NORMAS ISO/IEC 27037

La actuación de campo de la recopilación de las evidencias es un actividad extremamente delicada y compleja. La valía legal y técnica de las evidencias en la mayoría de ocasiones depende del proceso realizado en la recopilación y preservación de las mismas.

La norma ISO/IEC 27037 "Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence" viene a renovar a las ya antiguas directrices RFC 3227 estando las recomendaciones de la ISO 27037 más dirigidas a dispositivos actuales y están más de acorde con el estado de la técnica actual.

Esta norma ISO 27037 está claramente orientada al procedimiento de la actuación pericial en el escenario de la recogida, identificación y secuestro de la evidencia digital, no entra en la fase de Análisis de la evidencia.

Las tipologías de dispositivos y entornos tratados en la norma son los siguientes:

- Equipos y medios de almacenamiento y dispositivos periféricos.
- Sistemas críticos (alta exigencia de disponibilidad).
- Ordenadores y dispositivos conectados en red.
- Dispositivos móviles.
- Sistema de circuito cerrado de televisión digital.

Los principios básicos en los que se basa la norma son:

Aplicación de Métodos
La evidencia digital debe ser adquirida del modo menos intrusivo posible tratando de preservar la originalidad de la prueba y en la medida de lo posible obteniendo copias de respaldo.

Proceso Auditable
Los procedimientos seguidos y la documentación generada deben haber sido validados y contrastados por las buenas prácticas profesionales. Se debe proporcionar trazas y evidencias de lo realizado y sus resultados.

Proceso Reproducible

Los métodos y procedimientos aplicados deben de ser reproducibles, verificables y argumentables al nivel de comprensión de los entendidos en la materia, quienes puedan dar validez y respaldo a las actuaciones realizadas.

Proceso Defendible

Las herramientas utilizadas deben de ser mencionadas y éstas deben de haber sido validadas y contrastadas en su uso para el fin en el cual se utilizan en la actuación.

Para cada tipología de dispositivo la norma divide la actuación o su tratamiento en tres procesos diferenciados como modelo genérico de tratamiento de las evidencias:

La identificación

Es el proceso de la identificación de la evidencia y consiste en localizar e identificar las potenciales informaciones o elementos de prueba en sus dos posibles estados, el físico y el lógico según sea el caso de cada evidencia.

La recolección y/o adquisición

Este proceso se define como la recolección de los dispositivos y la documentación (incautación y secuestro de los mismos) que puedan contener la evidencia que se desea recopilar o bien la adquisición y copia de la información existente en los dispositivos.

La conservación/preservación

La evidencia ha de ser preservada para garantizar su utilidad, es decir, su originalidad para que a posteriori pueda ser ésta admisible como elemento de prueba original e íntegra, por lo tanto, las acciones de este proceso están claramente dirigidas a conservar la Cadena de Custodia, la integridad y la originalidad de la prueba.

Reflexiones sobre la norma ISO/IEC 27037:2012. Directrices para la identificación, recolección, adquisición y preservación de la evidencia digital.

Introducción

En el desarrollo de un análisis forense digital tradicional con medios magnéticos y ópticos, generalmente los analistas forenses acuden a la buena práctica internacional para soportar los pasos que se adelantan con el fin de asegurar la evidencia digital identificada en los diferentes componentes informáticos y tecnológicos presentes en la escena del crimen.

Estas prácticas permiten establecer un conjunto base de validación para la contraparte y el juzgador, con el fin de probar la idoneidad del proceso ejecutado y la confiabilidad de los resultados, luego de las técnicas aplicadas para obtener la evidencia digital clave para efectos de soportar las afirmaciones o declaraciones sobre una temática particular que se tenga en una diligencia civil, penal o de cualquier índole.

Así las cosas, prácticas como la HB171-2003 *Guidelines for the Management of IT Evidence*, creada en Australia por la academia, industria, administración de justicia, gobierno y entes policiales, permite una vista homogénea frente al reto de la evidencia digital como elemento de prueba real con todos sus elementos, permitiendo una valoración y análisis que motive y concrete los juicios bien fundados sobre las evidencias que se aporten en el desarrollo de una diligencia probatoria.

