidad de la información.
13. Autenticación de personas y control de acceso.
14. Seguridad en redes y en internet.
15. Seguridad en comunicaciones inalámbricas.
16. Seguridad en voz sobre IP y telefonía por internet.

II.4.2.1.1.2 Universidad Católica Andrés Bello (UCAB)

En la Universidad Católica Andrés Bello (UCAB), la Facultad de Ingeniería ofrece la carrera de Ingeniería Informática bajo la dirección de la Escuela de Informática.

El pensum de la carrera contiene la asignatura Seguridad Computacional, destinada a que los ingenieros informáticos mantengan la integridad del software y de todos los trabajadores de una compañía. Este curso posee las siguientes unidades de aprendizaje:

1. Principios y conceptos básicos de seguridad.
2. Criptografía simétrica y de clave pública.
3. Autenticación y firma digital.
4. Certificación digital.
5. Seguridad en redes.
6. Ataques y medidas preventivas y correctivas.

II.4.2.1.1.3 Universidad Central de Venezuela (UCV)

La Facultad de Ciencias de la UCV ofrece la carrera de Licenciatura en Computación, adscrita a la Escuela de Computación. Se ofrece la materia electiva de “Seguridad en Sistemas de Redes”, dirigida principalmente a los estudiantes de computación que decidan dedicarse al área de redes y sistemas, y exige como requisito haber cursado la materia Redes de Computadoras. El contenido de la asignatura es:

1. Fundamentos básicos de la seguridad de redes.

2. Amenazas y ataques.
3. Criptología convencional o simétrica.
4. Criptología de clave pública o asimétrica.
5. Integridad, autenticación y firmas digitales.
6. Seguridad en redes inalámbricas y en IP.

II.4.2.1.1.4 Universidad Simón Bolívar (USB)

La Coordinación de Ingeniería de Computación de la USB ofrece la carrera de Ingeniería de Computación, donde se dicta la asignatura "Criptografía y Seguridad de Datos", de corte electivo. El contenido de la asignatura es:

1. Introducción.
2. Criptografía.
3. Seguridad en redes.
4. Firewalls.
5. Temas adicionales.

II.4.2.1.1.5 Universidad Nacional Experimental de las Telecomunicaciones e Informática (UNETI)

Esta universidad está en la espera de la aprobación por el ente ministerial de la Especialización, Maestría y Doctorado en Seguridad de la Información, la cual a nivel de especialidad tiene cuatro menciones: Auditoría de Seguridad de la Información, Ciberseguridad, Informática Forense y Gestión y Control de Seguridad de la Información.

II.4.2.1.2 Cursos y Certificaciones

En Venezuela hay institutos que ofrecen cursos y certificaciones en seguridad de la información:

II.4.2.1.2.1 CENDITEL

La fundación CENDITEL (Centro Nacional de Desarrollo e Investigación en Tecnologías Libres), que forma parte del Ministerio para el Poder Popular para Ciencia y Tecnología, ofrece distintos cursos el área de informática, así como un curso de Seguridad de la Información que consta de los siguientes módulos:

- Módulo 1. Elementos Básicos sobre Seguridad de la Información

- Módulo 2. Aspectos Estratégicos sobre Seguridad de la Información
- Módulo 3. Lo Virtual bajo la mirada del Derecho

II.4.2.1.2.2 Diplomado STIT

El Diplomado STIT es un curso de especialización en Venezuela, con una duración de 160 horas académicas que se cubren en 13 semanas. Un alto porcentaje del tiempo es dedicado a actividades prácticas de laboratorio y al adiestramiento mediante talleres.

- Requisitos de ingreso:

  El aspirante debe poseer título universitario o de técnico superior, disponer de un equipo de computación con acceso a Internet y poseer conocimiento instrumental del idioma inglés. Además es deseable cierta experiencia en el área de informática y telecomunicaciones, redes y protocolos (especialmente TCP/IP), así como familiaridad con sistemas operativos (Windows, Linux).

El contenido del diplomado STIT está estructurado en los siguientes módulos:

- Módulo 1: Introducción a la Ciberseguridad

  1.1. Fundamentos de la Seguridad de la Información
  1.2. Amenazas, Vulnerabilidades y Riesgos
  1.3. Ataques y Delitos Informáticos
  1.4. Inseguridad en Redes y en Aplicaciones Web

- Módulo 2: Gestión de Seguridad de la Información

  2.1. Planificación de la Seguridad y Gestión de Riesgos
  2.2. Políticas, Normas y Estándares de Seguridad
  2.3. Seguridad Física, Electrónica y Ambiental
  2.4. Defensa contra Fallas, Accidentes y Desastres
  2.5. Planes de Contingencia y Continuidad de Operaciones

- Módulo 3: Auditoría de Seguridad, Gestión de Incidentes e Investigación Forense

3.1. Auditoría de Redes y Sistemas
3.2. Escaneo de Puertos y Evaluación de Vulnerabilidades
3.3. Hacking Ético y Pruebas de Penetración
3.4. Gestión de Incidentes de Seguridad
3.5. Forénsica Digital, Ley y Ética

- Módulo 4: Seguridad Aplicada a Redes y Sistemas

4.1. Defensa contra Intrusos y Barreras de Protección
4.2. Criptografía y Protección de la Confidencialidad
4.3. Integridad y Autenticidad de la Información
4.4. Autenticación de Personas y Control de Acceso
4.5. Seguridad en Redes y en Internet
4.6. Seguridad en Comunicaciones Inalámbricas
4.7. Seguridad en Voz sobre IP y Telefonía por Internet

II.4.2.2 Formación en seguridad de la información en España e Iberoamérica

Existen numerosas fuentes de formación en seguridad de la información, desde cursos de instituciones privadas hasta instituciones universitarias.

II.4.2.2.1 Universidad Carlos III de Madrid

Es una universidad pública española con sede en la comunidad autónoma de Madrid, fundada en 1989. Ofrece un máster universitario en Ciberseguridad para realizarse de forma presencial en el campus de Madrid, el cual busca que los estudiantes adquieran conocimientos científicos y tecnológicos avanzados sobre ciberseguridad, enfocándose en 3 bloques principales: técnicas de ciberataque, técnicas de ciberdefensa y comunicaciones seguras y gestión de la ciberseguridad. El máster puede ser orientado hacia dos tipos de formación según lo prefiera el estudiante: Ingeniería de Sistemas Seguros o Analista de Ciberseguridad. Esto lo haría según las materias optativas que escoja el estudiante, con un total de 4 materias optativas. Para culminar la maestría es necesario realizar un trabajo final. Dicho máster tiene una duración de 2 cuatrimestres. Las asignaturas son las siguientes:

Cuatrimestre 1

- Comunicaciones Seguras
- Explotación de Sistemas Software
- Protección de Datos
- Sistemas de Ciberdefensa
- Técnicas de Ciberataque
- Seminario I
- Ciberdelitos, Ciberterrorismo y Ciberguerra (Optativa)
- Análisis de Riesgos en Ciberseguridad (Optativa)

Cuatrimestre 2

- Identificación y Autenticación
- Gestión y Administración de la Ciberseguridad
- Seminario II
- Ingeniería de Sistemas Seguros (Optativa)
- Arquitecturas Seguras (Optativa)
- Seguridad en Sistemas y Comunicaciones Móviles (Optativa)
- Análisis e Ingeniería de Malware (Optativa)
- Amenazas persistentes y fugas de Información (Optativa)
- Análisis Forense de Sistemas Informáticos (Optativa)

II.4.2.2.2 Universidad de Buenos Aires (UBA)

Es una universidad pública argentina con sede en la ciudad de Buenos Aires y fue fundada en 1821. La Facultad de Ciencias Económicas de la Universidad, en conjunto con la Escuela Nacional de Inteligencia, dicta una maestría en Ciberdefensa y Ciberseguridad que tiene una duración de 2 años. En estos 2 años el estudiante adquiere una instrucción ética y formal sobre la programación, los algoritmos y el uso de las redes, viendo materias como Tecnología de Redes I o Malware I, que instruyen al estudiante en el uso de las redes de información y los distintos tipos de malware, al igual que hay materias tan específicas como Ciber Ataques masivos a Sistemas de Información. Para finalizar la maestría es necesario realizar una tesis o proyecto de grado. Las materias a cursar son las siguientes:

Asignaturas de formación general

- Tecnología de la Información, ética y normativa jurídica (32hs.)
- Introducción al gerenciamiento innovador (entrepreneurship) (16 hs.)
- Introducción a los paradigmas de programación (64 hs.)
- Tecnología de la Información (64 hs.)

Asignaturas fundamentales

- Introducción a la Criptología (32 hs.)
- Evolución de la Tecnología Militar hasta el enfoque “Network-Centric Warfare” (16 hs.)
- Tecnología de Redes I (32 hs.)
- Malware I (16 hs.) +
- Fundamentos y Gerenciamiento de la Ciberdefensa y de la Ciberseguridad (32 hs.)
- Ciberataques masivos a Sistemas de Información (16 hs.)

Asignaturas específicas

- Principios y enfoques de Diseño de Software Seguro (32 hs.)
- Proyecto sobre Principios y enfoques de Diseño de Software Seguro (32 hs.)
- Teoría Organizacional y Psicología Organizacional (16 hs.)
- Diseño y Desarrollo de la “Data Exchange Layer” en ambientes de Gobierno (16 hs.)
- Data Mining – Data warehousing – Big Data (48 hs.)
- Tecnología de Redes II (32 hs.)
- Seguridad en Redes de Computadoras (32 hs.)
- Malware II (16 hs.)
- Talleres de Investigación Supervisada y/o Tutoriales en Aspectos Operativos de Ciberdefensa y Ciberseguridad (160 hs.)

II.4.2.2.3 Universidad de Los Andes (Colombia)

Esta Universidad cuenta con un programa especializado en ciberseguridad bajo la plataforma en línea Coursera. El programa consta de 3 cursos:

1. **Principios y Regulaciones de Seguridad de la Información**: Es el curso principal y permite que el estudiante tenga los conocimientos básicos sobre la Seguridad de la Información y sus fundamentos.

2. **Vulnerabilidades y pruebas de penetración**: Permite al estudiante tener una mejor noción sobre las vulnerabilidades y entender las amenazas de los ciberataques a través de pruebas de penetración.

3. **Seguridad en la red**: Este curso busca que el estudiante aprenda sobre la arquitectura de ciberseguridad para las redes y pueda defender las redes de computadoras, el host y manejar de incidentes.

El programa sugiere que se estudien 4 horas por semana, con un total de 3 meses. Al finalizar cada curso, el estudiante obtiene una certificación y al finalizar la especialización se entrega otro certificado indicando que el estudiante culminó la especialización.

II.4.2.2.4 Universidad Rey Juan Carlos

Es una universidad pública española con sede en la comunidad autónoma de Madrid y fundada en 1996. Ofrece un máster de duración de 1 año en Ciberseguridad y Privacidad, dictado completamente en línea. El máster busca que los estudiantes recién graduados obtengan competencias en seguridad informática, tal como la búsqueda de vulnerabilidades, cifrado y seguridad de los datos entre otros, generando un perfil muy transversal dentro de la seguridad de la información. El plan de estudios es el siguiente:

- Criptografía y criptoanálisis
- Redes y comunicaciones seguras
- Explotación de vulnerabilidades
- Software seguro
- Ingeniería del malware
- Privacidad y anonimato
- Gestión de identidades y accesos
- Ciber-inteligencia
- Dirección de seguridad y gestión del ciberriesgo
- Trabajo de fin de máster

II.4.2.2.5 Instituto Internacional de Estudios en Seguridad Global (INISEG)

El Instituto Internacional de Estudios en Seguridad Global (INISEG) es una institución educativa internacional fundada en 2017 en España. En materia de seguridad de la información, ofrece los siguientes títulos en modalidad virtual: Máster Universitario en Ciberseguridad, Análisis e Ingeniería, Máster Universitario en Ciberseguridad, Ciberterrorismo y Ciberguerra y Máster Universitario en Dirección y Gestión de la Ciberseguridad. Los títulos emitidos por la INISEG cuentan con el aval de la Universidad Telemática Pegaso, una universidad privada de educación a distancia con sede en Italia.

