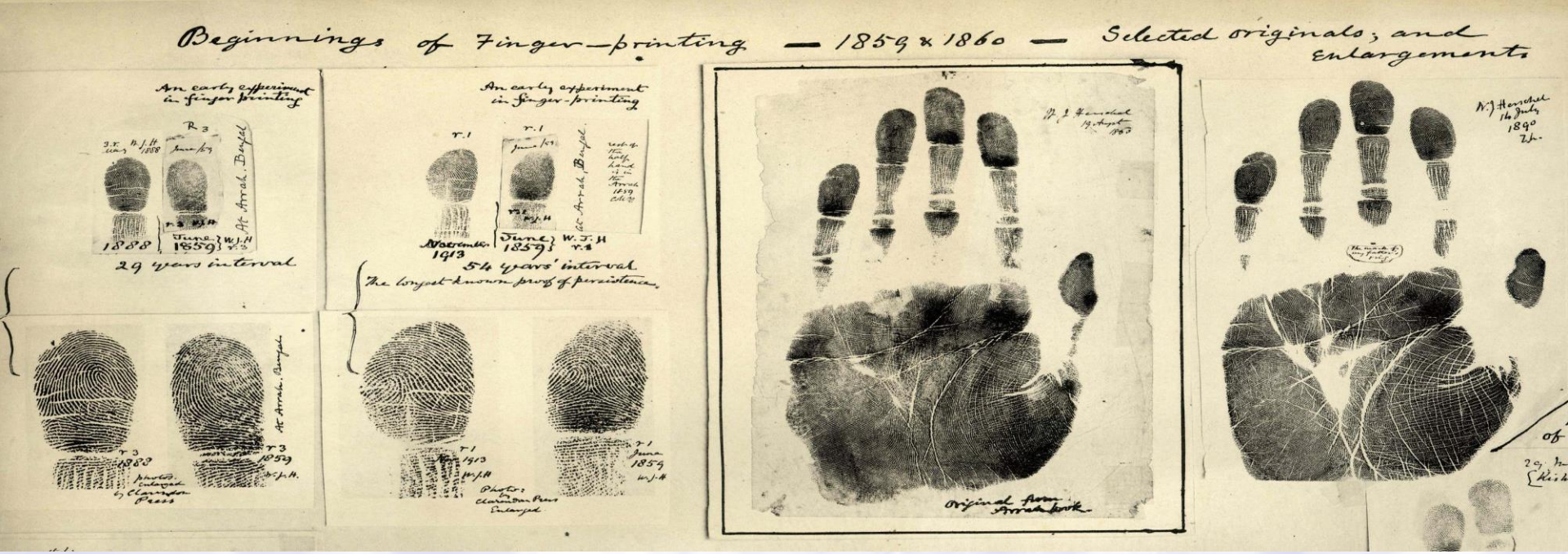
# Evidencia Digital en el Proceso Judicial

Dr. Santiago Acurio Del Pino

# Agenda

- Evidencia digital
  - Introducción
  - Qué es evidencia Digital
  - Necesidad de la evidencia digital
  - Problemática
- Validez de la Evidencia Digital
- Conclusiones




# Evidencia Digital

Introducción, necesidad de la evidencia y la problemática

# Introducción

- Los problemas tradicionales al manejar investigaciones relacionadas con equipos informáticos, es la forma como se recupera la información digital o electrónica de esta clase de equipos,.
- El problema radica en cómo instrumentalizar un procedimiento o un método adecuado para realizar esta tarea, cumpliendo con la premisa de que estas prácticas deben ser aceptadas y puestas en acción de forma universal y respetando el debido proceso.

# Definiciones

- Por **evidencia** entendemos cualquier dato o información que pueda ser utilizado para determinar o demostrar la veracidad, que prueba un hecho una vez realizado o bien que no ha sido realizado.
- Por **evidencia digital y electrónica** entendemos cualquier evidencia soportada en formato que se ha sido generada, transmitida, recibida por un dispositivo electrónico o informático que permiten archivar y reproducir la palabra, el sonido, la imagen y datos de cualquier otra clase.
- En definitiva son **campos magnéticos y pulsos electrónicos** que pueden ser recogidos y analizados usando técnicas y herramientas especiales

# Clases de Evidencia Digital

- En un principio el tipo de evidencia digital que se buscaba en los equipos informáticos era del tipo **CONSTANTE** o **PERSISTENTE** es decir la que se encontraba almacenada en un disco duro o en otro medio informático y que se mantenía preservada después de que la computadora era apagada.
- Posteriormente y gracias a las redes de interconexión, el investigador forense se ve obligado a buscar también evidencia del tipo **VOLÁTIL**, es decir evidencia que se encuentra alojada temporalmente en la memoria RAM, o en el CACHE, son evidencias que por su naturaleza inestable se pierden cuando el computador es apagado.
- Este tipo de evidencias deben ser recuperadas casi de inmediato.

