# 3. Metodología y sistema de evaluación

# Fundamentos de Seguridad Informática

Para empezar, recordemos que el curso se basa en una pregunta central y cuatro preguntas orientadoras, una por cada eje de pensamiento, estas preguntas permitirán reflexionar acerca del conocimiento adquirido y desarrollar una postura crítica frente al mismo.

- **Pregunta central**
  ¿Por qué la seguridad informática se ha convertido en un tema de gran importancia para las empresas y las personas?

**Pregunta por eje**

- Eje 1. Conceptualización: ¿De qué y qué se debe proteger en los sistemas informáticos y la información?
- Eje 2. Analicemos la situación: ¿Cuál o cuáles procesos permiten mitigar los riesgos de seguridad a los que está expuesta la información?
- Eje 3. Pongamos en práctica: ¿Cómo se pueden detectar las vulnerabilidades en los sistemas informáticos?
- Eje 4. Propongamos: ¿A qué amenazas se ven expuestos los sistemas informáticos y cómo se pueden minimizar sus posibles efectos?

De acuerdo con estas preguntas, se realizará la construcción del conocimiento a partir problemas reales, generando conceptos y soluciones apropiadas.

El tutor (docente) y el estudiante estarán en constante comunicación por medio de foros, encuentros sincrónicos, chat, entre otros medios.

- Las lecturas complementarias, las videos cápsulas, los talleres, los estudios de caso, hacen parte integral de la formación, ayudan a aclarar dudas y dan herramientas para el entendimiento de cada tema trabajado, por tal motivo es indispensable desarrollar las actividades en el momento que se les indique.

- El curso inicia con conceptos básicos de seguridad informática, los cuales se aplican en ejercicios y talleres prácticos. Durante el desarrollo de los contenidos aumenta su complejidad, y en el transcurso de las semanas se adquiere un conocimiento sólido en el tema de seguridad.

Por otra parte frente al sistema de evaluación encontramos que:

- El eje uno y el eje tres contienen trabajo evaluativo individual, tipo cuestionario y taller.
- Los ejes dos y cuatro presentan un trabajo evaluativo- colaborativo tipo taller del cual se deben generar evidencias.

Al finalizar el curso el estudiante se encuentra en capacidad de reconocer las principales vulnerabilidades y amenazas a las que está expuesta la información y los dispositivos que la contienen, en este sentido se desarrollan habilidades propias para el diseño, implementación, seguimiento y auditoría de una política de seguridad capaz de mitigar y/o minimizar el impacto de un incidente de seguridad, bajo la aplicación del ciclo de mejora continua PHVA.