



**internet  
solutions**  
*The information security experts*

# TEMARIO PRIMER RESPONDIENTE

**Duración 20 hrs**





**Internet  
solutions**  
*The information security experts*

## **Curso Primer Respondiente**

Presenta los conocimientos básicos asociados a la respuesta a incidentes informáticos y de ciberseguridad, así como laboratorios.

### **Objetivos de aprendizaje**

Al finalizar el curso el estudiante estará en la capacidad de:

- Identificar los términos y conceptos relacionados con la respuesta a incidentes informáticos y de ciberseguridad.
- Potencializar el saber hacer de las personas encargadas de la informática forense.

### **Pre-requisito**

Conceptos básicos de sistemas.



**01**

## **Conceptos básicos (2 hrs)**

*Los temas expuestos en la unidad brindan información puntual de la ciencia forense aplicada a la informática y la evidencia digital.*

- Temas de componentes de la información forense.
- Autoevaluación.

**02**

## **Legal (2 hrs)**

*Su componente principal es dar a conocer leyes y estándares nacionales e internaciones, en los cuales se enmarca los requisitos y buenas prácticas en la potencial evidencia digital.*

- Estándares, normas, leyes nacionales e internacionales
- Autoevaluación.



03

### **Paso a paso (1 hora)**

*Explicación de los pasos que cumple el procedimiento de policía judicial en respuesta a incidentes informáticos, aplicado al sector privado.*

- Procedimiento de Policía Judicial en respuesta a incidentes informáticos.
- Autoevaluación.

04

### **Función de Hash (2 hrs)**

*Desarrollo del tema teórico práctico, que conduce a la comprensión de la importancia del empleo de los algoritmos **hash** en la potencial evidencia digital.*

- Importancia y obligatoriedad de las funciones de hash.
- Laboratorio.
- Autoevaluación.



**05**

## **Sanitización (2 hrs)**

*Procedimiento de alistamiento de dispositivos de almacenamiento de datos digitales utilizados como destino de potencial evidencia digital.*

- Laboratorio.

**06**

## **Estampa de tiempo (2 hrs)**

*Aplicación de fecha, hora y función de hash, por intermedio de un tercero, el cual se respalde el desarrollo de una actividad con potencial evidencia digital.*

- Aplicación de la estampa de tiempo.
- Laboratorio.
- Autoevaluación.



**07**

## **Equipos y herramientas (1 hora)**

*Explicación de software y hardware empleado para el desarrollo de la informática forense.*

- Hardware y software.

**08**

## **Manejo de la potencial evidencia digital (8 hrs)**

*Laboratorios prácticos en el cual se desarrollan los principios de la identificación, recolección, adquisición y preservación de potencial evidencia digital, tomando como base la RFC 3227, ISO 27037 y otros estándares.*

- Identificación.
  - *Fijación fotográfica (laboratorio).*
- Recolección.
  - *Formatos (laboratorio).*
- Adquisición.
  - *Herramientas (laboratorio).*
- Preservación.
  - *Cadena de custodia (laboratorio).*



# internet solutions

*The information security experts*



Para más información:

[www.internet-solutions.com.co](http://www.internet-solutions.com.co)