# Necesidad de la evidencia digital

- En un mundo donde el uso de la redes de comunicaciones es cada vez es más intensivo (celulares, Internet, redes sociales y entornos 2.0 por poner algunos ejemplos) y, por lo tanto, donde las relaciones interpersonales se canalizan a través de medios electrónicos y telemáticos, es lógico que empiece a surgir la necesidad de probar o acreditar las actuaciones legítimas transferencias bancarias, declaraciones de impuestos….) o las conductas ilícitas de las que somos víctimas (fraudes informáticos como el PHISING, acosos a través de redes sociales, amenazas mediante SMS) en el formato en que se producen: el digital.

# Problemática

- Ahora se recibe un mensaje en el chat o un SMS en donde el componente digital o electrónico generan varios problemas:
  - 1.- **la manipulación** (¿puede un juez estar completamente seguro de que el mensaje de datos que se le muestra no ha sido manipulado por el receptor?),
  - 2.- **la volatilidad** (se puede borrar, perder, alterar) y cómo llevar ese mensaje de datos a un proceso con garantías de que no ha sido manipulado ante un Tribunal de Justicia


# Validez de la evidencia digital

Normas Legales COIP, COGEP, LCE, COFJ

# Necesidad de Prueba

- La prueba dentro del proceso judicial es de especial importancia, ya que desde ella se confirma o desvirtúa una hipótesis o afirmación precedente, el objetivo del proceso conduce hacia la averiguación de la verdad formal.

# Necesidad de Prueba

## COIP

### Materias Penales

- Comprobar la existencia material de la infracción y la responsabilidad penal de la persona procesada.
- Generar convicción en el Juzgador más allá de todo duda razonable.

## COGEP

### Materias no Penales

- A la hora de sustanciar ante cualquier Tribunal de Justicia una cuestión litigiosa hay que tener presente que para que las pretensiones de las partes prosperen no basta con relatar los hechos acaecidos sino que también hay que desplegar la actividad probatoria necesaria que acredite la veracidad del relato fáctico que se expone. (Art. 162 del COGEP)

# Normas Legales

**Ley de Comercio Electrónico y Firmas Electrónicas**

- **Artículo 2.- Reconocimiento jurídico de los mensajes de datos**.- Los mensajes de datos tendrá **igual valor jurídico que los documentos escritos.** Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta Ley y su reglamento.

**Ley de Comercio Electrónico y Firmas Electrónicas**

**Artículo 52.- Medios de prueba.-** Los mensajes de datos, firmas electrónicas, documentos electrónicos y los certificados electrónicos nacionales o extranjeros, emitidos de conformidad con esta Ley, cualquiera sea su procedencia o generación, **serán considerados medios de prueba.** Para su valoración y efectos legales se observará lo dispuesto en el Código de Procedimiento Civil.

# Concepto de Mensaje de Datos

- Es toda aquella información generada por medios electrónicos, digitales o similares que puede ser almacenada o intercambiada por cualquier medio. Ejemplos: documentos electrónicos, correo electrónico, páginas Web, telegrama, télex, fax, facsímil e Intercambio electrónico de datos.

# Ley de Comercio Electrónico

- Los mensajes de datos tienen el mismo valor que los documentos escritos en virtud del principio de equivalencia funcional.
  - Se equiparan a escrito y a original
- Los mensajes de datos son medios de prueba.
  - El medio probatorio es el camino que designa la ley para ingresar el objeto de prueba al proceso

# Normas Legales

- **Art. 147.- VALIDEZ Y EFICACIA DE LOS DOCUMENTOS ELECTRÓNICOS.-** **Tendrán la validez y eficacia de un documento físico original,** los archivos de documentos, mensajes, imágenes, bancos de datos y toda aplicación almacenada o transmitida por medios electrónicos, informáticos, magnéticos, ópticos, telemáticos, satelitales o producidos por nuevas tecnologías, destinadas a la tramitación judicial. Ya sea que contengan actos o resoluciones judiciales. Igualmente los reconocimientos de firmas en documentos o la identificación de nombre de usuario, contraseñas, claves, utilizados para acceder a redes informáticas. Todo lo cual, siempre que cumplan con los procedimientos establecidos en las leyes de la materia.

