# Principios durante la recolección de evidencias

# Normativa → principios

Existen diversas sugerencias y normativas, ninguna de carácter obligatorio, que abordan el procedimiento de recopilación de evidencias:

- La norma ISO/IEC 27037 fija las pautas para la identificación, recolección, obtención y conservación de evidencia digital.
- La guía RFC 3227 plantea una serie de prácticas recomendadas para recopilar y almacenar evidencias.
- AENOR UNE 71505-2:2013: sistema de gestión de evidencias electrónicas. Buenas prácticas en la gestión de las evidencias electrónicas.
- AENOR UNE 70506:2013: tecnologías de la información (TI). Metodología para el análisis forense de las evidencias electrónicas.

# Normativa → principios

Relación entre estándares internacionales y los fundamentos de la informática forense.

# Normativa → principios

### Verificable

Confirma la autenticidad de las conclusiones.

### Reproducible

Mismo resultado al replicar las pruebas.

### Repetible

Resultados coherentes con otros datos.

### Independiente

Conclusiones ajenas al individuo o método.

# Verificable

Que otra persona pueda comprobar que las evidencias y las conclusiones son correctas.

Lo que debe ser **verificable** es la evidencia y el proceso de obtención, no solo la conclusión del análisis.

**Ejemplo:**

- Haces una copia forense de un disco
- Calculas el hash SHA256
- Cualquiera puede comprobar que el hash coincide
- Eso permite verificar que no se ha modificado la evidencia.

# Reproducible

Si otra persona repite exactamente el mismo análisis con los mismos datos, obtiene el mismo resultado.

**Reproducible** se refiere principalmente al proceso de análisis de la evidencia, no tanto a su recolección.

**Ejemplo:**

- Analizas un log con una herramienta
- Detectas una IP atacante
- Si otro analista usa los mismos logs y el mismo procedimiento:
- Debe obtener la misma IP.

# Repetible

Definición: Significa que el método funciona también en otros casos similares.

**Repetible** se refiere principalmente al proceso de análisis de la evidencia, no tanto a su recolección.

**Ejemplo:** Un procedimiento para analizar logs de intrusión.

Si aplicas ese procedimiento a otro incidente diferente, debería seguir funcionando y dar resultados coherentes.

**Conclusión:** No depende de un caso concreto.

# Independiente

Definición: Significa que el resultado no depende de quién haga la investigación.

**Escenario de aplicación:**

- Lo haces tú.
- Lo hace otro analista.
- Lo hace un perito judicial.

**Conclusión:** Todos deberían llegar a las mismas conclusiones. Esto es fundamental si el caso llega a juicio.

# Documentada

La documentación es crucial para la cadena de custodia. Asegura la integridad y permite la admisibilidad judicial y auditoría externa.

# Rfc 3227

La guía RFC 3227 define una serie de pautas para la recopilación de evidencias, de modo que se garantice que la evidencia sea:

- **Admisible:** válida en un proceso legal.
- **Auténtica:** sin manipulación posible.
- **Completa:** debe ser una prueba completa no parcial.
- **Fiable:** no puede haber duda sobre el proceso de recolección de la prueba.
- **Creíble:** comprensible por el tribunal.

# RFC 3227

**De forma sintetizada, además de las consideraciones habituales de las metodologías, esta guía aconseja:**

- Acatar la política de seguridad de la organización y contar con el personal adecuado para la gestión de incidentes según lo estipulado en la ley.
- Conseguir una imagen lo más fiel posible del sistema.
- Mantener en la medida de lo posible un registro pormenorizado que contenga fechas y horas, preferiblemente generadas de forma automática.
- Examinar cómo está configurada la hora en el sistema, si es la hora local o la hora UTC (Universal Time Coordinated, hora universal coordinada), señalándolo en cada hora anotada. Se sugiere registrar las horas indicando su desfase con la hora UTC. Por ejemplo: en este instante son las 10:51:32 horas UTC+1.
- Prevenir las potenciales alteraciones sobre la evidencia.
- Confeccionar un inventario con todos los sistemas implicados en el incidente.
- Respetar el orden de volatilidad.
- Si es factible, los procedimientos deben ser automatizados por motivos de rapidez y exactitud.
- Efectuar copias a nivel de bits de los soportes del sistema.
- Eludir realizar análisis forenses en la evidencia original; se efectuarán sobre la copia de la evidencia a nivel de bits, para no modificar la original.

# RFC 3227

Dentro de estas sugerencias hay una que, en el supuesto de estar efectuando una pesquisa para responder a un incidente, sin propósito de presentarla ante un tribunal, no invariablemente debe acatarse. Es la que dice:

• Si se plantea la disyuntiva de optar entre recolectar la evidencia o examinarla, se dará preferencia al proceso de recopilación.

O sea, si el fin principal de la indagación es conseguir información para contener, atenuar o erradicar un incidente y así restaurar el sistema, y se descarta iniciar un procedimiento judicial, se escogerá primero por inspeccionar la evidencia, aun cuando haya el peligro de modificarla o eliminarla.