II.4.2.2.6 Universidad Internacional de la Rioja (UNIR)

Es una universidad privada española de educación en línea cuya sede central está en la ciudad de Logroño, fundada en 2008, con títulos avalados por la Agencia Nacional de Evaluación de la Calidad y Acreditación de España. La UNIR tiene un máster en Seguridad Informática impartido de forma completamente virtual, el cual busca preparar al estudiante a realizar análisis técnicos de los sistemas en conjunto con la formación ética y legal que necesita un experto en seguridad de la información, y también materias que vinculan la criptografía y la búsqueda de vulnerabilidades en los sistemas. Este máster tiene una duración de 1 año distribuidos en dos cuatrimestres, con un total de 60 créditos y un trabajo de fin de máster. Las asignaturas a cursar son las siguientes:

Primer cuatrimestre

- Aspectos legales y regulatorios
- Gestión de la seguridad
- Seguridad en redes
- Seguridad en sistemas operativos
- Análisis forense
- Criptografía y mecanismos de seguridad
- Análisis de vulnerabilidades

Segundo cuatrimestre

- Análisis de riesgos legales
- Auditoría de la seguridad
- Seguridad en aplicaciones online y bases de datos
- Seguridad en el software
- Delitos informáticos
- Prácticas en empresa
- Trabajo fin de máster

II.4.2.2.7 Campus Internacional de Ciberseguridad

Es una universidad en línea, que forma parte de la ENIIT Business School, y es una de las mayores escuelas de negocios especializadas en tecnología. Ofrece distintos títulos, como el Máster en Ciberseguridad avalado por la Universidad Católica de Murcia.

- Requisitos de ingreso: Diplomado, licenciado o graduado universitario o, en su defecto, debe poder acreditar una experiencia profesional (relacionada con las TICs en general) de al menos 5 años mediante certificado sellado de la/las empresas en las que ha trabajado. En caso de no poseer título universitario ni 5 años de experiencia en el sector, se puede acceder al máster igualmente, recibiendo al finalizar un certificado.

II.4.2.3 Principales cursos en seguridad de la información

Habiendo mencionado algunas de las instituciones en España e Iberoamérica, vamos a mencionar algunos cursos en un contexto más internacional.

II.4.2.3.1 Tech Universidad Tecnológica

Es una universidad en línea, catalogada por Forbes como la mejor universidad en línea. Ofrece un curso de especialización llamado Seguridad de la Ingeniería de Software y cuenta con un amplio temario, que puede ser cubierto por 6 meses, teniendo vigencia y relevancia a nivel de toda América Latina, Estados Unidos, España y Portugal. El temario de este curso se divide en 4 módulos de la siguiente forma:

1. Gestión de la Seguridad.

2. Seguridad en el Software.
3. Auditoría de Seguridad.
4. Seguridad en Aplicaciones Online.

II.4.2.3.2 Rochester Institute of Technology (RIT)

Es una universidad privada con sede en el estado de New York y fundada en 1829. El RIT, por medio de la plataforma en línea edX, ofrece un curso llamado Cybersecurity Fundamentals, con una duración estimada de 80 horas, distribuidos en 8 semanas. Cubre los conceptos generales, criptografía y la seguridad en las redes, así como la detección y prevención de cibercriminales y el malware, contando también con una parte de informática forense.

II.4.2.3.3 Cisco Cybersecurity Pathway

Cisco posee una ruta de aprendizaje que consta de 6 cursos, de los cuales, los 2 primeros pueden verse de forma virtual y gratuita, pero igualmente todos pueden verse de forma presencial en una academia hermanada con Cisco. Esta ruta consta de los siguientes cursos:

1. Introduction to Cybersecurity.
2. Cybersecurity Essentials.
3. CCNA Cybersecurity Operations.
4. Cloud security.
5. Network security.
6. IoT Fundamentals.

II.4.2.3.4 Platzi

Platzi es una plataforma de educación en línea que cuenta con una gran cantidad de cursos y contenido relacionado a las nuevas tecnologías en informática y diseño, con más de 2.6 millones de alumnos en toda Hispanoamérica. Entre la variedad de cursos que ofrece, hay una titulación de Seguridad Informática, que se completa al finalizar 17 cursos de alrededor de 4 horas cada uno, que sería un total de 68 horas aproximadamente. Estos cursos van desde la Introducción a la Línea de Comandos, pasando por temas como Introducción la Ingeniería Social, hasta cursos más avanzados como

Administración de Servidores Linux, Fundamentos de Pentesting, Hacking Ético e Informática Forense, Análisis del Malware.

II.4.2.3.5 INFOSEC Institute

Es un instituto de Seguridad de la Información con sede en Estados Unidos que permite a las empresas entrenar a sus empleados en Seguridad de la Información. Mediante la plataforma n línea Coursera ofrece distintos programas especializados en Informática Forense contando con los siguientes cursos:

- Digital Forensics Concepts
- Windows OSForensics
- Windows Registry Forensics

También existe, entre otros, un programa especializado llamado Advanced Python Scripting for Cybersecurity con una duración de 10 horas, que contiene los siguientes cursos:

- Advanced Python - Reconnaissance
- Establishing Command-and-Control and Finding Credentials
- Defensive Python

II.4.2.3.6 Cybersecurity MasterTrack Certificate

Es un certificado que ofrece la Universidad Estatal de Arizona, de Estados Unidos, tras completar tres de sus seis cursos, lo cual dura de seis a nueve meses. Los cursos son:

- Information Assurance and Security
- Applied Cryptography
- Software Security
- Advanced Computer and Network Security
- Distributed and Multiprocessor Operating Systems
- Accelerated Applied Security

II.4.2.3.7 New York University (NYU)

Es una universidad privada con sede en la ciudad de Nueva York, Estados Unidos, que fue fundada en 1831. La NYU posee un máster en ciberseguridad. donde el estudiante cursa en 1 año un total de 10 materias relacionados a la ciberseguridad, de las cuales 4 son obligatorias, 3 son electivas amplias (BE por las siglas de Breadth Electives), y 3 son electivas profundas (DE por las siglas de Depth Electives), permitiendo que el estudiante tenga el control del conocimiento a adquirir y el tipo de profesional al que se quiere dirigir, contando con un trabajo o proyecto final. Las materias a cursar son:

1. **Cursos de ciberseguridad requeridos**

    - Información, seguridad y privacidad
    - Seguridad de la red
    - Criptografía aplicada
    - Aplicación de la seguridad

2. **Electivas amplias (escoger 3)**

    - Introducción a los sistemas operativos
    - Redes del computador
    - Diseño y análisis de algoritmos I
    - Principios de los sistemas de bases de datos
    - Machine learning
    - Fundamentos de la Informática

3. **Electivas profundas (escoger 3)**

    - Forénsica digital
    - Ingeniería y gestión de la seguridad de los sistemas de información
    - Pruebas de penetración y análisis de vulnerabilidad
    - Proyecto avanzado en informática

CAPÍTULO III: Marco Metodológico

III.1 Tipo de investigación

Según Otero Ortega (p 19) “El proceso de investigación mixto implica una recolección, análisis e interpretación de datos cualitativos y cuantitativos que el investigador haya considerado necesarios para su estudio”.

El enfoque de la presente investigación es de tipo mixto, ya que existen elementos que forman parte del proceso de investigación que son posibles de medir y cuantificar, como por ejemplo: evaluar el interés de los reclutadores en la plataforma de certificación PCSI, midiendo los resultados en una encuesta. Al mismo tiempo, se busca ejecutar pruebas sobre la plataforma PCSI desarrollada para asegurar que funcione correctamente, por lo que su funcionamiento se medirá desde una perspectiva cualitativa.

III.2 Alcance de la investigación

De acuerdo con Cauas (2015) “Este nivel de investigación procura un avance en el conocimiento de un fenómeno, con el propósito de precisar mejor un problema de investigación o para poder generar hipótesis”. Por ello, la presente investigación tiene un alcance exploratorio. Se exploró la situación actual de certificaciones profesionales en Seguridad de la Información con respecto de la preparación ofrecida en estudios universitarios, para así generar y desarrollar una propuesta de sistema de certificación en Seguridad de la Información.

III.3 Variables de la investigación

A continuación se describen las variables utilizadas en el presente trabajo de investigación.

Tabla 1. Variables de investigación

Variable	Tipo	Descripción	Fuente
Pensum de	Cualitativa	Establece los temas, la	Bibliografía

estudios en instituciones		profundidad y los métodos de evaluación de titulaciones en temas relacionados con la informática.	
Interés de los reclutadores	Cuantitativa	Mide el interés de reclutadores y personal de IT en la certificación PCSI	Encuesta
Hosting	Cualitativa	Sus características establecen limitantes para utilizar el tipo de LMS	Requerimientos de los servidores para realizar el hosting

Fuente: Elaboración propia

III.4 Diseño de la investigación

Se trata de un diseño de investigación aplicada, en la que se llevó a cabo un estudio sobre los sistemas de gestión de aprendizaje y de certificación, y cómo esto impactaría en los profesionales de la Seguridad de la Información en Venezuela. Además se compararon las distintas plataformas LMS existentes, como Moodle, Chamilo y eFront. Se tomaron en cuenta distintos factores, empezando por los requisitos mínimos y finalmente se seleccionó Moodle.

III.4.1 Revisión de la bibliografía

La primera etapa de esta investigación consistió en recopilar información sobre las necesidades de las certificaciones profesionales, las formas en las que pueden estructurarse, y sus métodos de evaluación. Para ello se investigó sobre cuáles son las certificaciones en Seguridad de la Información más prestigiosas a nivel global, así como las instituciones que las ofrecen. Se investigó sobre los prerrequisitos que tienen estas certificaciones, las modalidades en que se efectúan las evaluaciones y el contenido que se evalúa.

También se investigaron varias de las universidades más importantes de Venezuela, con el objetivo de elaborar una comparación entre la preparación en Seguridad de la Información ofrecida por estas universidades y la ofrecida en las certificaciones profesionales. De estas universidades, se analizó el plan de estudios de materias relacionadas con la Seguridad de la Información, detallando los temas ofrecidos y modalidades de evaluación.

III.4.2 Diseño de la metodología de evaluación

La investigación sobre las principales certificaciones en Seguridad de la Información mostró que varias de ellas presentan evaluaciones con preguntas de selección múltiple, la cual es una de las funcionalidades más conocidas del LMS seleccionado (esto es Moodle), por lo que se decidió que la metodología de evaluación serán exámenes con preguntas de selección múltiple. Para crear una base de datos se crearon preguntas utilizando como base distintas fuentes, por ejemplo: Clinton, D. (2020) - *Linux Security Fundamentals,* Wiley. Bock, L. (2021) - *Modern Cryptography for Cybersecurity Professionals,* Packt Publishing. Santos, O. (2018) - *Developing Cybersecurity Programs and Policies,* Pearson Education. Seidl, D., & Chapple, M. (2018) - *(ISC)2 CISSP Certified Information Systems Security Professional Official Practice Tests,* Wiley.

Teniendo en cuenta el plan de estudios de las universidades investigadas y en los temas evaluados en las certificaciones mencionadas, se diseñó la certificación PCSI con los siguientes temas:

Tabla 2: Temas de la certificación PCSI

Temas	Subtemas
Fundamentos de la Seguridad de la Información	Objetivos y definiciones principales. Riesgos, vulnerabilidades y amenazas. Identificación y gestión de activos.
Malware y Ciberataques	Tipos de Malware. Software Anti-Malware.

	SQL Injection. XSS y CSRF. DoS y DDoS. DNS Spoofing. Eavesdropping. Phishing. Backdoor. ARP Spoofing. MAC Flooding.
Seguridad en Redes	Fundamentos de Sistemas de Redes. Modelo OSI y Protocolo TCP/IP. Seguridad en Redes Inalámbricas e Internet. VPN. Firewalls.
Gestión de Identidad y Acceso	Dispositivos e Instalaciones. Autenticación Única y Multifactor. Gestión de Sesiones. Control de Acceso Basado en Roles. Ciclo de Vida del Acceso.
Seguridad en Aplicaciones	Metodologías de Desarrollo. Seguridad de los Entornos. Seguridad de Endpoints. Vulnerabilidades en Aplicaciones Web. Prácticas Seguras de Programación.
Criptografía y Confidencialidad de Datos	Métodos Criptográficos. Infraestructura de Clave Pública. Métodos de Gestión de Claves. Firmas Digitales.

Seguridad Ofensiva y Seguridad Defensiva	Análisis y Auditorías de Seguridad. Metodologías y Buenas Prácticas. Respuesta a Incidentes. Pruebas de Penetración.

