Seguridad de aplicaciones web

Servicio Nacional de Aprendizaje - SENA

Nivel de formación: **Técnico**

01 Presentación

Estudia **Seguridad de aplicaciones web**, y como **egresado SENA diagnosticarás** el estado de la **seguridad de los servicios** y **aplicaciones web** aplicando **estándares y metodologías** nacionales e internacionales que permitan monitorear y controlar amenazas, de esta forma podrás **desempeñarte** en diferentes sectores económicos para **generar seguridad** y control sobre ataques **cibernéticos** de alto perfil.

Este **técnico** tendrá una duración de **15 meses** y se impartirá en **modalidad 100% virtual.** Para **inscribirte**, debes contar con un **computador** o *tablet* con acceso a internet.

¡Súmate a esta propuesta de formación y haz parte de los miles de **colombianos** que le **apuestan al cambio!**

Inscríbete en www.senasofiaplus.edu.co

Código
228133

Horas
2304

Duración
15 Meses

Modalidad
Virtual

02 Justificación del programa

Desde una perspectiva internacional, la macrotendencia que hoy transforma el mundo es la cuarta revolución industrial, de cara se muestran grandes retos y oportunidades para las industrias y organizaciones de diferentes sectores productivos. Por lo tanto, se están viviendo grandes cambios debido a la incursión de nuevas tecnologías que permiten desde, mejorar la toma de decisiones de una organización, hasta potencializar las interacciones de las máquinas con nosotros mismos. (Perasso, 2016).

Esta dinámica es producto de la incorporación de ciencias y disciplinas como lo son la Inteligencia artificial, el aprendizaje automático, la ciberfísica, la analítica de datos, el internet de las cosas, entre otras, que consecuentemente generan un aumento en el desarrollo de *hardware* como de *software* y servicios. De este modo se pude inferir, que naturalmente hay un aumento en los datos y en el intercambio de la información, un consumo alto de servicios y un desmesurado uso de aplicaciones, indicando que es necesario generar seguridad y control sobre estos procesos. Al respecto, esta observación se corrobora con el artículo de Esset: Tendencias en ciberseguridad 2022: entre la evolución de las amenazas y los desafíos del trabajo híbrido, el cual señala: "A medida que la infraestructura crece y abarca no solo equipos propios sino también servicios en la nube, redes VPN y cada vez más aplicaciones para comunicarse y acceder a la información, crece la cantidad de posibles fallos de seguridad". (Pastorino, 2021).

Este fenómeno se vio con mayor fuerza durante la pandemia del COVID-19, según el primer reporte de perspectivas de ciberseguridad del foro económico mundial "*Global Cybersecurity Outlook* 2022" señala que el cambio acelerado al trabajo remoto durante la pandemia de COVID-19, junto con los recientes ataques cibernéticos de alto perfil, han dado como resultado que la seguridad cibernética sea una prioridad entre los tomadores de decisiones clave en organizaciones y naciones. Esta afirmación solo corrobora la necesidad de talentos alrededor de la disciplina de la seguridad web, por lo que un hecho asociado es lo que indica el informe *Global Information Security Workforce Study* 2021, elaborado por ISC, afirmando que el año pasado faltaban 2,72 millones de profesionales de ciberseguridad en todo el mundo, en ese sentido aquí se vislumbra una gran oportunidad con respecto a la presente propuesta formativa.

Pasando a una perspectiva nacional, se encuentra el documento CONPES1 3995 de 2020 que formula una Política Nacional de Confianza y Seguridad Digital, en la que resalta de manera literal la importancia de: la alta dependencia de la infraestructura digital y el aumento en el uso y adopción de nuevas Tecnologías de la Información y las Comunicaciones (TIC) traen consigo una serie de riesgos e incertidumbres relacionados con la seguridad digital, lo cual exige que el país cuente con suficientes capacidades para su gestión adecuada y oportuna. Las amenazas, los ataques e incidentes de seguridad digital cada día son más sofisticados y complejos e implican graves consecuencias de tipo económico o social.

De este modo, esta afirmación corrobora el valor que da el Gobierno Nacional a la aplicación de mecanismos de ciberseguridad y al personal idóneo que pueda atender este panorama retador, que impacta de manera positiva en el crecimiento socio económico de la nación.

Considerando los hechos y oportunidades que tiene un perfil con estas competencias, es necesario dentro del estado del arte hacer una revisión sucinta sobre el estado de ocupación en el área, en ese sentido la exploración conduce a datos y cifras emitidos por el marco nacional de cualificaciones MNC, en el cual se presentan un informe que es el resultado del estudio de identificación y medición de brechas de capital humano del sector TIC, lo que señala el documento es lo siguiente:

1. El sector requiere una serie de perfiles, que entre los más destacados son desarrolladores, analistas y *Tester* que por lo regular apuntan a aplicaciones Web.

2. Las tendencias identificadas como las más relevantes y asociadas a la naturaleza disciplinar de la propuesta son: *blockchain*, *Cloud*, privacidad y ética.

3. Como competencia técnica más solicitada a nivel nacional son los analistas de sistemas de información, el cual sería un rol importante que el técnico puede desempeñar.

