



Computación Forense

Importancia en los crímenes de hoy en día

S1 V1

Profesor: Ing. Alex Araya Rojas, MT
CISSP, CISM

Importancia de la Computación Forense

- Hoy en día, no existe prácticamente un solo caso que no requiera o en el cual no esté presente un dispositivo electrónico.
- Estos dispositivos son vitales como elementos probatorios en las cortes todos los días, pueden confirmar o descartar sospechas por igual.
- Un teléfono celular, nos puede ayudar a probar la posición inicial y final de una persona, así como la velocidad, fecha y hora del trayecto.
- De igual manera, con los dispositivos electrónicos podemos demostrar hábitos de consumo y comportamiento muy fácilmente (Direcciones IP, páginas web, etc.)



Retos del Investigador

¿Es complejo realizar análisis forenses?

- El ritmo vertiginoso con el que se modernizan las tecnologías, el surgimiento de nuevas aplicaciones, protocolos y herramientas, hace imposible que los investigadores forenses se mantengan 100% al día, este es uno de los retos más importantes.
- Otras complicaciones que enfrentan los investigadores son los temas de globalidad, las deficiencias en conocimiento legal de los técnicos, la volatilidad de la evidencia y la aplicación de técnicas anti forense.



Reglas de Oro de la Investigación Forense

La evidencia

- Conocer las reglas que aplican para el lugar de la extracción o análisis de la evidencia, el tipo de caso, los objetivos, etc.
- Prevenir cualquier alteración de la evidencia digital, ya sea intencional o por negligencia.
- Trabajar siempre con copias de la evidencia, nunca con la evidencia original.



Es natural que, por la transformación digital, como sucedió en todas las herramientas mecánicas o industriales, surgiera el concepto de Ciberseguridad y la Seguridad de la Información.

Preparación Forense

The diagram illustrates the relationship between three key concepts in digital security. On the left, a large, dark purple, irregular blob shape is labeled 'Preparación Forense'. This shape has a hatched pattern on its left side. To its right is a 2x2 grid of rounded squares. The top-left square is labeled 'Procesos', the top-right 'Personas', the bottom-left 'Datos', and the bottom-right 'Tecnología'. The 'Tecnología' square is a darker shade of purple than the others. A large, light purple arrow points from the 'Preparación Forense' shape towards the grid. To the left of the grid is the text 'Seguridad de la Información' in a pinkish-purple color, and to the right is 'Seguridad Informática' in a dark purple color.

Seguridad de la
Información

Procesos

Personas

Datos

Tecnología

Seguridad
Informática



Preparación Forense

Ataques a la información o a los servicios empresariales



Seguridad Informática



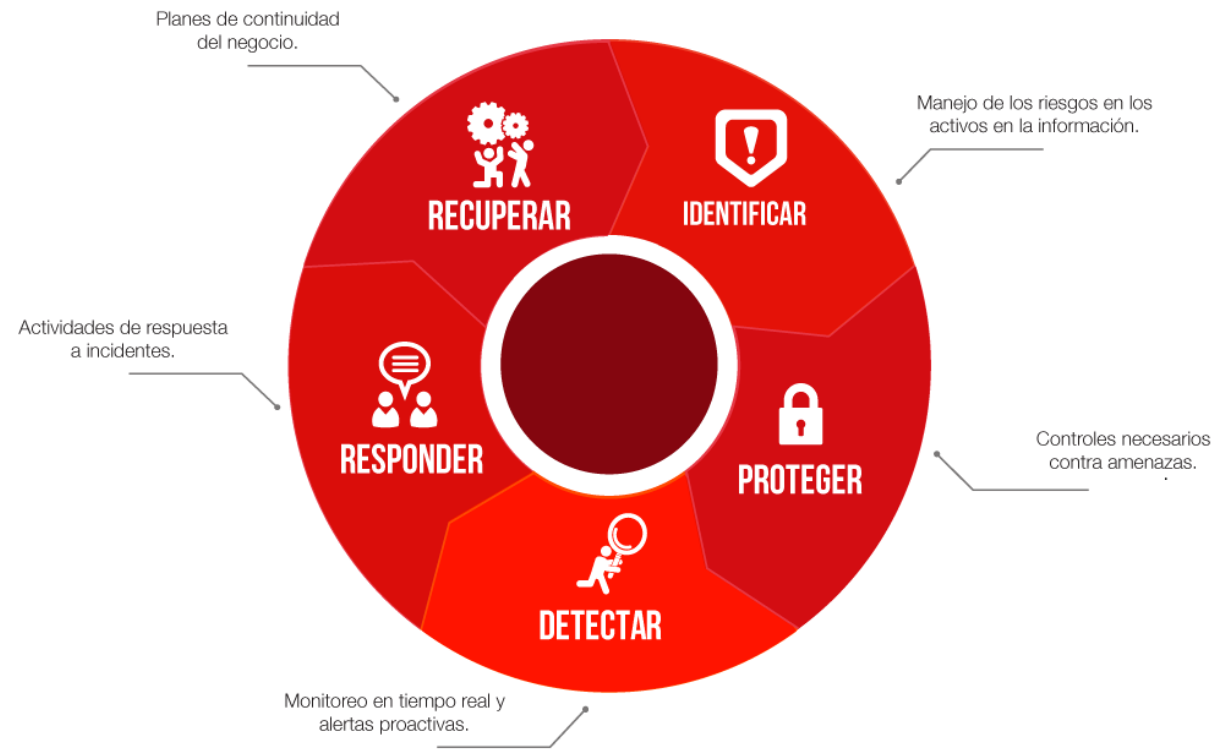
Seguridad de la
Información

Preparación Forense

Preparación Forense

¿Y en los ratos sin incidentes?

- El equipo debe trabajar en la preparación forense de la organización de forma proactiva, para que en los momentos en los que se requiera su participación, los procesos sean expeditos y se cumplan a cabalidad.
- La inclusión de los equipos en los procesos de respuesta a incidentes debe ser natural.





Gracias