IMPLEMENTACIÓN Y OPERACIÓN DE LA CIBERSEGURIDAD

Servicio Nacional de Aprendizaje - SENA

Nivel de formación: **Técnico**

01 Presentación

Código
228124

Horas
3984

Duración
27 mes

Modalidad
virtual

02 Justificación del programa

Según datos del Cyber Security Risk Report 2021 de Aon: "Equilibrando riesgos y oportunidades, facilitando la toma de mejores decisiones", el sector Tecnología, Medios de Comunicación y Telecomunicaciones se encuentra a nivel global de madurez en un nivel Básico (2.5), conforme al CyQu Scoring el cual tiene cuatro niveles, Inicial (1-1.9), Básico (2-2.5), Gestionado (2.6-3.4), Avanzado (3.5-4). El reporte explica que, "las prácticas y tecnologías de gestión de riesgos de ciberseguridad de las organizaciones no están formalizadas, y el riesgo se gestiona pensado para una situación concreta y a veces de forma reactiva, y Las prácticas y tecnologías de gestión de riesgos no están establecidas en toda la organización". Además, el reporte indica que "El Ransomware se convirtió en un riesgo de primera línea ya que la actividad creció de forma exponencial: un 400% desde el primer trimestre de 2018 hasta el cuarto trimestre de 2020". Al respecto, para todos los sectores, los controles de ciberseguridad relacionados con Ransomware y otras amenazas digitales se encuentran en los niveles básicos y la mitad de ellos apenas alcanzan el nivel gestionado con puntajes de 2.6 y 2.7, por lo que se ve necesario fortalecer los controles de ciberseguridad1.

De acuerdo con el reporte Digital Trust Insights 2021, de la PricewaterhouseCoopers - PWC, resultado de una encuesta realizada a más de 3200 directivos de negoció y tecnología a nivel mundial, donde el 40% afirman que está acelerando la digitalización, El 96% aseguró que ajustará su estrategia de ciberseguridad a raíz del COVID-19, El 20% manifestó que necesita un CISO (Oficial de Seguridad de la Información) como líder transformacional y otro 20% como líder operativo y técnico, además el 55% indicó que aumentará su presupuesto en ciberseguridad2.

El entorno del trabajo remoto hace que los empleados laboren en redes no seguras, aumentando el riesgo de amenazas cibernéticas externas y violaciones a las políticas de seguridad digital pudiendo generar impactos adversos en la organización. Esto hace que las organizaciones requieran personal de apoyo para la implementación y operación de políticas y controles de seguridad digital. Lo anterior según el artículo de Boston Consulting Group, Remote Work Works—Where Do We Go from Here?3

Actualmente en Colombia, a raíz de la pandemia del COVID-19, se ha notado una creciente participación de ciudadanos en el entorno digital, haciendo uso de las TIC (Tecnologías de la información y la comunicación) para el trabajo, el estudio, el entretenimiento, la cercanía digital entre personas, realizar pagos y otros microservicios de la vida cotidiana. Debido a lo anterior, se genera un escenario de riesgo en el crecimiento de vulnerabilidades, aumento en las amenazas digitales y delitos informáticos para las personas en los ambientes y sectores públicos y privados. En virtud de lo anterior, el gobierno nacional a dispuesto de un documento CONPES (Consejo Nacional de Política Económica y Social) 3995, Política Nacional de Confianza y Seguridad Digital que tiene como objetivo establecer medidas para ampliar la confianza digital y mejorar la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital4.

El Índice de Ciberseguridad Nacional en inglés National Cyber Security Index (NCSI), desarrollado y soportado por el e-Governance Academy (eGA), que mide en uno de sus pilares la educación y desarrollo profesional en materia de seguridad digital. Al respecto, Colombia en este pilar muestra un bajo avance, el cual es del 44%, esto de acuerdo al análisis realizado sobre la existencia de programas de educación superior a través del Sistema Nacional de Información de la Educación Superior (SNIES) del Ministerio de Educación Nacional. Lo anterior refleja la necesidad de fortalecer los programas de educación sobre seguridad digital y ciberseguridad.