Fuente: Elaboración propia

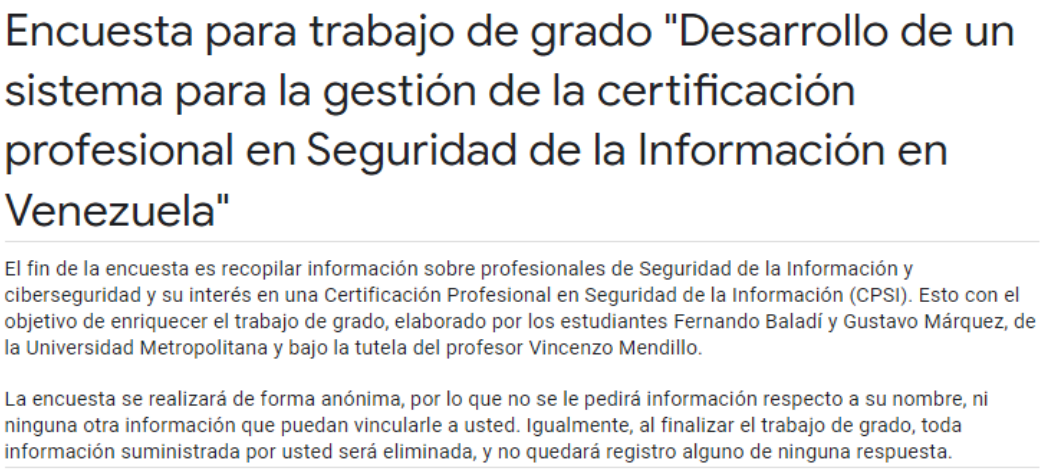
III.4.3 Apreciación de reclutadores

Gran parte de la utilidad de esta investigación es la confianza que podría demostrar un profesional al tener una certificación, ya que de esta manera el reclutador puede conocer qué conocimientos tiene y su experiencia, lo que hace mucho más rápido el proceso de contratación (Ruiz Bueno, 2006), evitando que las empresas tengan que gastar grandes sumas de dinero evaluando ellos mismos a los candidatos.

Para medir la apreciación de los reclutadores se desarrolló una encuesta con la herramienta *Google Forms* dirigida a profesionales en el área de TI, Seguridad de la Información y Ciberseguridad. En la encuesta se colocaron 6 secciones de preguntas de tipo cerrado, “Las preguntas cerradas contienen categorías u opciones de respuesta que han sido previamente delimitadas. Es decir, se presentan las posibilidades de respuesta a los participantes, quienes deben acostarse a éstas” (Fernández Collado et al., 2014, p217).

Figura 1

Título y descripción de la encuesta



Fuente: Elaboración propia

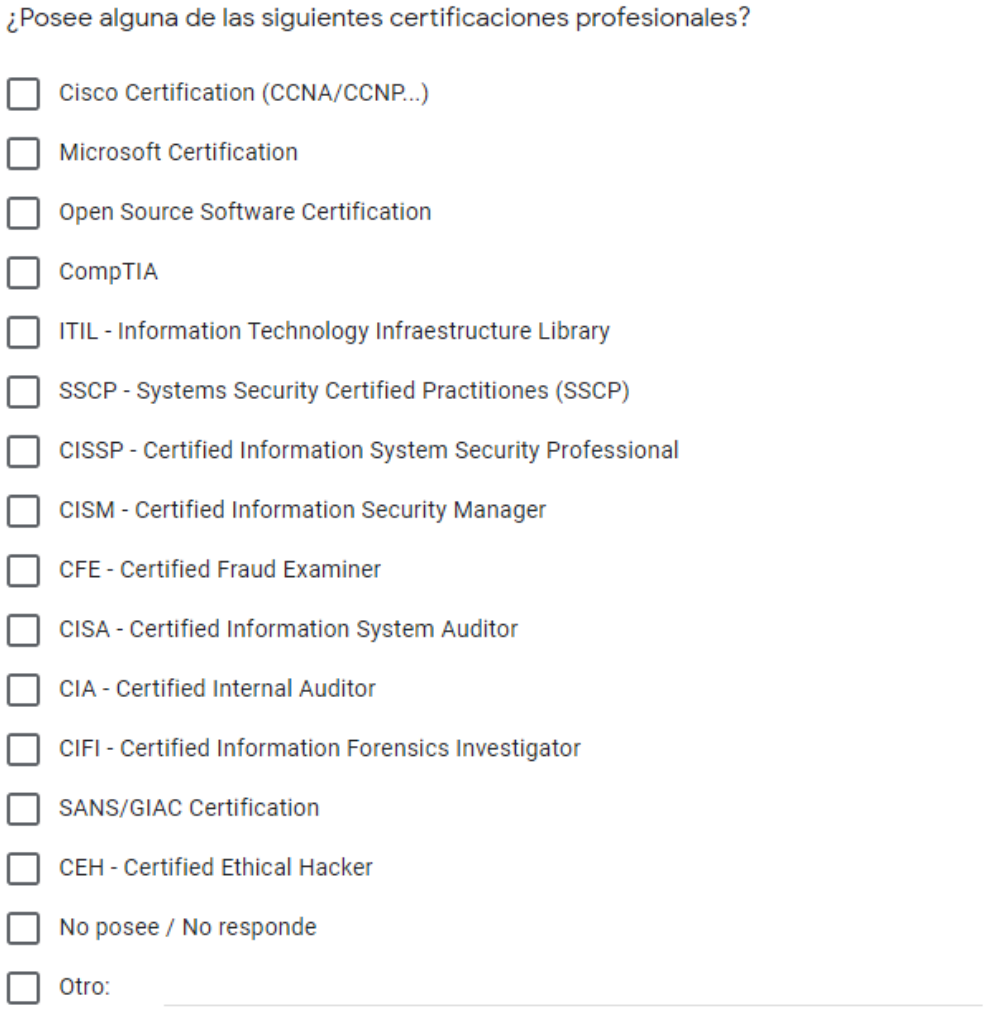
En la primera sección se le pregunta al encuestado “¿Qué tan de acuerdo está con las siguientes oraciones?” y a continuación se le muestra una serie de trece preguntas, a las cuales las posibles respuestas son: Totalmente en desacuerdo, en desacuerdo, ni de acuerdo ni en desacuerdo, de acuerdo y totalmente de acuerdo. Las preguntas que componen esta sección son las siguientes:

- En Venezuela es fácil encontrar buenos profesionales en Seguridad de la Información
- Las certificaciones internacionales son muy buenas para medir el conocimiento del individuo
- Las certificaciones internacionales son muy costosas y poco accesibles
- Una certificación internacional es mejor vista en Venezuela que una nacional
- Es común ver profesionales en Seguridad de la Información con certificaciones internacionales
- El personal certificado es mucho mejor a alguien que no esté certificado
- Una de mis metas es obtener una certificación profesional en Seguridad de la Información
- Un profesional que sólo realice cursos en línea es igual de confiable a que tenga sólo certificaciones profesionales
- Un profesional que tenga maestrías es igual de confiable a que tenga sólo certificaciones profesionales
- Las certificaciones internacionales, al estar en otros idiomas representan un reto para mí
- Preferiría realizar una certificación que se encuentre en español
- Una profesional con certificaciones puede conseguir mejores puestos de trabajo a que uno sin certificaciones
- Un profesional sin certificaciones gana más que un profesional con una o más certificaciones

A continuación se describe el contenido del resto de la encuesta:

Figura 2

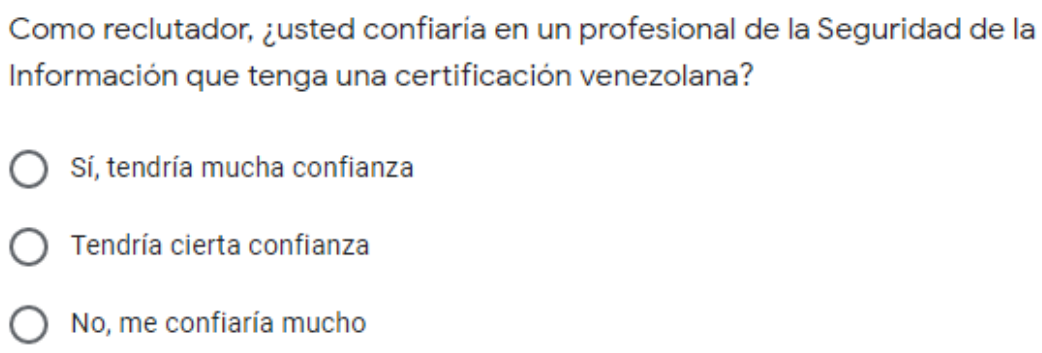
Segunda pregunta de la encuesta



Fuente: Elaboración propia

Figura 3

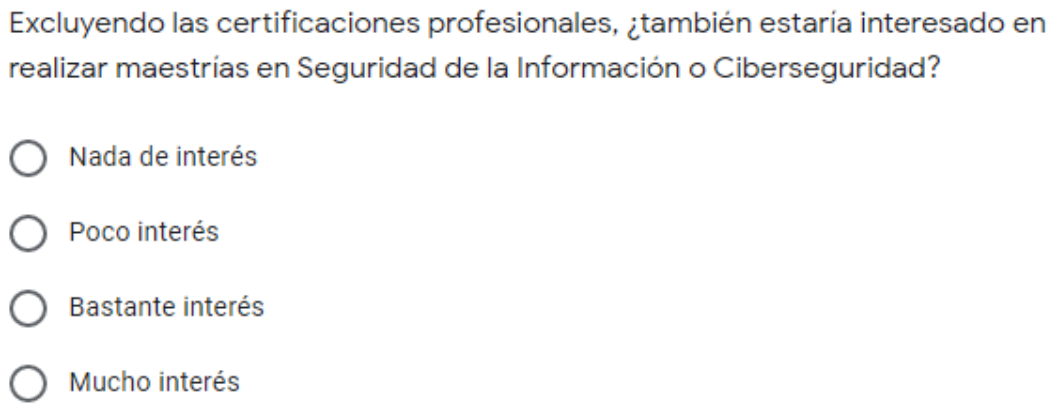
Tercera pregunta de la encuesta



Fuente: Elaboración propia

Figura 4

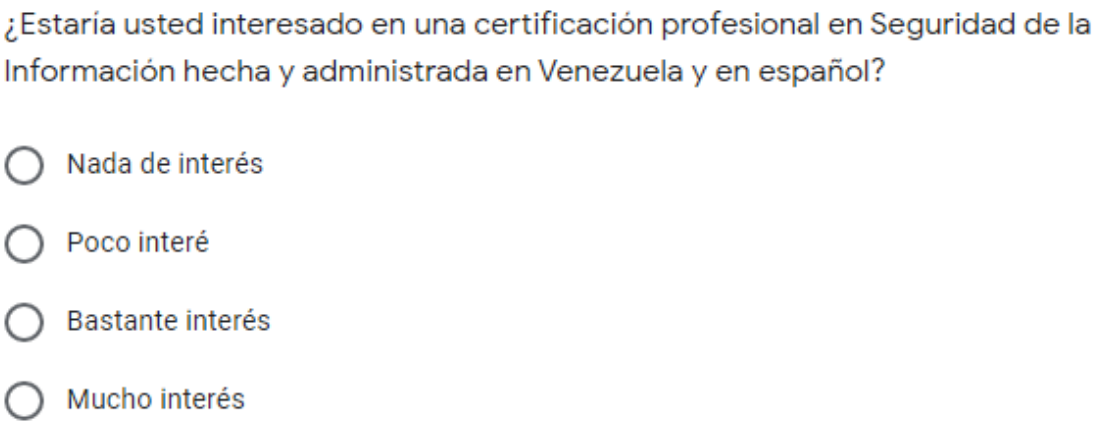
Cuarta pregunta de la encuesta



Fuente: Elaboración propia

Figura 5

Quinta pregunta de la encuesta

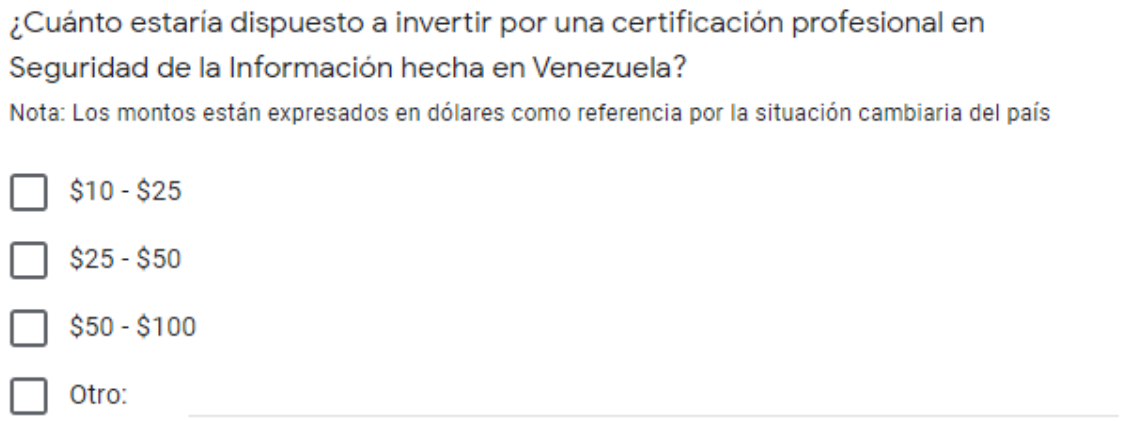


Fuente: Elaboración propia

La pregunta mostrada en la figura 5 permite medir el interés de los reclutadores en la plataforma junto con la certificación diseñada.