De igual forma, las guías del NIST sobre estos temas particularmente en dispositivos móviles, web services, entre otros, así como las indicaciones del Departamento de Justicia de los Estados Unidos en los documentos como *Forensic Examination of Digital Evidence: A Guide for Law Enforcement, Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition*, son generalmente instrumentos utilizados por los analistas forenses digitales con el fin de establecer un marco de actuación formal y verificable que permita a los terceros validar las acciones que adelanten sobre la evidencia digital disponible en los medios informáticos.

En este sentido, el peritaje forense informático y tecnológico, siguiendo lo indicado por LOPEZ RIVERA (2012, pág.48) como la "obtención de información y evidencias de los bits que se encuentran en los dispositivos físicos de almacenamiento o virtuales en las redes que intervienen en la interacción de las personas con los sistemas", requiere un contexto general de actuación que permita a todos los involucrados contar con referentes verificables y de alcance global que exhiban formas de asegurar que los procedimientos aplicados en la pericia son confiables y con arreglo a ley.

Como quiera que a la fecha no se reconoce buena práctica de alcance global, se introduce en este documento la norma ISO/IEC 27037:2012 donde se establecen directrices para la identificación, recolección, adquisición y preservación de la evidencia digital, como un primer documento reconocido por la comunidad internacional y de alcance global para efectos de adelantar pericias forenses informáticas, el cual de ahora en adelante será un referente base para todos los informáticos forenses respecto de sus prácticas y

procedimientos actuales. La norma ISO/IEC 27037:2012 fue ratificada el 2016 y esta vigente a la fecha.

Principios que gobiernan la evidencia digital

De acuerdo con la ISO/IEC 27037:2012 la evidencia digital es gobernada por tres principios fundamentales: la relevancia, la confiabilidad y la suficiencia. Estos tres elementos definen la formalidad de cualquier investigación basada en evidencia digital, bien ésta sea utilizada para que sea admisible en corte o no.

La **relevancia** es una condición técnicamente jurídica, que habla sobre aquellos elementos que son pertinentes a la situación que se analiza o investiga, con el fin de probar o no una hipótesis que se ha planteado alrededor de los hechos. Todo aquello que no cumpla con este requisito será irrelevante y excluido del material probatorio recabado para efectos del caso bajo estudio.

La **confiabilidad** es otra característica fundamental, que busca validar la repetibilidad y auditabilidad de un proceso aplicado para obtener una evidencia digital, esto es, que la evidencia que se extrae u obtiene es lo que deber ser y que, si un tercero sigue el mismo proceso, deberá obtener resultados similares verificables y comprobables.

Finalmente y no menos importante la **suficiencia**, la cual está relacionada con completitud de pruebas informáticas, es decir que, con las evidencias recolectadas y analizadas tenemos elementos suficientes para sustentar los hallazgos y verificar las afirmaciones efectuadas sobre la situación investigada. Este elemento está sujeto a la experiencia y formalidad del perito informático en el desarrollo de sus procedimientos y priorización de esfuerzos.

Si bien puede haber otros elementos que ayuden en el gobierno de la evidencia digital, ISO ha determinado que estos tres, establecen las condiciones necesarias y suficientes para que los expertos en informática forense recaben, aseguren y preserven elementos materiales probatorios sobre medios digitales, los cuales podrán ser revisados y analizados por terceros interesados y sometidos a contradicción según ordenamiento jurídico donde se encuentren.

Habida cuenta de lo anterior, los informáticos forenses deberán prestar atención a estas indicaciones del estándar y recabar en el desarrollo de prácticas que permitan validar estos tres principios, que si bien se describen en el documento, no se concretan en acciones específicas que de alguna forma, sugieran una vía de aplicación que pueda validarse.

