



Nivel de formación: **Técnico**

Seguridad de aplicaciones web

01 Presentación

Bienvenidos a este espacio formativo en el que obtendrán las competencias y habilidades requeridas para desempeñarse como técnico en seguridad de aplicaciones web.

En el sector empresarial, cada día crece la necesidad de competir utilizando la internet, y esto permite que se pueda aprovechar todos los servicios, llevando a las organizaciones a invertir en la construcción de aplicaciones .

Lo que lleva, a que se conozcan los productos o servicios que se ofrecen a sus clientes, realizando transacciones desde cualquier lugar y dispositivo. Este fenómeno es llamado la internet 2.0. Lo que permite que se abran brechas de seguridad dejando vulnerable la información que cada una posee y colocando en riesgo toda la organización.

Por esta razón, crece la demanda en todo el mundo de profesionales que se dediquen a velar y salvaguardar la información de los ciberataques.

El Servicio Nacional de Aprendizaje pretende ser un referente, aportando a la sociedad técnicos de calidad desde las competencias y personales, respondiendo a las demandas del sector que exige una transformación digital en el país y en el mundo.

En si, este programa, permitirá:

Identificar, monitorear, diagnosticar y probar las vulnerabilidades y ataques a las aplicaciones que se utilizan en las organizaciones, utilizando el Top Ten de OWASP.



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 *hardware* como de *software* y servicios. De este modo se puede 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 ciberneticos de alto perfil, han dado como resultado que la seguridad cibernetica 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 que se quiere lanzar.

El énfasis de este programa 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.

En este orden de ideas, el Servicio Nacional de aprendizaje SENA pretende ser un referente con este tipo de apuestas novedosas, que busca aportar a la sociedad técnicos y tecnólogos de calidad y que respondan a las demandas del sector que exige una transformación 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.** 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.
- **220201501.** Aplicación de conocimientos de las ciencias naturales de acuerdo con situaciones del contexto productivo y social.

04 Perfil de ingreso

- **Nivel académico adecuado para caracterizar al aspirante de acuerdo con el perfil de egreso:**
Educación básica y/o media
- **Grado:** 9
- **Requiere certificación académica:** Si
- **Requiere Formación para el trabajo y desarrollo humano:** Si

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**