Figura 6

Sexta pregunta de la encuesta



Fuente: Elaboración propia

III.4.4 Selección de las tecnologías

En este punto se investigó sobre las distintas tecnologías de gestión de aprendizaje disponibles, con el objetivo de seleccionar la más conveniente para el presente caso de estudio. Por su alta popularidad, sus positivas reseñas y la rápida implementación con el hosting de cPanel que utiliza ASOVESINFO, se tomaron en consideración los siguientes LMS: Moodle, Chamillo y eFront. También se tomaron en cuenta otras plataformas como Classroom, Canvas y Edmodo, sin embargo, para utilizar estos últimos, 3 era necesario realizar la configuración dentro de cada una de las plataformas, sin poder pasarlas a servidores externos.

III.4.4.1 Moodle

Como se mencionó, una de las plataformas analizadas fue Moodle, la cual es un sistema de gestión de aprendizaje de código libre basado en PHP. Es uno de los LMS más famosos y uno de los primeros, siendo lanzado al público en 2002. Moodle es una plataforma utilizada por una gran diversidad de instituciones y universidades en todo el mundo. Según Moodle, en 2021 hay más de 39 millones de cursos.

Su facilidad de instalación y una documentación robusta y traducida por la comunidad a varios idiomas, permite que se pueda entender su uso de forma rápida, así que cualquier administrador puede modificarla y mejorarla. También, al ser software libre, se puede intentar modificar el software a conveniencia propia.

La variedad de plugins e interconexiones con otras aplicaciones permite una gran flexibilidad al momento de realizar cursos o certificaciones. Para efectos de este trabajo de grado, se buscaba un plugin que permitiera generar certificados e insignias, así como un plugin o aplicación que permitiera realizar el proctoring de los exámenes.

Para Moodle se encontraron 2 plugins que facilitan el manejo los certificados y entregar la certificación. También se encontró y probó una aplicación de proctoring llamada Safe Exam Browser, la cual permite realizar los exámenes sin que el usuario pueda hacer trampa.

III.4.4.2 Chamilo

Chamilo es un sistema de gestión de aprendizaje de software libre programado en PHP y JavaScript, que fue lanzado al público en 2010. Es una de las plataformas LMS más utilizadas en el mundo, con más de 28 millones de usuarios en el 2021.

Su facilidad de instalación y uso permite que una gran cantidad de personas lo utilicen y puedan realizar cursos y certificaciones, así como configurar exámenes y tareas. Sin embargo el proctoring no es tan poderoso como el de Safe Exam Browser, ya que permite que se pueda grabar la pantalla y usar cualquier navegador web.

III.4.4.3 Efront

Es un sistema de gestión de aprendizaje que fue de código libre hasta el lanzamiento de su versión paga en 2018, programado en PHP y lanzado al público en el año 2015. A pesar de estar muy extendido su uso y ser de fácil uso, es necesario una licencia paga, lo que limita bastante su uso para realizar la certificación de bajo costo.

Su sistema de proctoring permite grabar con la cámara web y micrófono, pero esto no es suficiente porque el usuario podría no poseer cámara o micrófono. Así mismo, su sistema de proctoring permite el uso de cualquier navegador.

III.4.4.4 Decisión final sobre la plataforma LMS a utilizar

Después de una cuidadosa revisión de la documentación de las tecnologías, los requerimientos, las funcionalidades y el costo, se determinó que Moodle era el LMS más conveniente para el presente trabajo, debido a la facilidad para operarlo y la posibilidad de utilizar otras funcionalidades requeridas de forma gratuita, como entregar certificados y verificarlos o realizar un proctoring bastante robusto.

Se descartó la posibilidad de utilizar Chamilo porque no posee un sistema de proctoring tan robusto y a Efront por ser necesaria la licencia de pago.

III.4.5 Desarrollo del sistema

Para la implementación de la plataforma se utilizó el hosting de Google Cloud mediante el servicio de crédito gratuito por USD 400,00 durante los primeros 90 días de uso, lo que permitió que se generara una máquina virtual en la que corre Ubuntu y una imagen de Moodle 3.11.5 distribuida por Bitnami de forma gratuita. Esto permitió mantener hosteada la plataforma y hacerla accesible a cualquier persona mediante el dominio de enlace www.cpsi.one.

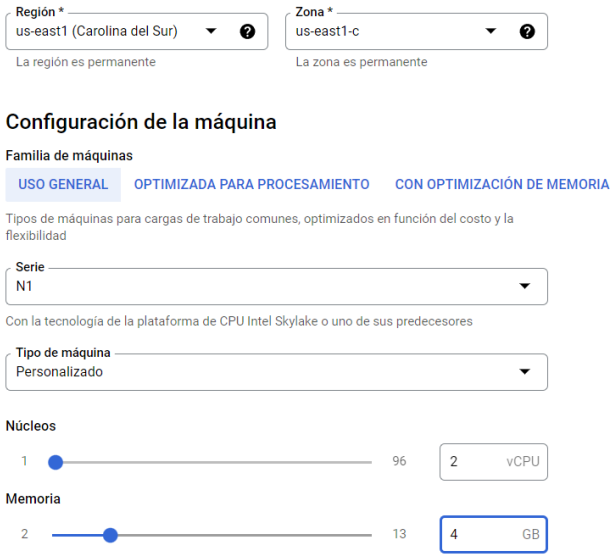
Para instanciar la máquina virtual se seleccionó la región us-east1 (Carolina del Sur) por ser una de las más cercanas a Venezuela y más económicas, lo cual abarata los costos en el uso mensual. También se eligió que el CPU a utilizar fuese de la familia de CPU Intel Skylake o anteriores, esto por no demandar una gran cantidad de procesamiento durante su uso. Se seleccionaron 2 núcleos de estos procesadores y 4 GB de memoria.

Estos recursos de la máquina virtual representa aproximadamente USD 43,99 al mes. Sin embargo, después de varios días corriendo, la consola de Google Cloud sugirió que los requerimientos podían bajar a la mitad, esto es 1 núcleo y 2 GB de memoria, por el bajo impacto que tenía utilizar la plataforma.

Esta sugerencia, la cual fue aceptada, bajó el costo mensual aproximadamente a USD 30,00.

Figura 7

Vista de Google Cloud al instanciar una nueva máquina virtual

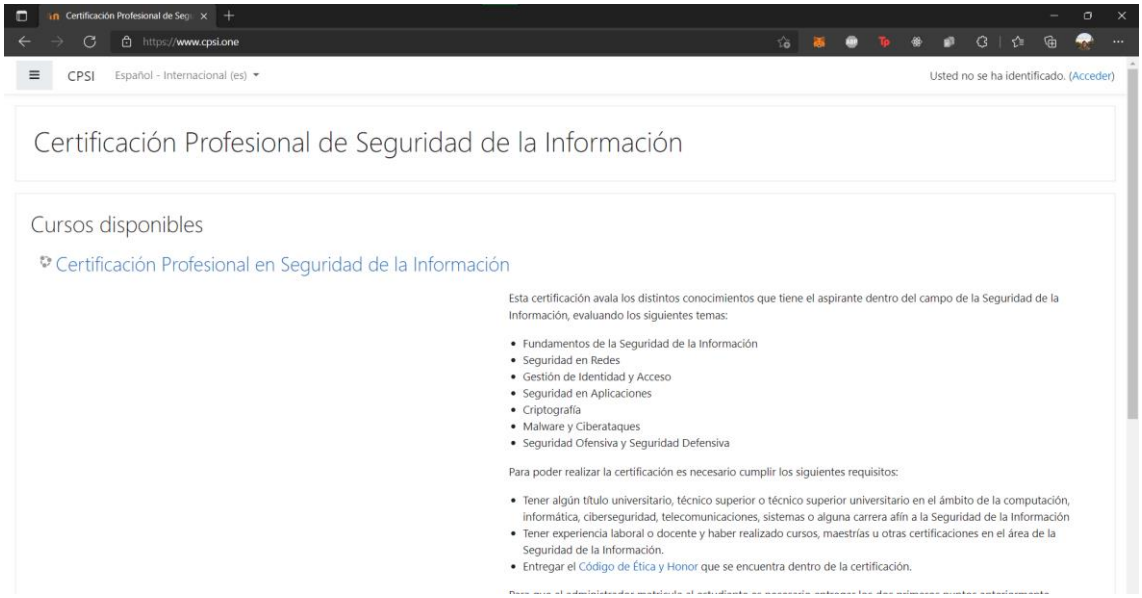


Fuente: Elaboración propia

Al entrar en la página principal de la plataforma ya operativa, se muestran los detalles de la Certificación Profesional en Seguridad de la Información. El interesado puede registrar y confirmar el correo, pero es necesario que el administrador del sitio matricule al interesado. Esto se decidió así para que el administrador pueda revisar los requisitos antes de que el interesado pueda avanzar en el proceso de certificación.

Figura 8

Página principal de la certificación



Fuente: Elaboración propia.

Aparte del hosting en Google Cloud, también existen otras alternativas donde se puede hostear Moodle, como Gnomio, el cual, a pesar de tener versiones pagas, tiene una versión gratuita pero que, debido a sus limitaciones, sirve como demo o para aplicaciones pequeñas. Otra alternativa sería Moodle Cloud, un servicio de hosting ofrecido por Moodle, sin embargo, todas sus versiones son de pago.

III.4.6 Ejecución de pruebas

Como última etapa del proceso de desarrollo, se llevaron a cabo pruebas funcionales para verificar que la plataforma funcione correctamente. Esto se hizo a pesar de que Moodle también realiza en su software pruebas unitarias y pruebas funcionales.

Para dichas pruebas se hizo uso de las distintas funcionalidades de la plataforma, tal como lo haría un atacante y se intentó hacer ediciones o acceder a recursos y exámenes así no tenga permisos el propio usuario. Además, se realizó un análisis de vulnerabilidades mediante la herramienta de auditoría *Acunetix*, con el objetivo de verificar que la plataforma sea segura y no pueda ser atacada por usuarios con intenciones maliciosas.

CAPÍTULO IV: Análisis de Resultados

IV.1 Resultados generales

Se desarrolló y probó una plataforma para la certificación profesional en Seguridad de la Información utilizando Moodle como sistema de gestión de aprendizaje (LMS). Los distintos tópicos de la certificación PCSI y su orden fueron seleccionados basándose en lo que se describió en el capítulo anterior.

La plataforma fue montada en un servidor de Google Cloud, para posteriormente cederlo y traspasarlo a los servidores de ASOVESINFO. La migración se realizaría según la documentación de Moodle, se activaría el modo seguro y se realizarían las copias de seguridad tanto a la base de datos como a los datos que mantiene Moodle.

IV.2 Comparación entre certificaciones internacionales y otras fuentes de estudio

IV.2.1 Comparación de títulos de pregrado

La información recopilada sobre algunas de las principales universidades venezolanas demuestra que las universidades que ofrecen carreras relacionadas con el mundo de la informática, ofrecen materias sobre Seguridad de la Información, aunque algunas sean de categoría electiva.

Podemos observar que, al igual que las distintas certificaciones prestigiosas estudiadas, el contenido de las materias sobre Seguridad de la Información de las universidades nacionales ofrece el apartado de seguridad en redes, ya que este tema es uno de los pilares fundamentales de la seguridad de la información. No obstante, las certificaciones estudiadas ofrecen este tema de una forma más profunda y detallada. Por ejemplo, la certificación CISSP del $(ISC)^2$ estudia como temas específicos Seguridad en endpoints, Funcionamiento del hardware y Dispositivos de control de acceso a la red en su dominio de Comunicación y Seguridad de red, mientras que las universidades estudiadas no mencionan estos temas dentro del plan de estudios de sus asignaturas sobre seguridad de la información.

