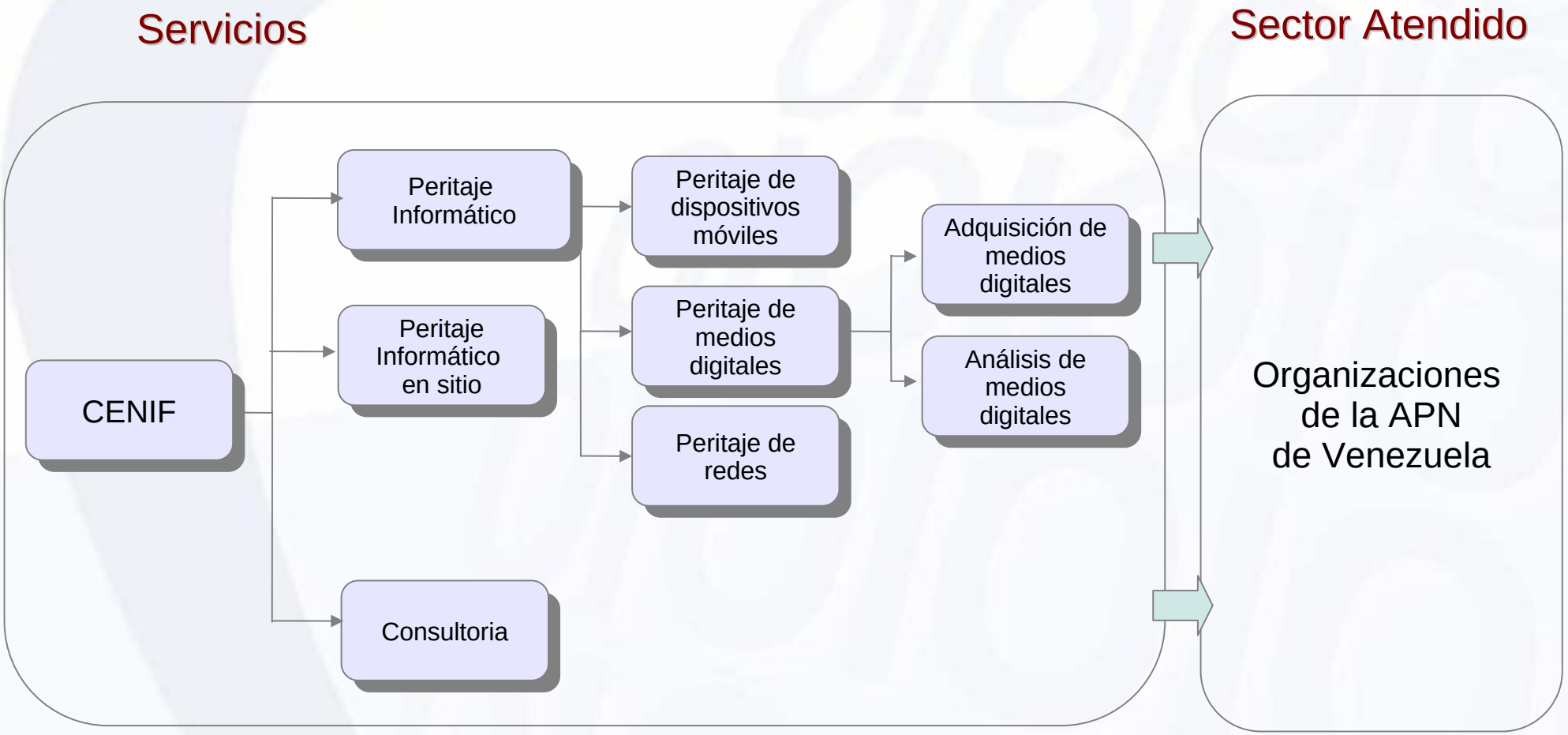
Estudio de incidentes: Antes, durante y análisis forense

