

The background of the slide features a person wearing a hooded sweatshirt, sitting at a desk and working on a laptop. A large, semi-transparent digital interface is overlaid on the scene, displaying various data visualizations such as a globe, charts, and code snippets. This theme is consistent with the title of the presentation.

# Hacking ético en sistemas y redes

## 01 Presentación

Bienvenido al programa de formación **Hacking ético en sistemas y redes**, el cual busca poder comprender la seguridad informática y la ciberseguridad en los entornos emergentes de virtualización de información, apropiando conceptos y herramientas en los procesos inherentes a los sistemas y redes de información. El poder conocer las amenazas y vulnerabilidades a las cuales se está expuesto en los entornos virtuales y digitales ayudará a desarrollar competencias y habilidades tecnológicas para poder solucionar problemas de seguridad electrónica, los cuales son más comunes de lo que se imagina en la nueva era digital que enfrenta el mundo. Este programa le ayudará a conocer herramientas especializadas aplicadas para la seguridad informática, con visión ética y legal del uso de información, que construyen una estructura en la que viven los usuarios digitales, utilizando diferentes herramientas de *hacking* ético e ingeniería social, y de igual manera, formar parte de la transformación de innovación y cultural de Colombia.

Este curso está compuesto por una competencia y cuatro resultados de aprendizaje, a desarrollarse en 96 horas de formación, con trabajo colaborativo y autónomo, que se abordarán con cinco componentes formativos que permitan identificar herramientas digitales de seguridad informática y ciberseguridad orientadas al *Hacking* ético.



Código  
21720183



horas  
96



Duración  
2 meses



Modalidad  
Virtual

## 02 Justificación del programa

El software y el hardware son indicadores del crecimiento T.I en el mundo y, con este crecimiento, la ciberdelincuencia también lo hace exponencialmente, siguiendo sus pasos. Las malas prácticas, configuraciones incorrectas y uso inadecuado de las tecnologías son procesos que se ejecutan día a día, enmarcados por los ataques informáticos. Comprender el ecosistema de los ciberdelincuentes contribuye a mitigar los ataques de gran y pequeña escala, logrando minimizar la afectación a las organizaciones.

Los sistemas de gestión y planes de continuidad del negocio son de vital importancia; sin embargo, los aspectos técnicos son la base sostenible de la ciberseguridad y la seguridad informática. Los ataques informáticos lamentablemente pueden ser llevados a cabo por personas sin gran experiencia, las cuales, por medio de herramientas básicas, pueden conseguir objetivos de fácil acceso. Es importante resaltar que tener conocimiento del modus operandi ciberdelincuencial, articulado con conocimientos técnicos, marca la diferencia en cargos relacionados con la ciberseguridad y la seguridad informática, ya que de esta manera se puede evidenciar un ataque difícil de ser detectado.

Por lo anterior, la inversión en capacitación de personal es indiscutiblemente el pilar fundamental de toda implementación de seguridad, teniendo en cuenta que adquirir sistemas de seguridad con altas capacidades y características lleva a las organizaciones a entrar en un estado de falsa seguridad, dando un segundo lugar a las capacidades humanas.

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. Así mismo, 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 "*Hacking ético en sistemas y redes*" como parte de la línea formativa en *Hacking ético*, 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**

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

## 04 Perfil de ingreso

- Bachilleres, técnicos, tecnólogos o profesionales de cualquier Núcleo Básico de Conocimiento
- Con conocimientos mínimos de herramientas ofimáticas e inglés.
- Cumplir con el trámite de selección definido por el centro de formación.
- Certificación curso en Caracterización de componentes en ciberseguridad o Apropiación de conceptos en ciberseguridad.

## 05 Estrategia metodológica

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; soportada en el 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 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**