De manera adicional, de acuerdo con el informe del Observatorio Laboral y Ocupacional del SENA, correspondiente al primer semestre de 2021 indica que las vacantes para el nivel de cualificación de técnicos y tecnólogos son 51.603, se han inscrito 70.822 y han ingresado o colocado 25.833, por lo que la tasa de colocación es del 50%. Además, señalan el top 10 de las ocupaciones más demandadas por las empresas, en la cual son los técnicos en tecnologías de la información y afines que ocupan ese selecto grupo. De esta forma, se percibe la pertinencia e importancia de la creación de la presente propuesta formativa.

De otro lado, según vigilancia tecnológica a la oferta académica sobre seguridad web, a las necesidades y tendencias del sector, se encuentra que desde la sola idea de la concepción de la propuesta se precisan algunos rasgos distintivos más destacados en aspectos de formación, como son:

1. Se cuenta con formación socio humanística. Al respecto, se pretende una formación integral para el aprendiz en el cual permita entender su entorno y transformarlo de una manera positiva. Estas competencias abarcan alrededor de un 42% de la malla curricular.

2. Se cuenta con la participación de la industria a través de grupos focales que evalúan y analizan la pertinencia de la propuesta de formación. Esto con el fin de enriquecer y mejorar aspectos que desde la academia se desconocen.

3. El énfasis del Técnico está orientado al análisis de vulnerabilidades y riesgos de las aplicaciones web, este hecho dista de otras propuestas formativas que están más alineadas al diagnóstico de vulnerabilidades de toda una organización utilizando el marco de referencia de la ISO 27001, mientras que el técnico adopta una metodología llamada OWSP que es la idónea para este campo disciplinar.

En este orden de ideas, con el Técnico, el SENA es referente en una apuesta que busca aportar a la sociedad técnicos y tecnólogos de calidad, que responden a las demandas del sector que exige una trasformación digital en el país y en el mundo; objetivo al cual apunta el perfil del egresado del programa de Seguridad de aplicaciones Web.

03 Competencias a desarrollar

220501108 - Diagnosticar la seguridad de la información de acuerdo con métodos de análisis y normativa técnica.

220501099 - Probar la solución del *software* de acuerdo con parámetros técnicos y modelos de referencia.

220501111 - Controlar sistema de seguridad de la información de acuerdo con los procedimientos y normativa técnica.

240201528 - Razonar cuantitativamente frente a situaciones susceptibles de ser abordadas de manera matemática en contextos laborales, sociales y personales.

240201524 - Desarrollar procesos de comunicación eficaces y efectivos, teniendo en cuenta situaciones de orden social, personal y productivo.

240202501 - Interactuar en lengua inglesa de forma oral y escrita dentro de contextos sociales y laborales según los criterios establecidos por el Marco Común Europeo de Referencia para las Lenguas.

220501046 - Utilizar herramientas informáticas de acuerdo con las necesidades de manejo de información.

240201530 - Resultado de aprendizaje de la inducción.

230101507 - Generar hábitos saludables de vida mediante la aplicación de programas de actividad física en los contextos productivos y sociales.

240201526 - Enrique Low Murtra. Interactuar en el contexto productivo y social de acuerdo con principios éticos para la construcción de una cultura de paz.

220601501 - Aplicar prácticas de protección ambiental, seguridad y salud en el trabajo de acuerdo con las políticas organizacionales y la normatividad vigente.

240201533 - Fomentar cultura emprendedora según habilidades y competencias personales.

210201501- Ejercer derechos fundamentales del trabajo en el marco de la Constitución Política y los convenios internacionales.

04 Perfil de ingreso

Nivel académico: básica secundaria.

Grado: 9

Edad mínima definida en la ley: 14 años.

05 Perfil de egreso

El egresado del programa técnico en seguridad de aplicaciones web es un talento humano con la capacidad de diagnosticar el estado actual de la seguridad de los servicios y aplicaciones web para el sector empresarial, con conocimientos y habilidades para evaluar los controles que garantizan la seguridad digital, aplicando estándares y metodologías nacionales e internacionales que permitan monitorear y controlar amenazas. El técnico con actitud crítica y ética tendrá la capacidad de realizar evaluaciones objetivas dentro del marco de la legislación aplicable articulado con el plan de pruebas de seguridad. Cabe resaltar que las funciones de este nivel demandan responsabilidad de supervisión, un apreciable grado de autonomía y juicio evaluativo. Además, podrá demostrar la apropiación de la cultura del autoaprendizaje, actualización permanente, trabajo colaborativo, valores y principios éticos, que le permitirán abordar las nuevas tendencias, innovar en su proceso personal y laboral apoyando procesos de transformación organizacional, así como emprender en líneas de negocio relacionadas.

06 Estrategia metodológica

La estrategia metodológica del programa, está centrada en la construcción de autonomía para garantizar la calidad de la formación en el marco de la formación por competencias, el aprendizaje por proyectos y el uso de técnicas didácticas activas que estimulan el pensamiento para la resolución de problemas simulados y reales; soportadas en la utilización de las tecnologías de la información y la comunicación, integradas, en ambientes virtuales de aprendizaje, que en todo caso recrean el contexto productivo y vinculan al aprendiz con la realidad cotidiana y el desarrollo de las competencias.

Igualmente, debe estimular de manera permanente la autocrítica y la reflexión del aprendiz sobre el que hacer y los resultados de aprendizaje que logra a través de la vinculación activa de las cuatro fuentes de información para la construcción de conocimiento:

- El instructor - Tutor.
- El entorno.
- Las TIC.
- El trabajo colaborativo.