La certificación CCNA Security tiene un enfoque práctico orientado a soluciones con casos prácticos reales, según Proyecto Universidad Empresa, “Los alumnos aprenderán las habilidades necesarias para instalar, resolver problemas y monitorizar dispositivos de redes para mantener la integridad, confidencialidad y disponibilidad de los datos y dispositivos”. Las universidades estudiadas también presentan contenido práctico y especifican la cantidad de horas prácticas en el contenido de sus asignaturas de seguridad de la información, por ejemplo, las actividades prácticas requeridas para aprobar Seguridad de la Información en la Unimet. Sin embargo, el enfoque práctico en dichas asignaturas es significativamente menor que el de la certificación CCNA.

El tema de IAM (Identity Access Management) es fundamental en la seguridad de la información, ya que con este tipo de técnicas se evita que personal sin autorización manipule información empresarial sensible, entre otras cosas. La certificación CISSP ofrece un amplio apartado de este tema, desde control de acceso físico y lógico, hasta la implementación y gestión de diversos mecanismos de autorización. Las universidades estudiadas también incluyen este tema entre los tópicos de sus asignaturas de seguridad de la información, pero no en la misma profundidad que la certificación CISSP.

Algunas de las certificaciones estudiadas están dedicadas específicamente al tema de seguridad en la nube, como por ejemplo, la certificación CCSK de la Cloud Security Alliance, o la certificación CCSP del (ISC)². Sin embargo, este tema se ve ausente en el plan de estudios de las universidades mencionadas.

IV.2.2 Comparación de títulos especializados

Con respecto a cursos independientes y formación de más alto nivel, como la especialización ofrecida por la UNETI o el diplomado STIT, los planes de estudios son mucho más detallados al tratarse de formación especializada. Las instituciones estudiadas, tanto en Iberoamérica como a nivel más global, demuestran que existe una amplia oferta de maestrías y títulos especializados a nivel de estudios superiores. No obstante, la oferta y facilidad de encontrar este tipo de instituciones a nivel nacional es mucho más limitada que a nivel internacional.

Estas comparaciones nos permiten observar que las universidades estudiadas ofrecen materias sobre seguridad de la información, que, en esencia, contienen los temas principales para conocer sobre seguridad de la información, tales como: Fundamentos de la seguridad de la información, ataques y amenazas, criptografía, seguridad en redes, entre otros. Sin embargo, estas universidades no ofrecen estos temas en la misma profundidad y detalle que lo hacen las principales certificaciones internacionales. De igual forma, tampoco tienen el mismo enfoque práctico que brinda a sus estudiantes un mejor posicionamiento a la hora de optar por posiciones de trabajo en seguridad de la información, lo que confirma la afirmación que suele hacerse sobre aspirantes a puestos de trabajo en seguridad de la información: La formación obtenida en la universidad, ya sea a nivel de pregrado que de postgrado, no suele ser suficiente y hay que complementar con certificaciones profesionales.

IV.3 Evaluación del interés de los reclutadores

Para medir el interés de los reclutadores se aplicó una encuesta a través de *Google Forms*. Dicha encuesta circuló a través de canales de comunicación de personal de TI y de profesionales de la seguridad de la información y de ciberseguridad.

El 44% de los encuestados respondió tener “Mucho interés” en una certificación profesional en Seguridad de la Información hecha y administrada en Venezuela y en español, a lo que otro 44% respondió tener “Bastante interés”, lo que muestra que el 88% de los encuestados demostró interés en la plataforma y la certificación diseñadas en el presente estudio. También, el 66,7% respondió estar dispuesto a pagar entre $50 y $100 para adquirir la certificación descrita.

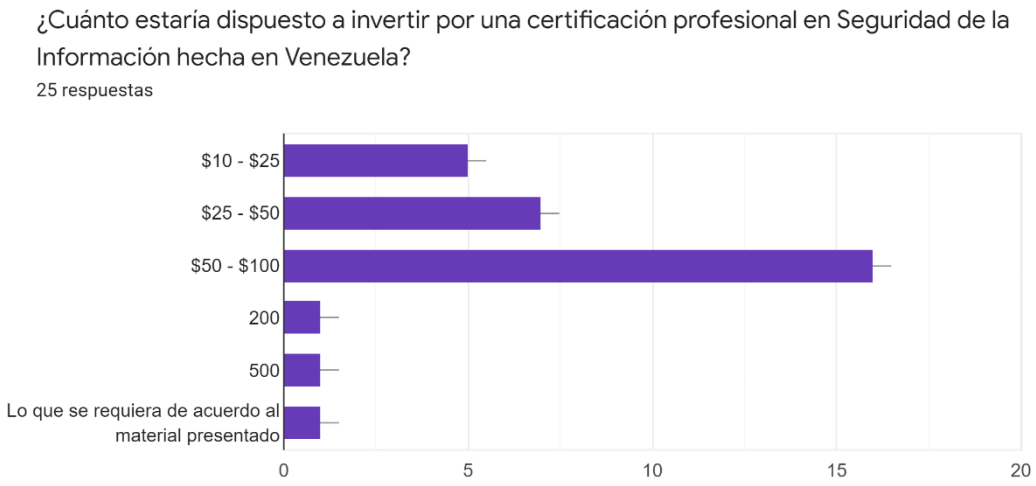
Figura 9

Respuestas de la encuesta sobre el interés por la certificación.

Fuente: Elaboración propia.

Figura 10

Respuesta de la encuesta sobre el precio que debería tener la certificación.



Fuente: Elaboración propia.

Otros resultados arrojados por la encuesta, muestran que el 76,2% de los encuestados respondió “No posee/no responde” cuando se le preguntó si posee una certificación profesional en seguridad de la información.

Figura 11

Respuesta de la encuesta sobre las certificaciones que poseen los encuestados.

Fuente: Elaboración propia

IV.4 Diseño y formato de la certificación

IV.4.1 Diseño de la certificación

La certificación fue diseñada para evaluar los principales tópicos de la Seguridad de la Información. Para cada uno de los tópicos se entrega una insignia al aprobar la evaluación correspondiente. Estos tópicos son los siguientes:

1. Fundamentos de la Seguridad de la Información
2. Malware y Ciberataques
3. Seguridad en Redes
4. Gestión de Identidad y Acceso
5. Seguridad en Aplicaciones
6. Criptografía y Protección de Datos
7. Seguridad Ofensiva y Seguridad Defensiva

Después de finalizar las evaluaciones de los 7 tópicos, se desbloquea una evaluación final, que contiene preguntas de los 7 tópicos anteriormente mencionados. Es ahí cuando finalmente se otorga el certificado al aspirante.

IV.4.2 Requerimientos para el proceso de la certificación

Dentro de los requerimientos está el pago de la inscripción (todavía no se ha decidido el monto). También es necesario que el aspirante deba tener algún título universitario, técnico superior o técnico superior universitario en el ámbito de la computación, informática, ciberseguridad, telecomunicaciones, sistemas o alguna carrera afín a la Seguridad de la Información y experiencia laboral o docente, así como haber realizado cursos, maestrías u otras certificaciones en el área de la Seguridad de la Información. Esto es así para poder filtrar un poco a los aspirantes y que no cualquier persona, sobre todo sin conocimientos, tenga la oportunidad de intentar obtener la certificación.

Después de esto, se matricula al usuario y se le pide que lea el Código de Ética, lo firme y lo envíe para que el administrador de la página pueda validarlo, y así colocarlo como entregado, lo que permitirá que el aspirante a la certificación pueda comenzar a hacer las evaluaciones.

El Código de Ética fue elaborado en base a otros códigos de ética importantes para los profesionales que trabajan en Seguridad de la Información y Tecnologías de la Información, tal como:

- Código de Ética y Conducta Profesional de ACM
- IT Code of Ethics - SysAdmin Audit, Networking and Security Institute (SANS)
- Code of Ethics - International Information Systems Security Certification Consortium (ISC)[2]

De esta forma se insta al aspirante a seguir una conducta modelo y a seguir manteniéndose al día, así como también a que no participe en actividades delictivas ni actividades en las que su profesión sea utilizada para dañar de forma directa o indirecta a otras personas o entes.

IV.4.3 Diseño de las evaluaciones

Para evaluar al candidato se efectúa un examen de 20 preguntas por cada tópico, y 35 preguntas en el examen final, donde cada pregunta contiene varias posibles respuestas y el candidato debe elegir 1 respuesta (en el caso de ser selección simple), o varias respuestas (en caso de ser selección múltiple). Por lo general las preguntas tienen únicamente 4 alternativas de respuesta. En el caso de ser necesario, se colocan más alternativas para las preguntas de opción múltiple.

Cada pregunta se genera de forma aleatoria de uno de los bancos de preguntas separados por tópicos y previamente cargados. De igual forma, las preguntas se muestran sin ningún orden específico, aumentando así la aleatoriedad del examen. Para el examen final se seleccionan 5 preguntas del banco de preguntas de cada tópico, esto es un total de 35 preguntas a responder.

Estos exámenes por tópico cuentan de una duración máxima de 20 minutos y 35 minutos en el examen final. Pasado este tiempo, el examen se evalúa automáticamente con las respuestas seleccionadas.

Para las preguntas de opción múltiple, se decidió colocar una penalización por el 50% del valor de la pregunta si sólo deben seleccionarse 2 respuestas correctas y una penalización del 100% si deben seleccionarse 3 respuestas correctas. Esto es para que el aspirante no seleccione las respuestas al azar, y si se equivoca con la pregunta, pueda notar que no acertó en la respuesta.

Figura 12

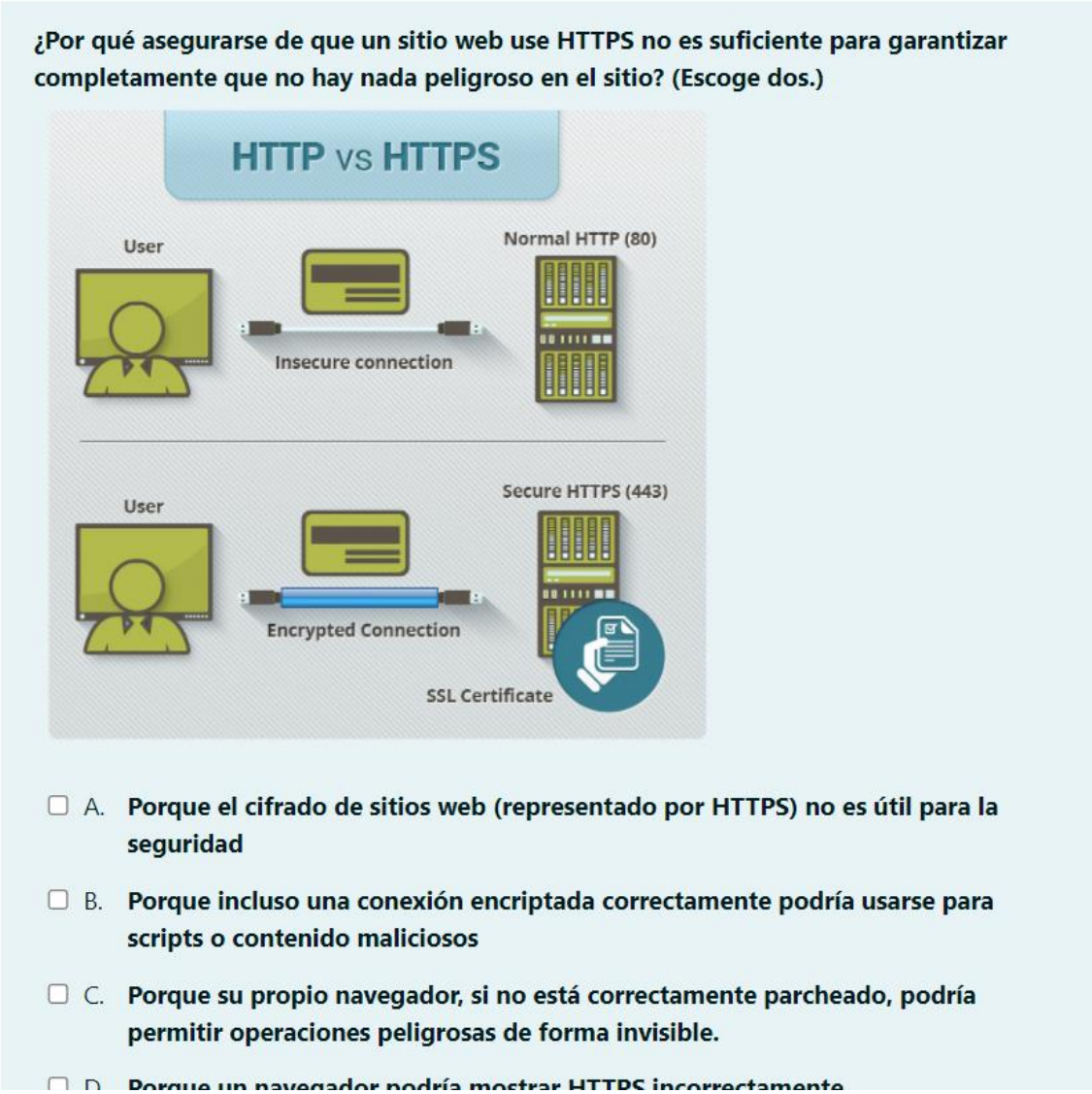
Examen a punto de iniciar

Fuente: Elaboración propia.