Carlos Augusto Loyo
Coordinador CENIF

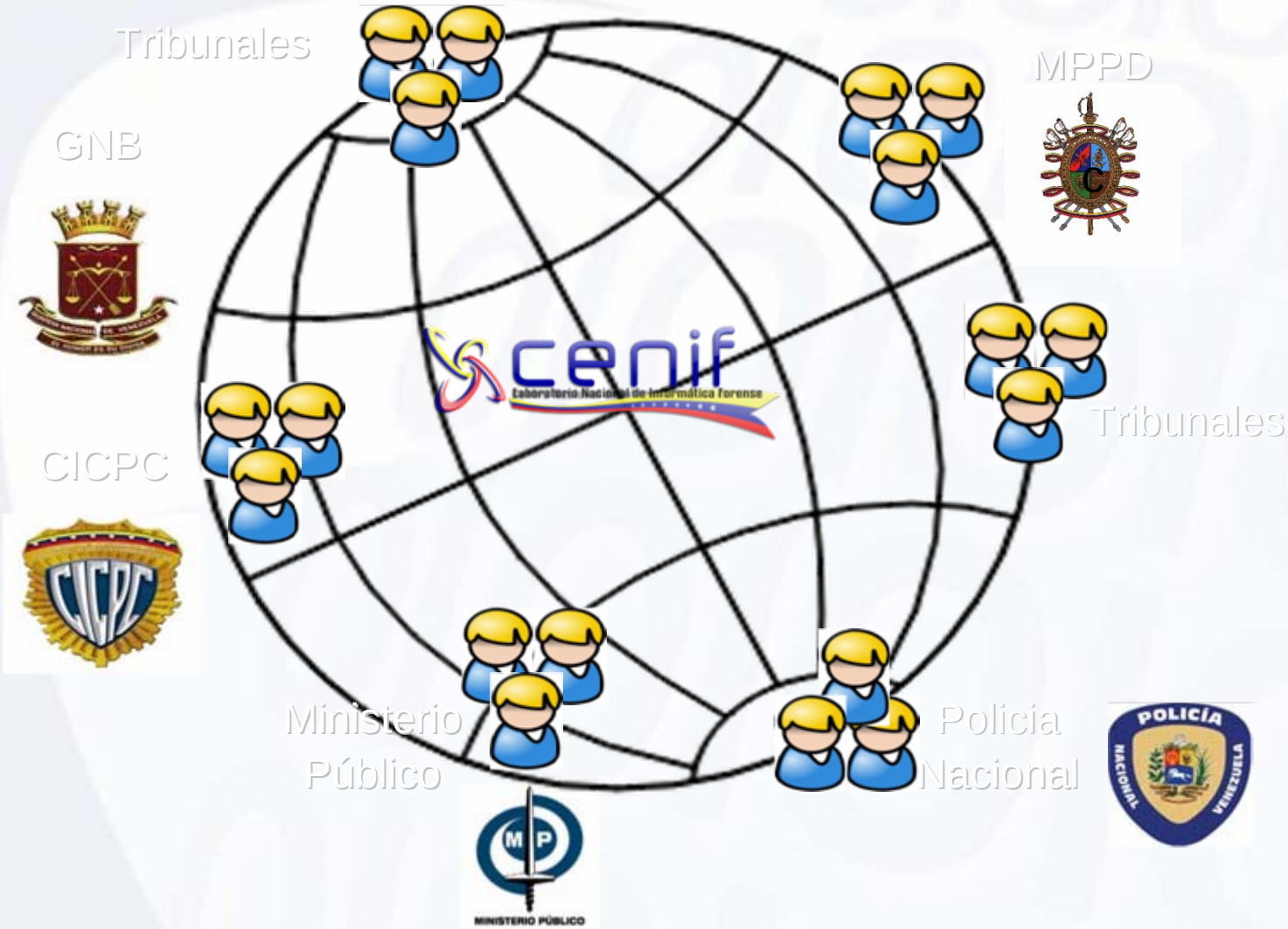
OBJETIVO

El Centro Nacional de Informática Forense
es un laboratorio de informática forense
para la adquisición, análisis, preservación y presentación de las
evidencias relacionadas a la tecnologias de información
y comunicación, con el objeto de prestar apoyo a los
cuerpos de investigación judicial órganos y entes del Estado
que así lo requieran.

