

# 1. Nuestra pregunta

## Fundamentos de Seguridad Informática

### Pregunta Principal

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

### Eje 1

**¿De qué y qué se debe proteger en los sistemas informáticos y la información?**

### Justificación

Un paso fundamental en el análisis de seguridad, es definir qué elementos proteger y contra qué tipo de riesgos, además, generar un plan de acción tendiente a minimizar el impacto de cualquier acción que atente contra la seguridad física y/o lógica.

### Eje 2

**¿Cuál o cuáles procesos permiten mitigar los riesgos de seguridad a los que está expuesta la información?**

### Justificación

Garantizar al 100% la seguridad es imposible, por tal motivo, se deben generar procesos que minimicen el impacto de algún evento inesperado e imprevisto.

El ciclo de mejora continua PHVA es una excelente herramienta ya que permite optimizar el proceso de gestión de la seguridad de la información y se orienta al desarrollo de un plan adecuado de seguridad.

### Eje 3

**¿Cómo se pueden detectar las vulnerabilidades en los sistemas informáticos?**

### Justificación

Las vulnerabilidades en los sistemas son los agujeros que aprovechan los delincuentes informáticos para acceder de manera irregular al sistema, con diversos fines u objetivos (manipulación, robo, daño, alteración, entre otros).

Dichas vulnerabilidades son predecibles y deben hacer parte de una adecuada política de seguridad.

#### **Eje 4**

**¿A qué amenazas se ven expuestos los sistemas informáticos y como se pueden minimizar sus posibles efectos?**

Justificación

Las amenazas a diferencia de las vulnerabilidades, no son predecibles por lo cual se deben tratar con mayor atención, generando políticas de seguridad, planes de continuidad del negocio, y comités de emergencia capacitados en la toma de decisiones en situaciones extremas.

#### **Competencia**

**C1:** El estudiante conoce, actualiza y profundiza sobre los conceptos, ámbitos, metodologías, técnicas y procesos aplicados en la seguridad informática, para diseñar estrategias básicas que permitan proteger los recursos informáticos de las organizaciones.

Propósito de formación

Al finalizar el curso, el estudiante se encuentra en capacidad de reconocer los principales riesgos a los que están expuestos los sistemas informáticos, puede diferenciar una vulnerabilidad de una amenaza y genera planes de acción tendientes al mejoramiento continuo de la seguridad de la información y de los equipos informáticos.