Finalmente, para poder obtener una calificación aprobatoria, es necesario responder correctamente el 80% de las preguntas, por lo que en cada tópico el aspirante necesita responder 16 preguntas correctamente y en el examen final son necesarias 28 preguntas correctas. Si el aspirante no logra obtener una calificación aprobatoria, debe ponerse en contacto con el administrador del sitio para asignarle un nuevo intento. Si reprueba el examen, tampoco se le generará la insignia asociada a dicho examen.

Figura 13

Pregunta de ejemplo con imagen



Fuente: Elaboración propia

IV.4.4 Retroalimentación

Buscando el hermetismo, se decidió que el candidato sólo pudiese saber el puntaje obtenido, evitando así cualquier fuga de información sobre las preguntas y respuestas de los exámenes. Así que, al finalizar el intento, el candidato puede ver el puntaje, pero no cuáles fueron las respuestas correctas o incorrectas.

IV.4.5 Proctoring

Para realizar la vigilancia o *proctoring* de los usuarios durante los exámenes, se utiliza una aplicación totalmente compatible con Moodle llamada Safe Exam Browser. Esta aplicación es, esencialmente, un explorador web, pero que limita al usuario a sólo realizar la prueba, bloqueando algunos comandos y otras aplicaciones, impidiendo que se pueda ir a otras pestañas o realizar búsquedas en Internet. También bloquea grabaciones y capturas de pantalla, por lo que evita el filtrado de las preguntas y respuestas de los exámenes.

El programa tampoco permite la navegación por URLs, por lo que sólo se puede navegar por la evaluación tanto como el programa lo permita. Esto evita el riesgo de un ataque mediante inyección de SQL.

Sin embargo, al configurar los exámenes con Safe Exam Browser, se permitió que se visualizara información sobre la red Wi-Fi a la que se está conectado, y poder cambiarla, así como la hora o la cantidad de batería que posee el dispositivo. De ser el caso, el administrador también puede bloquear éstas y otras funcionalidades desde la configuración del examen.

A pesar de que esta aplicación se integra muy bien con Moodle, sigue siendo una aplicación externa que el usuario debe descargar e instalar en su equipo. Tiene la ventaja de que pueda ser descargada desde Windows, macOS y iOS, permitiendo una amplia cantidad de dispositivos desde los cuales se puede realizar el examen.

IV.4.6 Insignias y certificado final

Se decidió entregar una insignia al finalizar cada una de las pruebas. Estas insignias y el certificado son manejados y entregados por dos plugins llamados *Workplace certificate manager* y *Workplace course certificate*.

Técnicamente, las insignias son iguales a los certificados, pero su diseño y su obtención se realizan de formas distintas. El motivo de generar las insignias fue de mantener la motivación del candidato con cada examen que apruebe y que pueda compartir su progreso en la certificación en las redes sociales.

Una desventaja de los distintos plugins encontrados, e incluso de los que se utilizaron, es que la fecha de expiración es una fecha fija, no se puede colocar

como una fecha dinámica con respecto al día de emisión, por lo que constantemente el administrador debe cambiar la fecha de expiración de las insignias y del certificado.

Las insignias y el certificado contienen el nombre y apellido del aspirante, el número de insignia o número de certificación, y un código QR que lleva, a quien lo escanee, al apartado de la página donde se comprueba la autenticidad del documento.

Figura 14

Ejemplo de insignia entregada al administrador

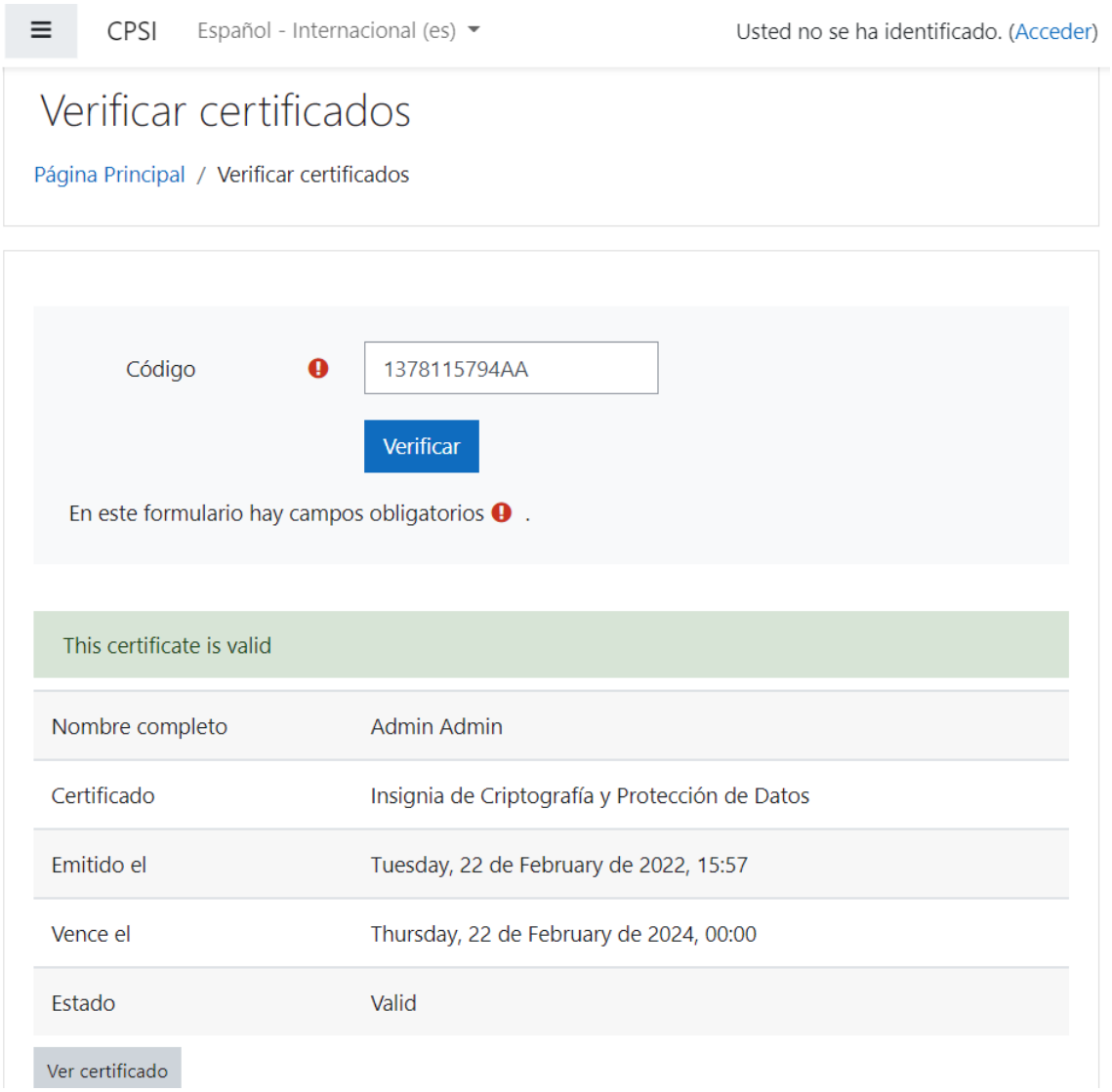
Fuente: Elaboración propia

Para verificar las insignias o los certificados es necesario entrar a la sección de verificación de certificados escaneando el código QR que se

encuentran en las insignias y certificados o mediante el enlace https://www.cpsi.one/admin/tool/certificate/index.php. En esta página se coloca el Número de Insignia o Número de Certificado y verifica que exista el certificado o insignia y que esté vigente, además que se puede descargar la insignia o certificado.

Figura 15

Sección de verificación de certificados



Fuente: Elaboración propia

IV.5 Características y limitaciones de la página PCSI: Profesional Certificado en Seguridad de la Información

Actualmente ASOVESINFO ofrece una certificación llamada Profesional Certificado en Seguridad de la Información (PCSI), ofrecida a través de la página

web http://mendillo.info/PCSI/. En ella están los enlaces para poder contactar a los administradores y habilitar el examen al aspirante, al igual que enlaces al código de ética y a más información sobre la certificación. Además de un enlace a un examen demostrativo sobre cómo funciona el examen real y un enlace al examen real una vez que inicias sesión. También hay un enlace a la página principal de ASOVESINFO, así como a otras certificaciones internacionales importantes.

La página se limita a poseer sólo una certificación, lo que impide desarrollar otras certificaciones, así como realizar solamente un examen dentro de la certificación, sin posibilidad de colocar rápidamente nuevos exámenes u otras certificaciones. Al igual que, aunque la certificación pueda ser rastreable, no puede generar insignias.

El modelo de examen también permite ver cómo será el examen real, lo que da un indicio a que el examen será dentro del mismo navegador, y que se podría navegar y utilizar otras páginas web, así como cualquier otro material que permitiese al aspirante de la certificación hacer trampa y comunicarse con personas que pudiesen alterar el resultado del examen.

Por otro lado, vemos que la plataforma implementada mediante Moodle, permite utilizar múltiples herramientas como crear distintas certificaciones al mismo tiempo, así que, con una misma plataforma podrían manejarse todos los alumnos o aspirantes a la certificación y centralizar toda la información de las distintas certificaciones. Además que Moodle es una plataforma de distribución libre, lo que tendrá actualizaciones constantes y permitirá reforzar las versiones venideras, cosa que no se puede con la página web actual, ya que es el mismo desarrollador el que debe realizar las actualizaciones y mantener la página al día.

También permite utilizar el sistema de *proctoring* Safe Exam Browser, asegurando que quien esté realizando el examen no pueda cometer algún tipo de fraude mediante el mismo dispositivo, minimizando así el fraude dentro de la evaluación. Así como también permitiría el uso de distintos exámenes para una misma certificación, y la entrega de insignias y el certificado de forma automática.

Es por esto que, aunque sea muy parecida la forma de la evaluación, la certificación hecha en Moodle tiene ventajas notables sobre la certificación actual que utiliza ASOVESINFO, como el uso de insignias, la posibilidad de albergar varios exámenes y varias certificaciones dentro de la página y el uso de un sistema de proctoring.

IV.6 Ejecución de pruebas

IV.6.1 Ejecución de pruebas de funcionalidades básicas

Para verificar que la plataforma funcione correctamente se ejecutaron una serie de pruebas funcionales. Las funcionalidades puestas a prueba fueron el registro de usuarios nuevos así como el acceso de usuarios registrados, la creación de nuevos tópicos en la certificación, la creación de nuevos exámenes y administración de los bancos de preguntas.

Para el registro de usuario se probó crear un usuario sin agregar nada en los campos disponibles, y cuando esto sucedía, la aplicación se devolvía a la página de registro e indicaba los campos vacíos. También se configuró el reCAPTCHA de Google, lo que permitió proteger la página de ataques DDoS en la parte de registro de usuario, y al igual que los otros campos, si no se completa el reCAPTCHA, no se puede avanzar en la página.

Una vez que el usuario ya ha iniciado sesión, aparece en la página principal del sitio, donde puede hacer clic en la certificación, sin embargo, si el usuario no está matriculado, no podrá acceder a la certificación, por lo que es necesario que se matricule. Una vez matriculado por el administrador del sitio, el usuario ya puede entrar a la certificación.