# Normas Legales

## Código Orgánico Integral Penal

- Artículo 499.- La prueba documental se regirá por las siguientes reglas:
  - 6. Podrá admitirse como medio de prueba todo contenido digital conforme con las normas de este Código.

## Código Orgánico General del Procesos

- Art. 196.- Producción de la prueba documental en audiencia. Para la producción de la prueba documental en audiencia de juicio se procederá de la siguiente manera:
  - 3. Las fotografías, grabaciones, los elementos de pruebas audiovisuales, computacionales o cualquier otro de carácter electrónico apto para producir fe, se reproducirán también en su parte pertinente en la audiencia y por cualquier medio idóneo para su percepción por los asistentes.

# Normas Legales COGEP

- Art. 202.- Documentos digitales. los documentos producidos electrónicamente con sus respectivos anexos, serán considerados originales para todos los efectos legales.
  - Las reproducciones digitalizadas o escaneadas de documentos públicos o privados que se agreguen al expediente electrónico tienen la misma fuerza probatoria del original.
  - Los documentos originales escaneados, serán conservados por la o el titular y presentados en la audiencia de juicio o cuando la o el juzgador lo solicite.
  - Podrá admitirse como medio de prueba todo contenido digital conforme con las normas de este código.

# Contenido Digital

- **Artículo 500 COIP.-** El contenido digital es todo acto informático que representa hechos, información o conceptos de la realidad, almacenados, procesados o transmitidos por cualquier medio tecnológico que se preste a tratamiento informático, incluidos los programas diseñados para un equipo tecnológico aislado, interconectado o relacionados entre sí.

# Reglas para recuperar el Contenido Digital

- El análisis, valoración, recuperación y presentación del contenido digital almacenado en dispositivos o sistemas informáticos se realizará a través de **técnicas digitales forenses**.
  - Art. 500.1 del COIP

# Reglas para recuperar el Contenido Digital

- Cuando el contenido digital se encuentre almacenado en sistemas y **memorias volátiles** o equipos tecnológicos que formen parte de la **infraestructura critica** del sector público o privado, se realizará su recolección, en **el lugar y en tiempo real**, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido.
  - La Integridad se garantiza con el uso de códigos de integridad, a través de la aplicación de algoritmos matemáticos que calculan un número único basado en el contenido del mensaje de datos, conocido como función HASH.
  - Art. 500.2 del COIP

# Recuperación en el lugar y en tiempo real

- Este numeral nos indica la priorización que debe hacer el investigador forense cuando el contenido digital se encuentre en memorias volátiles o equipos tecnológicos que sean parte de la infraestructura crítica, y que **no se pueden trasladar a un laboratorio forense**, debido a que se pueden perder debido a la volatilidad del dispositivo de almacenamiento como son las memorias RAM o por pertenecer a una infraestructura crítica **no pueden ser desconectados**, por ello la norma recomienda:
  - una adquisición en tiempo real, para lo cual el investigador debe estar entrenado en obtener esta clase de evidencia digital de un equipo encendido, de igual forma debe recuperar la información importante de la red donde se encuentre el equipo informático con fuente importante de evidencia digital, sus hallazgos deben estar descritos de forma detallada en un documento que muestre todos los pasos para conseguir la evidencia en tiempo real, tratando de minimizar el impacto de sus acciones en el sistema.

# Recuperación en el lugar y en tiempo real

- En este caso los servidores policiales y del Sistema Especializado Integral de investigación, Medicina Legal y Ciencias Forenses deberán de acuerdo al **Instructivo para el manejo de indicios y/o evidencia digital** realizar:
  - **Captura de la Memoria RAM.** a) Acoplamiento físico por una interfaz nuevo (USB, disco externo, cd, DVD, etc.) proporcionado por el Sistema Especializado Integral de Investigación, Medicina Legal y Ciencias Forenses. b) Volcado (adquisición) de la información capturada al medio externo para su conservación y preservación. c) Apagar el dispositivo y/o equipo informático. d) Entrega del medio de almacenamiento, al Centro de Acopio e inicio de cadena de custodia.

# Infraestructura crítica

- Debemos mencionar que este procedimiento solamente se aplica a la memoria RAM, pero no dice nada del contenido digital de equipos tecnológicos que sean parte de la infraestructura crítica, es por ello que el investigador debe aplicar el denominado **“orden de volatilidad”** que hace relación al periodo de tiempo en que cierta información (mensajes de datos o contenido digital) está disponible en el equipo o sistema informático.