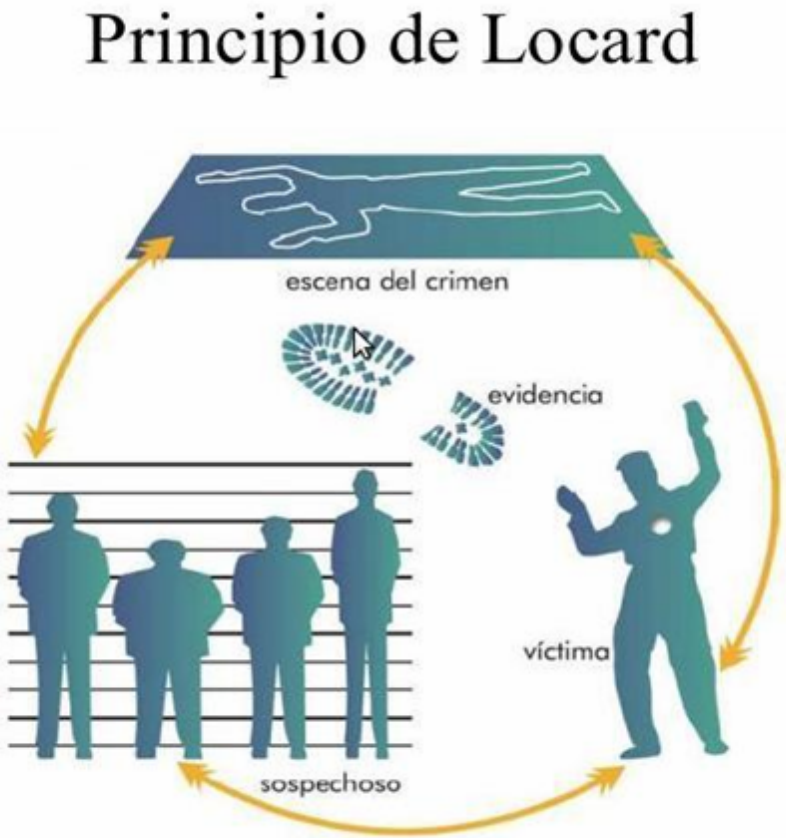
MODELO DE SERVICIO



SECTORES ATENDIDOS



PRINCIPIO DE INTERCAMBIO DE LOCARD



- "Siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto"

De Uso Público

INCIDENTE

Incidente de Seguridad Informática

"Es cualquier evento adverso, relacionado con la seguridad de un sistema informático o de las comunicaciones informáticas "
http://www.cert.org

INCIDENTE

¿Qué hacer frente al incidente ?

- **Mitigar** : Restaurar la operatividad.
- **Identificar** : ¿Cómo? ¿Cuándo? ¿Dónde?
- **Preservar evidencia** : Posible judicialización.

INCIDENTE

Mejor escenario: Posible judicialización

Validez judicial : Merituada por el juez según el ámbito.

Validez técnica: Colección y análisis mediante buenas prácticas que asegure la inalterabilidad.

EVIDENCIA DIGITAL

Toda información digitalizada susceptible, de ser analizada por un método técnico y de generar conclusiones irrefutables en lo legal, debe poseer las siguientes características:

De Uso Público

CARACTERÍSTICAS

- No podemos “verla”.
- No se puede interpretar sin conocimientos técnicos.
- Es sumamente volátil.
- Puede copiarse sin límites.
- Las copias son indistinguibles del original.
- Bueno para los peritos: podemos analizar una copia sin contaminar la prueba original.
- Malo para los juristas: el concepto de “original” carece de sentido.
- Suele requerir información contextual para su interpretación.

CASO: Carro Bomba

Escena del Crimen

Victimario

Ejecuta

Carro Bomba

Escena del Crimen

Se colecta

Memoria Flash

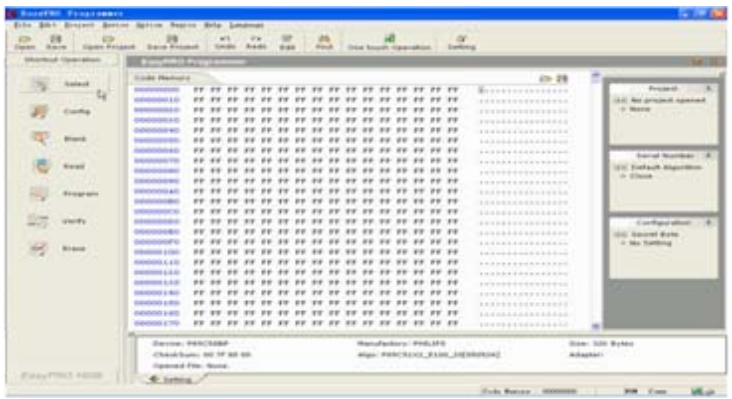
CASO: Carro Bomba

Análisis Forense

Memoria Flash

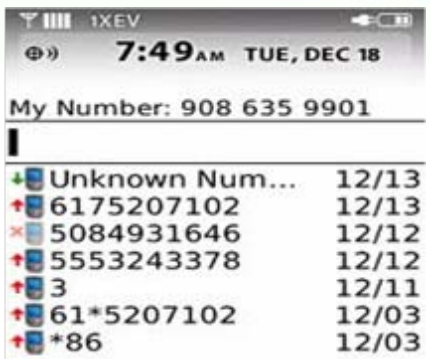
Soporta 0° C a 70° C

Analizado por



Análisis Memoria Flash

Últimas llamadas



Resultado: Identificación del victimario