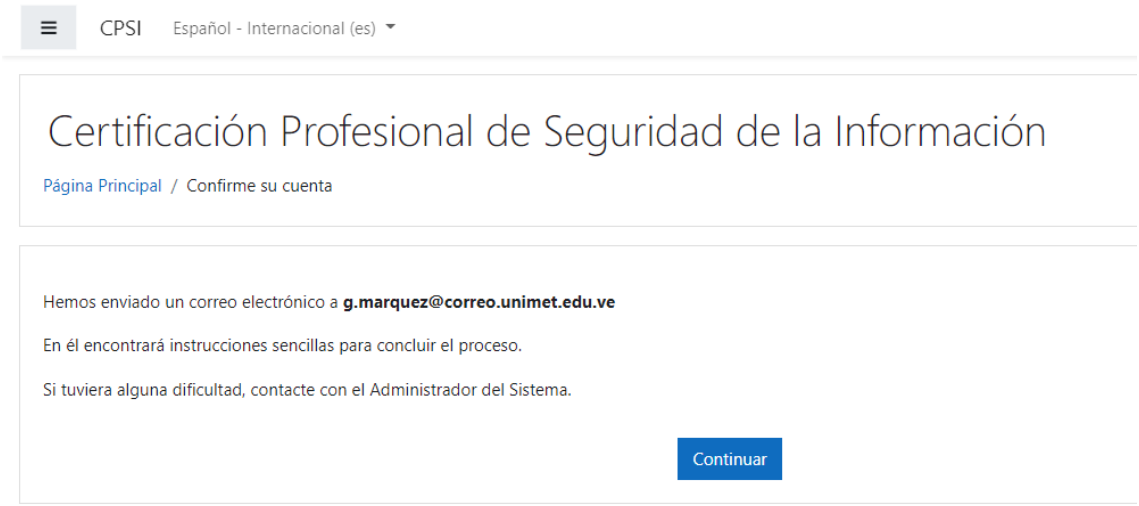
Al entrar en la certificación, el usuario puede ver diversas actividades que se encuentran bloqueadas por otras actividades que debe realizar primero, como por ejemplo, las insignias que no se emiten hasta que el usuario complete el examen correspondiente.

Por último, se realizaron pruebas como estudiante para confirmar que no podría editar la certificación así como los resultados, y al chequear estas

secciones como estudiantes, no se mostraba la opción para editar las configuraciones.

Figura 16

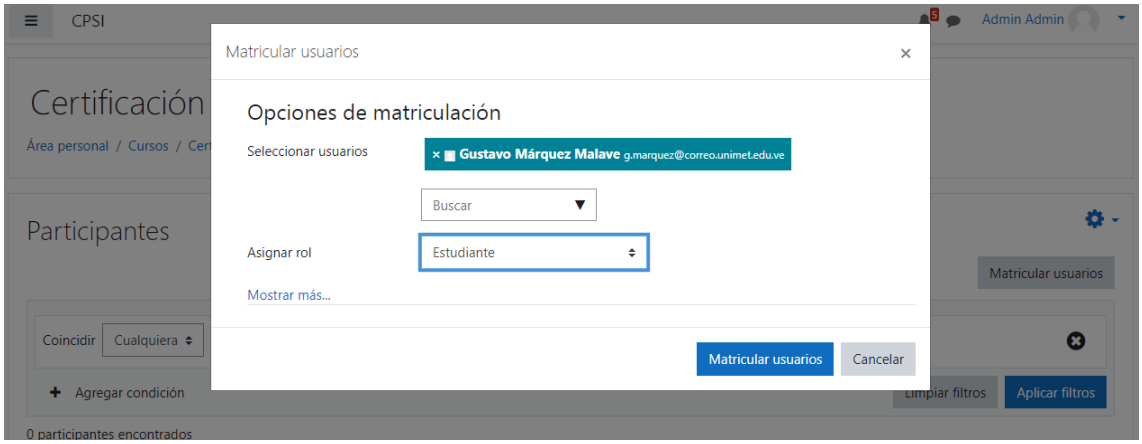
Registro exitoso de un nuevo usuario



Fuente: Elaboración propia

Figura 17

Nuevo usuario matriculado



Fuente: Elaboración propia

IV.6.2 Ejecución de pruebas en Safe Exam Browser

Para asegurarse de Safe Exam Browser realizaba su correcta labor de proctoring, se realizaron pruebas en ella, aplicando comandos como “Alt + Tab” y “Win + Tab” para intentar cambiar de aplicación o pestañas, así como “Ctrl + Alt + Del” para entrar a la pantalla de bloqueo o pantalla segura. Sin embargo, estos comandos no funcionaron como normalmente lo hacen. Los comandos

“Win + Tab” y “Ctrl + Alt + Del” no realizaron nada en el dispositivo y el comando “Alt + Tab” intentó el cambio de aplicación pero la única aplicación que aparecía era el mismo Safe Exam Browser.

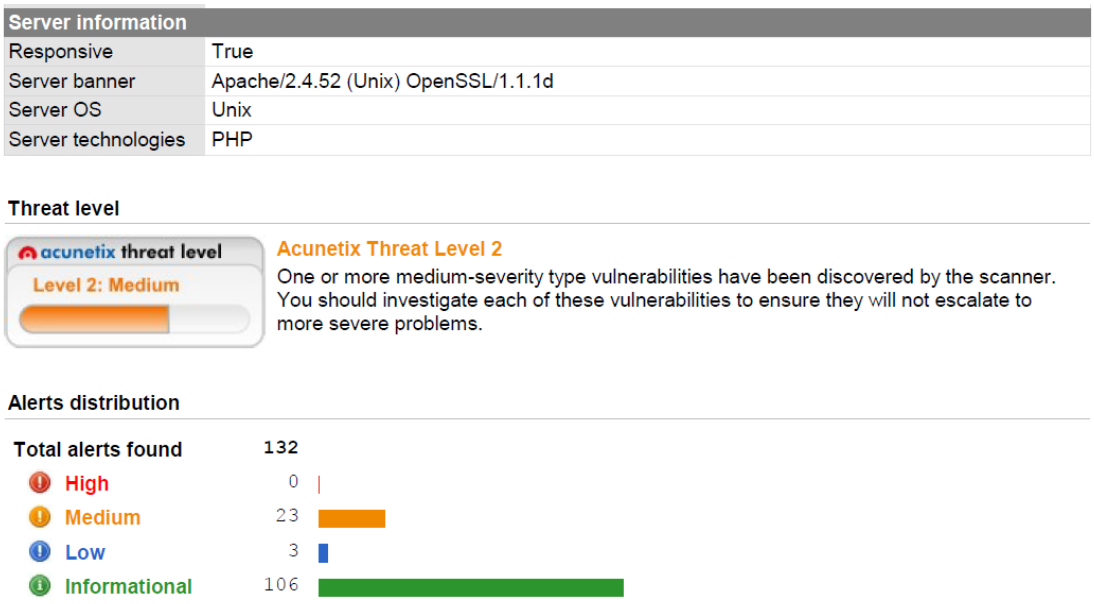
También se realizaron pruebas de capturas de pantalla y grabación de pantalla, y al hacerlas, no se pudo obtener ninguna información de la pantalla del Safe Exam Browser. Al presionar la tecla “Prt Scr”, e intentar pegar la información fuera del Safe Exam Browser, actúa como si nunca se hubiese ejecutado el comando. Por otro lado, al iniciar una grabación antes de ejecutar la aplicación, y luego ejecutarla, la grabación se mantiene en el escritorio y no pasa al Safe Exam Browser. Esto ocurre porque Safe Exam Browser crea una aplicación kiosco que limita el sistema a estar únicamente dentro de esta aplicación kiosco, y que todo lo demás se mantenga en segundo plano.

IV.6.3 Análisis de vulnerabilidades con Acunetix

Se ejecutó Acunetix sobre la página https://www.cpsi.one/ junto a las credenciales del administrador, para así encontrar las vulnerabilidades dentro de la página web, a lo que después de 8 minutos y 54 segundos, había encontrado 132 alertas, de las cuales 106 eran informativas por enlaces rotos, que al probarlos de forma manual, redirigen a una página de error o de vuelta a la página inicial.

Figura 18

Parte del resumen del informe realizado por Acunetix



Server information	
Responsive	True
Server banner	Apache/2.4.52 (Unix) OpenSSL/1.1.1d
Server OS	Unix
Server technologies	PHP

Threat level

acunetix threat level
Level 2: Medium

Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Alerts distribution

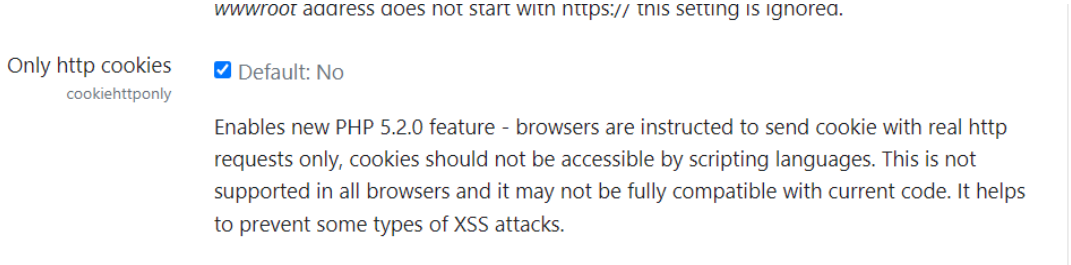
Total alerts found	132
High	0
Medium	23
Low	3
Informational	106

Fuente: Elaboración propia

También se encontraron 3 alertas de bajo impacto, donde 1 era por falta de la cabecera X-Frame-Options y las otras 2 porque las cookies no tenían la HttpOnly flag, lo que permitía que cualquier usuario pudiese sobreescribir las cookies. Esto último fue arreglado desde el apartado de seguridad, habilitando el HttpOnly en las cookies.

Figura 19

Apartado de seguridad de Moodle donde se activa la modificación de las cookies únicamente por HTTP



wwwroot address does not start with https:// this setting is ignored.

Only http cookies
cookiehttponly

Default: No

Enables new PHP 5.2.0 feature - browsers are instructed to send cookie with real http requests only, cookies should not be accessible by scripting languages. This is not supported in all browsers and it may not be fully compatible with current code. It helps to prevent some types of XSS attacks.

Fuente: Elaboración propia

Por último, se encontraron 23 vulnerabilidades de grado medio, las cuales todas ocurren porque el HTML no posee la protección contra ataques CSRF. Sin embargo, Moodle alega que esto lo resuelve la plataforma mediante una clave

de sesión, la cual no debe ser compartida. Moodle también propone utilizar el protocolo HTTP correctamente para que no ocurran este tipo de ataques.

CAPÍTULO V: Conclusiones y Recomendaciones

La información recopilada sobre distintos institutos de estudios superiores en el país y en exterior demuestra que, ya sea a nivel de pregrado o de postgrado, se imparte algún tipo de formación en seguridad de la información, no obstante, el nivel de formación ofrecido por lo general no es suficiente y hay que complementar con certificaciones profesionales para aspirar a obtener un puesto de trabajo en el área. De igual forma, existen institutos que ofrecen preparación más detallada que los convencionales, sin embargo, la facilidad de encontrar este tipo de instituciones en el país es significativamente menor que a nivel internacional.

Los resultados obtenidos de la encuesta permiten concluir que la mayoría de los reclutadores, personal de TI y de Seguridad de la Información, estarían interesados en una certificación profesional en Seguridad de la Información hecha y administrada en Venezuela.

Por su parte, fue exitosa la implementación de la plataforma y sus funcionalidades básicas, esto es registro, exámenes y expedición de certificados. Igualmente fueron satisfactorias las pruebas y la evaluación de su seguridad.

La realización de los exámenes mediante Safe Exam Browser permite que se tenga una mayor capa de seguridad y evita tanto que los aspirantes a la certificación puedan hacer trampas, como también la fuga de información de los exámenes, esto es sobre las preguntas y las respuestas.

Para la gestión futura de la plataforma se recomienda los siguiente:

- Al necesitar un administrador para matricular a los usuarios, corroborar que se firmen los códigos de ética y estar atento a los errores que puedan ocasionarse durante los exámenes (cortes eléctricos, cortes de Internet, etc).
- Efectuar períodos o ciclos de inscripción, donde se pueda promocionar la certificación, y que los aspirantes entreguen los recaudos, brindándoles así un lapso de tiempo donde todos estos aspirantes pueden realizar los exámenes y al finalizar el lapso, se anula su matriculación.

- Estos ciclos también serían necesarios para mantener registro de los cohortes de los aspirantes, así como modificar la fecha de expiración de las insignias y certificados el día de finalización del lapso de tiempo que duren los ciclos.
- Para la duración de los ciclos se considera prudente un tiempo de 3 meses, tomando un 1 mes de promoción e inscripción y los otros 2 meses como el lapso de tiempo que tienen los aspirantes para realizar los exámenes de la certificación.
- Otra recomendación es crear sub-tópicos dentro de los tópicos del banco de preguntas. Esto permitiría especificar las preguntas de acuerdo a los temas del tópico, y al momento de realizar el examen, se podría seleccionar las preguntas de acuerdo al tema y no sólo al tópico.
- También se recomienda realizar un refrescamiento del contenido de las preguntas cada 6 meses, evaluando las preguntas que están en el banco de preguntas, así como agregando nuevas preguntas para hacer los exámenes lo más variados posible.
- Se recomienda utilizar la misma página para implementar otros certificados. Al tener la facilidad de Moodle de poseer varios cursos o certificaciones, esto permite al administrador de la página generar varias certificaciones dentro de la misma plataforma y mantenerla al día sin necesidad de administrar distintas páginas web.
- Finalmente se recomienda realizar la migración de los servidores para traspasar el control total de la plataforma, y con ella la certificación, a ASOVESINFO.