# Orden de volatilidad

- Registros y contenido cache
- Tabla de enrutamiento, Cache ARP, tabla de procesos, estadísticas del kernel, memoria.
- Información temporal del sistema
- Logs o bitácoras del sistema
- Configuración física y topología de red
- Documentos

# Cadena de Custodia / Integridad

- Luego de recuperada la información se menciona que para preservar la integridad del contenido digital esto se debe hacer mediante la cadena de custodia, esta situación planteada en el COIP es un error ya que **no se puede probar la integridad del contenido digital por medio de cadena de custodia**, ya que esta es sobre los elementos físicos, basados en el principio criminalístico de mismisidad.
  - **En el Art. 456 se dice que se aplicará la cadena de custodia a los elementos físicos y al contenido digital.**
- Para garantizar la integridad del contenido digital esta se debe hacer a través de **un código de integridad o función HASH**, es decir de una firma electrónica como así lo dispone el Art.7 del reglamento a la Ley de Comercio Electrónico y Mensajes de Datos.

# Contenido Digital en medios no volátiles

- Cuando el contenido digital se encuentre almacenado en medios no volátiles, se realizará su recolección, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido.

# Procesamiento medios de almacenamiento de contenido digital

- Cuando se recolecte cualquier **medio físico** que almacene, procese o transmita contenido digital durante una investigación, registro o allanamiento, se deberá **identificar e inventariar cada objeto individualmente**, fijará su ubicación física con fotografías y un plano del lugar, se protegerá a través de técnicas digitales forenses y se trasladará mediante **cadena de custodia** a un centro de acopio especializado para este efecto.

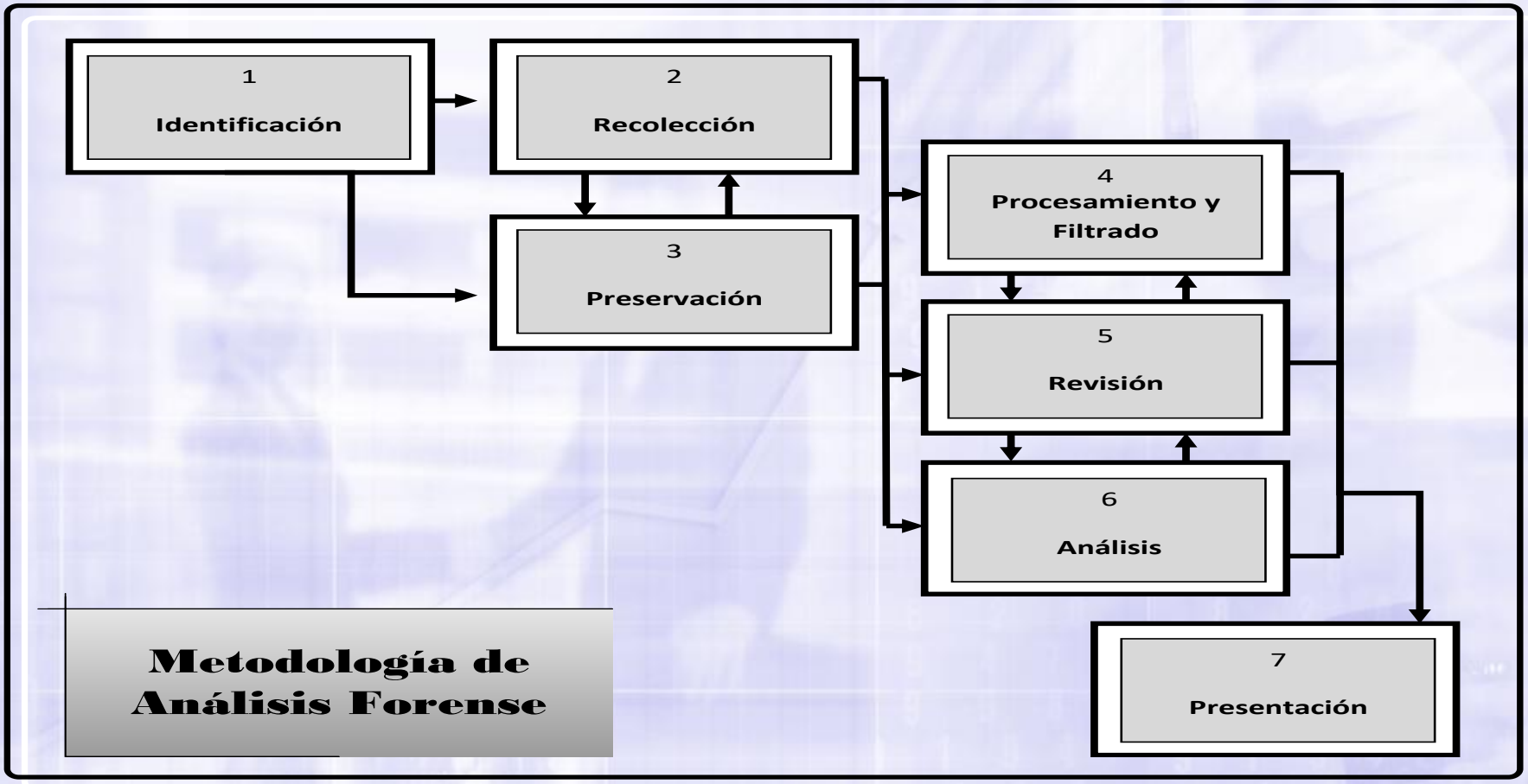
# Procesamiento….

