



PROTECTED

## Implementación de auditoría técnica en seguridad de la información

Nivel de formación: Complementario

## 01 Presentación

Estimado aprendiz, bienvenido al programa de formación Implementación de auditoría técnica en seguridad de la información, donde podrá fortalecer los conocimientos, destrezas y habilidades que le permitirán desempeñarse y destacarse en el mundo laboral.

El egresado del programa será competente para realizar el estudio, definición, conceptualización y aplicación de las políticas del Sistema de Gestión de Seguridad de la Información - SGSI - en sectores empresariales y áreas como el comercio, las finanzas o las inversiones.

Tendrá la capacidad para desarrollar actividades como: recolectar información sobre las posibles vulnerabilidades e implementar planes de auditoría, técnicas de control y monitoreo ante posibles ataques cibernéticos.

El programa está adaptado para satisfacer las necesidades empresariales del sector productivo del país, articulado con la industria 4.0, y considera los retos que implican la Cuarta Revolución Industrial, estimada como la nueva era de las tecnologías.

Al finalizar su formación, será competente para auditar e implementar políticas de SGSI en cualquier empresa de industria TIC, financiera, agrícola, minera y, en definitiva, en cualquiera que decida avanzar hacia el auge tecnológico a que están abocados los sectores económicos, permitiendo, con su aporte, contribuir al crecimiento tecnológico y desarrollo del país.

**¡Bienvenidos a un nuevo aprendizaje!**



Código  
21720182



Horas  
96



Duración  
2 meses



Modalidad  
Virtual

## 02 Justificación del programa

La evolución de los modelos de negocio, la transformación digital y el contexto de amenazas está influyendo sobre las organizaciones para que pongan mayor atención a la gestión de la seguridad de la información y a la designación de los recursos necesarios para tal fin. Adicionalmente, la ciberseguridad se ha convertido en una de las principales prioridades y preocupaciones de las empresas. Muchas tecnologías que hace unos años nos parecían lejanas se han asentado como parte de nuestro día a día, y con ellas, la necesidad de garantizar nuestra seguridad y privacidad, tanto en la esfera privada como en la empresarial. El camino para convertirse en una organización adaptada a los riesgos tecnológicos y actuales debe iniciarse a partir de la toma de conciencia de los niveles ejecutivos de la organización sobre las amenazas propias del nuevo ambiente digital de negocios.

El proceso de auditoría de los sistemas de información es una de las herramientas que se han creado para tal fin y abarca las normas, principios, métodos, directrices, prácticas y técnicas que utiliza un auditor de sistemas de información para planificar, ejecutar, evaluar y revisar los sistemas comerciales o de información y los sistemas de procesos. Las políticas y estrategias de seguridad empresariales no son una inversión de un día, sino que se trata de un trabajo periódico, que necesita de actualización y mejora continua; para ello y para desempeñar estas tareas, es importante contar con un equipo de expertos que trabajen día a día en la seguridad de la información, garantizando el mantenimiento de la confidencialidad, disponibilidad e integridad de los datos de las organizaciones y de sus clientes. Si antes de la pandemia las empresas estaban obligadas a revisar sus estrategias de seguridad informática, la era post-COVID tendrá que acelerar este proceso por el bien de las compañías y lo que más valor tiene para ellas: su información.

Colombia expidió en 2011 el documento CONPES 3701, con los Lineamientos de Política para Ciberseguridad y Ciberdefensa, que concentró los esfuerzos del país en la creación y aplicación de unos lineamientos orientados a desarrollar una estrategia nacional en materia de ciberseguridad y ciberdefensa, con el fin de enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético, creando la institucionalidad y promoviendo el ambiente y condiciones para brindar protección en el ciberespacio. Asimismo, menciona "Solicitar al Ministerio de Tecnologías de la Información y las Comunicaciones realizar las gestiones necesarias con el Ministerio de Educación Nacional y el SENA para la generación de un plan de capacitación para el sector privado en temas de ciberseguridad y de seguridad de la información".

Igualmente, el Gobierno Nacional, a través del documento CONPES 3854 de 2016, estableció la política nacional de seguridad digital de Colombia, la cual pretende que las múltiples partes interesadas hagan un uso responsable del entorno digital y fortalezcan sus capacidades para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en el desarrollo de sus actividades socioeconómicas en el entorno digital.

A través del documento CONPES 3995 y su Política Nacional de Confianza y Seguridad Digital, el Gobierno establece medidas para ampliar la confianza digital y mejorar la seguridad digital para hacer de Colombia una sociedad incluyente y competitiva en el futuro digital, y recomienda: "Solicitar al Servicio Nacional de Aprendizaje (SENA) diseñar programas de formación profesional con el enfoque de la formación para el trabajo y desarrollo humano, los cuales atenderán las necesidades sectoriales para fortalecer las competencias en áreas como la seguridad digital, seguridad de la información, ciberseguridad e infraestructuras críticas".

El SENA, conocedor de estas necesidades, ofrece el programa complementario "Implementación de Auditoría Técnica en Seguridad de la Información", como parte de la línea formativa en Gobierno, Riesgo y Cumplimiento, con el fin de brindar a la población interesada y a las organizaciones herramientas que conlleven la mitigación del riesgo, incorporando tecnologías que anticipen el accionar de la cibercriminalidad y así cumplir con las políticas y directrices gubernamentales, coadyuvando al mejoramiento de la seguridad digital del país.

### **03 Competencias a desarrollar**

**220501110 - Implementar el sistema de seguridad de la información según modelo y estándares técnicos.**

## 04 Perfil de ingreso

- Bachilleres, técnicos, tecnólogos o profesionales de cualquier Núcleo Básico de Conocimiento.
- Tener conocimientos mínimos de herramientas ofimáticas e inglés.
- Cumplir con el trámite de selección definido por el centro de formación.
- Certificación del curso en Caracterización de Componentes en Ciberseguridad.

## 05 Perfil de egreso

No aplica.

## 06 Estrategia metodológica

Centrada en la construcción de autonomía para garantizar la calidad de los procesos formativos 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; soportada en la utilización de las tecnologías de la información y la comunicación, integradas en ambientes abiertos y pluritecnológicos, 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 autocritica y la reflexión del aprendiz sobre el quehacer 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.**