Según el plan de acción para fortalecer las capacidades en seguridad digital en los ciudadanos, del sector público y privado para aumentar la confianza digital en el país del CONPES 3995, plantea en el quinto lugar que "el SENA, con apoyo del Ministerio de Tecnologías de la Información y las Comunicaciones, diseñará programas de formación profesional con enfoque para el trabajo y desarrollo humano, los cuales atenderán las necesidades sectoriales que se identifiquen durante el desarrollo de esta acción, para fortalecer las competencias en áreas como la seguridad digital, seguridad de la información, ciberseguridad e infraestructuras críticas"5. En relación a lo anterior, se diseña el programa Tecnólogo en Implementación y Operación de la Ciberseguridad, enfocado en brindar los conocimientos para diagnosticar, diseñar, implementar, operar y monitorear estrategias de ciberseguridad. Asimismo, evaluar y proponer estrategias de mejora continua. El programa ofrece la oportunidad de incorporar personal con alta calidad humana, laboral y profesional en todos los sectores, ya sean industriales, comerciales, de servicios, extractivos o primarios, contribuyendo con el desarrollo económico, social y tecnológico del país.

El SENA conocedor de la necesidad del sector, ofrece este programa de formación tecnológico con todos los elementos de formación profesional, sociales, tecnológicos y culturales, aportando como elementos diferenciadores de valor agregado metodologías de aprendizaje innovadoras, el acceso a tecnologías de última generación y una estructuración sobre métodos más que contenidos, lo que potencia la formación de ciudadanos librepensadores, con capacidad crítica, solidaria y emprendedora, factores que lo acreditan y lo hacen pertinente y coherente con su misión, innovando permanentemente de acuerdo con las tendencias y cambios tecnológicos y las necesidades del sector empresarial y de los trabajadores, impactando positivamente la productividad, la competitividad, la equidad y el desarrollo, alineado con las estrategias de gobierno y en concordancia al avance de las tecnologías a nivel mundial.

1 Cyber Security Risk Report 2021: "Equilibrando riesgos y oportunidades, facilitando la toma de mejores decisiones" - AON.
https://insights.aon.com/2021-cyber-risk-report-spanish

2 Digital Trust Insights 2021, PricewaterhouseCoopers - PWC.
https://www.pwc.com.ar/es/prensa/assets/encuesta-global-digital-trust-insights-2021.pdf

3 Remote Work Works—Where Do We Go from Here?, Boston Conulting Group - BCG.
https://www.bcg.com/publications/2020/remote-work-works-so-where-do-we-go-from-here

4 POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL, CONPES 3995.
https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

5 POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL, CONPES3995.
https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

03 Competencias a desarrollar

Competencias técnicas o específicas:

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

220501109 - Diseñar el modelo de seguridad de la información de acuerdo con estándares y marco de referencia.

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

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

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

220601044 - Monitorear sistemas de gestión de acuerdo con normativa y requerimientos técnicos.

Competencia inducción:

240201530 - Resultado de Aprendizaje de la inducción-inducción.

Competencias transversales:

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.

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

240201533 - Fomentar cultura emprendedora según habilidades y competencias personales.

240201064 - Orientar investigación formativa según referentes técnicos.

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

Competencias clave

Unidad de competencia:

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

220201501 - Aplicación de conocimientos de las ciencias naturales de acuerdo con situaciones del contexto productivo y social.

220501524 - Desarrollar procesos de comunicación eficaces y efectivos, teniendo en cuenta situaciones de orden social, personal y productivo.

240201046 - Utilizar herramientas informáticas de acuerdo con las necesidades de manejo de información.

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.

04 Perfil de ingreso

El aspirante que busca ingresar al Tecnólogo en implementación y operación de la ciberseguridad debe tener una **edad mínima de 16 años** y contar con el **nivel de educación media aprobado y certificado;** lo que quiere decir que deberá **tener aprobado el grado 11.** No requiere tener, previamente, formación para el trabajo y el desarrollo humano. Adicionalmente, debe **aprobar una prueba de aptitud y conocimiento.**

05 Perfil de egreso

El egresado del programa **Tecnólogo en implementación y operación de la ciberseguridad** es un talento humano con la capacidad de diagnosticar el estado actual de la ciberseguridad para cada contexto empresarial, con conocimientos y habilidades para implementar políticas y controles que garantizan la seguridad digital, aplicando estándares y metodologías nacionales e internacionales que permitan monitorear y controlar ciberamenazas. El tecnólogo con actitud crítica y ética tendrá la capacidad para realizar evaluaciones objetivas dentro del marco de la legislación aplicable, articulado con la mejora continua. 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.

06 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; soportadas en el 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 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.