- El último numeral hacer relación a la cadena de custodia sobre los elementos físicos (medios), relacionados con el almacenamiento, procesamiento o trasmisión del contenido digital (mensajes de datos), y la forma que deben estos ser preservados y recolectados.

# Procesamiento…

- En este caso los servidores policiales y del Sistema Especializado Integral de investigación, Medicina Legal y Ciencias Forenses deberán de acuerdo al Instructivo para el manejo de indicios y/o evidencia digital realizar:
  - **Fijación Digital de los dispositivos y equipos informáticos en funcionamiento**: La fijación digital se fundamenta en tres tomas fotográficas: a) Estado inicial del equipo, componentes y conexiones (accesorios externos del equipo). b) Plaquetas de identificaciones técnicas (número de serie y modelo). c) Fijación del escritorio (ubicación de los íconos instalados por programas).
  - **Fijación Digital de los dispositivos y equipos informáticos que se encuentren apagados:** a) Identificación del dispositivo y/o equipo informático, componentes y conexiones (accesorios externos del equipo). b) Plaquetas de identificaciones técnicas (número de serie y modelo). c) Fijación del indicio en el lugar de los hechos e inicio de cadena de custodia.

# Metodología de análisis forense



# Normas Legales

## Ley de Comercio Electrónico y Mensajes de Datos

Art. 55.- Valoración de la prueba.- (….)

Para la valoración de las pruebas, el juez o árbitro competente que conozca el caso deberá designar los peritos que considere necesarios para el análisis y estudio técnico y tecnológico de las pruebas presentadas.

## Código Orgánico General por Procesos

- Art. 164 Valoración de la Pruebas.- Las Pruebas deberán valorarse en conjunto de acuerdo a la sana crítica, y deben ser solicitadas, practicadas e incorporadas de acuerdo al COGEP.
- Art. 168.- Prueba para mejor resolver. El Juez podrá de manera excepcional podrá ordenar de oficio la práctica de prueba. (Art. 130.10 del COFJ)

# Reglas en la obtención de la evidencia digital

- En la obtención de la evidencia digital, el juez se debe verificar estas sencillas reglas:
  - Que la obtención de la evidencia digital, se hecho **sin alterar o dañar el dispositivo** de almacenamiento que la contiene.
  - Que la evidencia digital obtenida, sea autentificada, es decir verificando que esta es **idéntica a la original**.

# Otras reglas en la obtención de la evidencia digital

- El juez verificará que la evidencia digital fue obtenida
  - En concordancia con los principios de la ciencia forense informática
  - Usando de **estándares y mejores prácticas**
  - Usando herramientas probadas y verificadas en la identificación, recuperación, filtrado de evidencias digitales, al igual usando los elementos correctos para embalar, etiquetar y preservar evidencia digital.
  - Todo el trabajo debe ser **documentado** de manera profunda y en detalle.
  - Si existe un peritaje. **Este debe ser sustentado oralmente en la audiencia correspondiente**