Bibliografía Consultada

(n.d.). Official Chamilo statistics page. Retrieved January 15, 2022, from https://version.chamilo.org/stats/

(n.d.). eFront LMS: A fully adaptable LMS solution for modern enterprise training. Retrieved January 15, 2022, from https://www.efrontlearning.com/

(n.d.). InteliCorp Seguridad - Inicio | InteliCorp Seguridad. Retrieved January 19, 2022, from https://intelicorps.com/index.html

(n.d.). ASOVESINFO. Retrieved January 19, 2022, from https://asovesinfo.org/

(n.d.). REDES Se denomina red de transmisión de datos al conjunto formado por los equipos y los medios físicos y lógicos que permiten. Retrieved February 19, 2022, from http://www.edificacion.upm.es/informatica/documentos/redes.pdf

(2021, July 14). MoodleDocs. Retrieved January 15, 2022, from https://docs.moodle.org/311/en/Main_page

Bock, L. (2021). *Modern Cryptography for Cybersecurity Professionals: Learn how You Can Leverage Encryption to Better Secure Your Organization's Data*. Packt Publishing.

2019 Cybersecurity Workforce Study. (n.d.). ISC2. Retrieved January 24, 2022, from https://www.isc2.org/Research/2019-Cybersecurity-Workforce-Study

Web Security Series Web Security Associate v2.0. (n.d.). CIW. Retrieved January 24, 2022, from

https://www.ciwcertified.com/resources/documents/course-descriptions/CCN02CAWSAACU2001.pdf

Brousell, L. (2014, 11 21). *How CSOs Can Help CIOs Talk Security to the Board*. CIO from IDG. Retrieved January 12, 2022, from https://web.archive.org/web/20170701002830/https://www.cio.com/article/2850855/security0/how-csos-can-help-cios-talk-security-to-the-board.html

Cárdenas, F. A. (n.d.). *¿Qué es la gestión de activos de información?* NovaSec MS. Retrieved January 11, 2022, from https://www.novasec.co/blog/67-gestion-de-activos-de-informacion

Cauas, D. (n.d.). *Definición de las variables, enfoque y tipo de investigación*. Retrieved 10 2, 2021, from https://docplayer.es/13058388-Definicion-de-las-variables-enfoque-y-tipo-de-investigacion.html

Cisco. (n.d.). *¿Qué es la seguridad de red?* https://www.cisco.com/c/es_mx/products/security/what-is-network-security.html

CISSP domain 7: Security operations- What you need to know for the exam - Infosec Resources. (n.d.). Infosec Resources. Retrieved January 11, 2022, from https://resources.infosecinstitute.com/certification/security-operations/

CISSP domain 8 overview: Software development security. (2017, July 6). Infosec Resources. Retrieved January 11, 2022, from https://resources.infosecinstitute.com/certification/cissp-domain-8-overview-software-development-security/

Clinton, D. (2020). *Linux Security Fundamentals*. Wiley.

Cobb, M. (2019, September 18). *Qué se necesita para ser un ingeniero DevSecOps*. Computer Weekly. Retrieved January 24, 2022, from https://www.computerweekly.com/es/consejo/Que-se-necesita-para-ser-un-ingeniero-DevSecOps

Comisión Europea. (2016, 04 27). *Comisión Europea*. ¿Qué es un responsable o encargado del tratamiento? Retrieved January 24, 2022, from https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_es

CSO España. (2020, January 14). *¿Cuál es el rol de un 'threat hunter'?* CSO España. Retrieved February 3, 2022, from https://cso.computerworld.es/tendencias/cual-es-el-rol-de-un-threat-hunter

Curso de Redes Cisco en Barcelona y Madrid - Cursos Cisco. (n.d.). PUE. Retrieved January 24, 2022, from https://www.pue.es/cursos/cisco/cisco-ccna-security-seguridad-redes-cisco

Datasec. (n.d.). *¿Qué nos indica el número de profesionales certificados en seguridad informática en el país?* Retrieved septiembre 14, 2021, from https://www.datasec-soft.com/es/blog/cantidad-de-profesionales-certificados-cissp#:~:text=Al%201%C2%B0%20de%20enero,siendo%20el%201.03%25%20del%20total.

Diferencia entre Ciberseguridad, Seguridad Informática y Seguridad de la Información. (2021, March 3). LISA Institute. Retrieved January 7,

2022, from https://www.lisainstitute.com/blogs/blog/diferencia-ciberseguridad-seguridad-informatica-seguridad-informacion

Difference between Skill Badges and Certifications - Cloud Certification Help. (n.d.). Google Support. Retrieved January 15, 2022, from https://support.google.com/cloud-certification/answer/9981085?hl=en

Esquema del examen de Certificación. (n.d.). ISC2. Retrieved January 11, 2022, from https://www.isc2.org/-/media/ISC2/Certifications/Exam-Outlines/CISSPSpanish.ashx

European Data Protection Supervisor. (2018, 05 25). *Data Protection Officer (DPO)* | *European Data Protection Supervisor*. European Data Protection Supervisor. Retrieved January 24, 2022, from https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en

Evaluación de la Seguridad - Seguridad de la información. (n.d.). B-SECURE. Retrieved January 11, 2022, from https://www.b-secure.co/soc/analisis-vulnerabilidades-pentest

Fernández Collado, C., Baptista Lucio, P., & Hernández Sampieri, R. (2014). *Metodología de la investigación* (P. Baptista Lucio, Ed.). McGraw-Hill Education.

Gonález González, C., Infante Moro, A., & Infante Moro, J. (2020, 04 24). *Implementation of E-Proctoring in Online Teaching: A Study about Motivational Factors*. MDPI Open Access Journals. https://www.mdpi.com/2071-1050/12/8/3488

González, Y. (2020, 06 17). *Proctoring o cómo supervisar exámenes online*. Grupo Atico 34. https://protecciondatos-lopd.com/empresas/proctoring/

Hooper, V., & McKissack, J. (2016). The emerging role of the CISO. *Business Horizons*, *59*(6), 585-591. Retrieved enero 11, 2021, from https://sci-hub.st/10.1016/j.bushor.2016.07.004

IBM. (n.d.). *¿Qué es la cacería de amenazas?* IBM. Retrieved February 3, 2022, from https://www.ibm.com/es-es/topics/threat-hunting

IT Digital Security. (2018, August 24). *CISO y CSO: ¿tienes clara la diferencia de roles?* IT Digital Security. Retrieved January 24, 2022, from https://www.itdigitalsecurity.es/actualidad/2018/08/ciso-y-cso-tienes-clara-la-diferencia-de-roles

López, O., Amaya, H., & León, R. (2001). *INFORMÁTICA FORENSE : GENERALIDADES, ASPECTOS TÉCNICOS Y HERRAMIENTAS*. https://scholar.google.com/scholar?hl=es&as_sdt=0%2C5&q=Inform%C3%A1tica+Forense&btnG=

Martínez, A. (2021, 06 10). *CISO, una figura imprescindible en las grandes empresas y también en pymes*. Revistas de elEconomista. Retrieved 01 12, 2022, from https://revistas.eleconomista.es/franquicias/2021/junio/ciso-una-figura-imprescindible-en-las-grandes-empresas-y-tambien-en-pymes-BG7976461

McLaughlin, L. (2020, 02 7). *CIO role 2020: Everything you need to know about today's Chief Information Officers*. The Enterprisers Project. Retrieved January 12, 2022, from

https://enterprisersproject.com/article/2019/9/cio-chief-information-officer-role-explained#q1

Mieres, J. (2009). *Ataques informáticos Debilidades de seguridad comúnmente explotadas*. https://www.evilfingers.net/publications/white_AR/01_Ataques_informaticos.pdf

Objetos de aprendizaje integrados a un sistema de gestión de aprendizaje. (n.d.). Redalyc. Retrieved January 14, 2022, from https://www.redalyc.org/pdf/688/68800310.pdf

Orellana, F. (2020, December 4). *Educación en línea: Características e Importancia*. UNIR Ecuador. Retrieved January 14, 2022, from https://ecuador.unir.net/actualidad-unir/educacion-en-linea-caracteristicas/

Otero Ortega, A. (n.d.). *ENFOQUES DE INVESTIGACIÓN*. Research Gate. https://www.researchgate.net/profile/Alfredo-Otero-Ortega/publication/326905435_ENFOQUES_DE_INVESTIGACION/links/5b6b7f9992851ca650526dfd/ENFOQUES-DE-INVESTIGACION.pdf

Pérez, A. (2019, 05 21). *¿Qué es CTO? Explicación y funciones*. OBS Business School. Retrieved 01 12, 2022, from https://www.obsbusiness.school/blog/que-es-cto-explicacion-y-funciones

Proctoring: reto para la enseñanza del siglo XXI. (n.d.). RIULL Principal. Retrieved February 17, 2022, from https://193.145.118.245/xmlui/bitstream/handle/915/8087/Proctoring%20reto%20para%20la%20ense%c3%b1anza%20del%20siglo%20XXI%20JICV18_paper_29.pdf?sequence=1&isAllowed=y

PwC Chile. (2018, Octubre). *Supervisión de riesgos introducidos por terceros*. PwC. Retrieved February 2, 2022, from https://www.pwc.com/cl/es/publicaciones/assets/2018/Supervision-de-riesgos-introducidos-por-terceros.pdf

¿Qué es la arquitectura de seguridad de la información y por qué es relevante para las PYMES? (2021, May 18). DocuSign. Retrieved January 11, 2022, from https://www.docusign.mx/blog/arquitectura-de-seguridad

¿Qué es la Gestión de Identidades y Accesos (IAM)? (2018, March 15). Blog SYNNEX Westcon-Comstor. Retrieved January 11, 2022, from http://digital.la.synnex.com/que-es-la-gestion-de-identidades-y-accesos-iam

¿Qué es la Seguridad Ofensiva? (2020, September 7). Campus Internacional de Ciberseguridad. Retrieved January 12, 2022, from https://www.campusciberseguridad.com/blog/item/144-que-es-la-seguirdad-ofensiva

¿Qué es un curso MOOC? - Universitat Autònoma de Barcelona. (n.d.). UAB. Retrieved January 15, 2022, from https://www.uab.cat/web/estudiar/mooc/-que-es-un-curso-mooc-1345668281247.html

Ruiz Bueno, C. (2006). La certificación profesional: algunas reflexiones y cuestiones a debate (Universidad Autónoma de Barcelona, Ed.). *LÍNEAS DE INVESTIGACIÓN EN LA FORMACIÓN PARA EL TRABAJO*, *38*, 133 - 150. http://www.raco.cat/index.php/Educar/article/download/72352/82606

Sánchez Dávila, A. (2019, 08 28). *Kaspersky registra 45 ataques por segundo en América Latina*. Kapersky. Retrieved septiembre 27, 2021, from https://latam.kaspersky.com/blog/kaspersky-registra-45-ataques-por-segundo-en-america-latina/15274/

Santos, O. (2018). *Developing Cybersecurity Programs and Policies*. Pearson Education.

Seidl, D., & Chapple, M. (2018). *(ISC)2 CISSP Certified Information Systems Security Professional Official Practice Tests*. Wiley.

Stranieri, S. (2021, 05 22). *Ciberataques 2020: pérdidas económicas y de confianza*. ámbito. Retrieved septiembre 27, 2021, from https://www.ambito.com/negocios/ciberataques/2020-perdidas-economicas-y-confianza-n5194573

Strategies for Building and Growing Strong Cybersecurity Teams. (n.d.). ISC2. Retrieved February 19, 2022, from https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482

Sullivan, P. (2016, November 22). *Gestión de riesgos de seguridad de la información: Comprensión de los componentes*. Computer Weekly. Retrieved January 10, 2022, from https://www.computerweekly.com/es/consejo/Gestion-de-riesgos-de-seguridad-de-la-informacion-Comprension-de-los-componentes

Tiwari, A. (2018, 07 23). *Information Security Team Roles & Responsibilities – Primary & Major*. SysTools. Retrieved 01 12, 2022,

from https://www.systoolsgroup.com/updates/information-security-team-roles-responsibilities/