# Legitimación de la Evidencia Digital o Electrónica

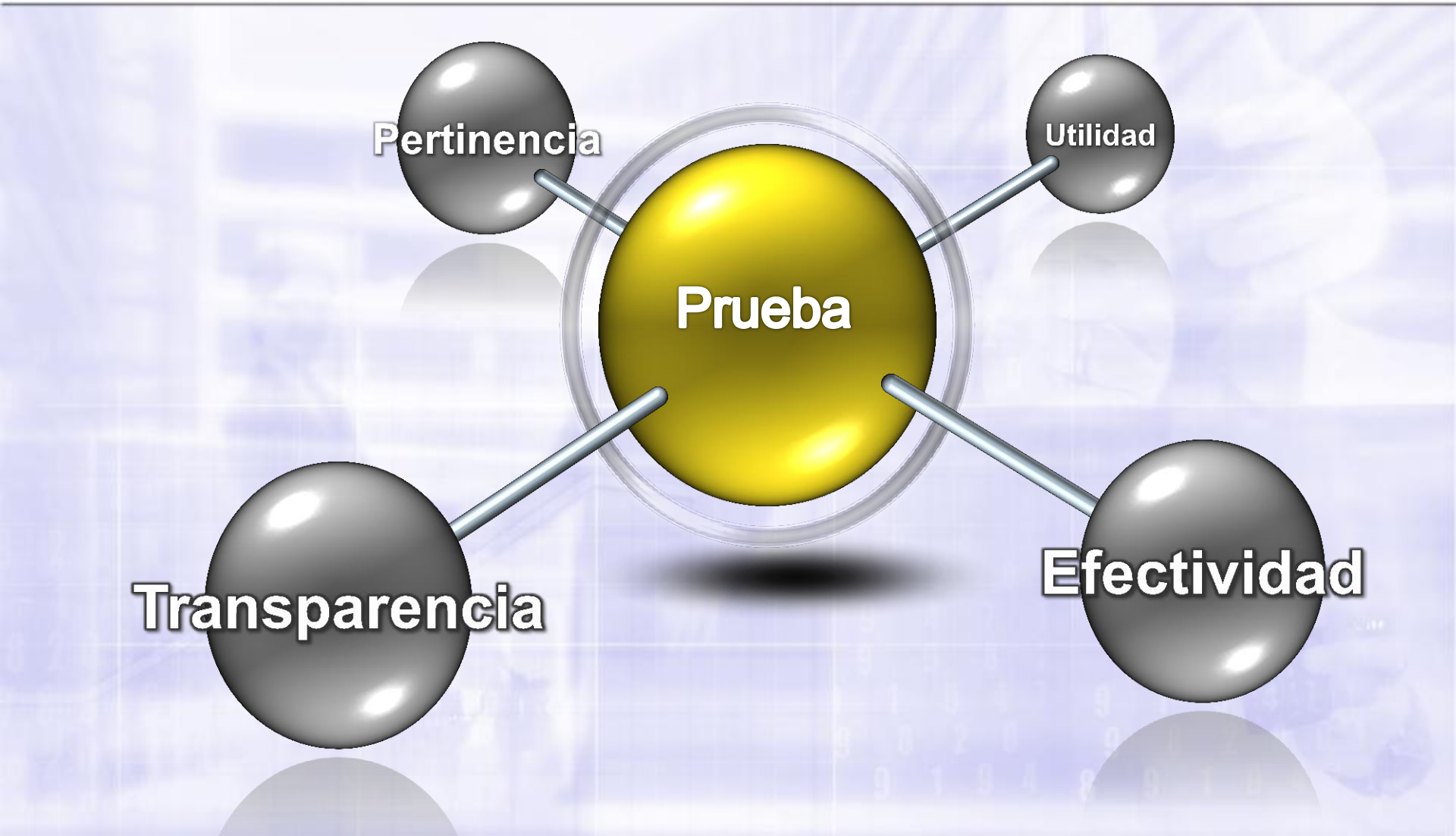
**Efectividad**

- Respeto por la protección de datos personales
- Respeto por la intimidad personal
- Respeto por el Secreto de las Comunicaciones
- Respeto por la libertad de expresión

**Utilidad**

- Finalidad lícita
- Necesidad de recolección
- Transparencia en el recolección
- Proporcionalidad en el recolección

# Legitimidad de la Prueba



# Conclusiones y Preguntas

Evidencia Digital

# Conclusiones

- La evidencia digital tanto en el COIP como en el COGEP es un medio de prueba **DOCUMENTAL**
- La Ley de CE, permite que para la valoración de los mensajes de datos se recurra al **auxilio de peritos**
- Todo peritaje deberá ser sustentado con el **testimonio del perito** en la audiencia correspondiente

# Preguntas

- Gracias por su atención
- Dr. Santiago Acurio Del Pino
- smacurio@gmail.com
- sacurio@hotmail.com