En este contexto, se detallan algunas preguntas (a manera de ejemplo) que pueden ser útiles para efectos de validar los tres principios enunciados:

Relevancia

· ¿La evidencia que se aporta vincula al sujeto con la escena del crimen y la víctima?
· ¿La evidencia prueba algunas hipótesis concreta que se tiene del caso en estudio?
· ¿La evidencia recolectada valida un indicio clave que permita esclarecer los hechos en estudio?

Confiabilidad

· ¿Los procedimientos efectuados sobre los dispositivos tecnológicos han sido previamente probados?
· ¿Se conoce la tasa de error de las herramientas forenses informáticas utilizadas?
· ¿Se han efectuado auditorias sobre la eficacia y eficiencia de los procedimientos y herramientas utilizadas para adelantar el análisis forense informático?

Suficiencia

· ¿Se ha priorizado toda la evidencia recolectada en el desarrollo del caso, basado en su apoyo a las situaciones que se deben probar?
· ¿Se han analizado todos los elementos informáticos identificados en la escena del crimen?
· ¿Se tiene certeza que no se ha eliminado o sobreescrito evidencia digital en los medios analizados?

Dos roles claves: *Digital Evidence First Responder* (DEFR) y el *Digital Evidence Specialist* (DES)

Por primera vez un estándar ISO establece definiciones de roles para efectos de las actividades requeridas en informática forense. Estos dos roles DEFR, cuya traducción podría ser “Primer respondiente de la evidencia digital” y el DES, como “Especialista en evidencia digital”.

El primero es aquella persona que está autorizada, formada y habilitada para actuar en la escena de un incidente, y así recoger y adquirir las evidencias digitales con las debidas garantías. Este es un rol que deben tener todas las organizaciones, toda vez que cualquier persona en una empresa puede actuar como primer respondiente frente a un incidente donde la evidencia digital sea parte de los elementos materiales probatorios.

Según la norma, esta persona y su formación dependerán del contexto de cada legislación y política organizacional, como quiera que, es en el contexto del ejercicio de primer respondiente que se establecen las condiciones y habilidades requeridas para asegurar de primera mano la evidencia digital propia de la situación en estudio.

¿Qué debe hacer un primer respondiente frente a un incidente informático? Si bien no detalla la norma la respuesta a esta pregunta, si podríamos indicar algunos elementos claves que se deben seguir frente a un proceso fundamental en el aseguramiento y custodia base de la evidencia informática, mientras el especialista en evidencia digital llega al sitio.

· Asegurar el área dónde ocurre el evento informático y los elementos materiales probatorios que se encuentren allí: notas, documentos, dispositivos electrónicos, entre otros.
· Evitar que personal extraño al área, tenga acceso a la misma y a los equipos que allí se encuentren.
· Tomar fotos o video de cómo encontró el área y documentar fecha, hora y condiciones en las cuales llega al sitio donde ocurren los hechos.

De otro lado, el Especialista en Evidencia Digital (EED) lo califica como aquella persona que puede hacer lo que hace el primer respondiente la evidencia digital y además cuenta con conocimientos, destrezas y entrenamiento especializado en un amplio rango de aspectos tecnológicos, lo que podríamos llamar un perito informático o en inglés un *computer expert witness*.

En este contexto, se presenta una primera insinuación sobre esta problemática del perito informático, que siguiendo los conceptos de LOPEZ RIVERA (2012, pág.21), debe estar asistida por tres elementos fundamentales:

· Ser un tercero neutral, alguien ajeno al proceso y a los intereses particulares que se encuentren en discusión.
· Ser un experto, una persona con formación formal, con experiencia fruto de sus desempeños laborales, conocimientos especializados, científicos o prácticos según el caso.
· Ser una persona que voluntariamente, acepte incorporar sus conocimientos al proceso.

Si bien el estudio de cómo se debe formar un perito informático, escapa al alcance de este documento, si es preciso anotar que a la fecha existen diversos programas formales de

formación de investigadores de crímenes de alta tecnología o en ciencias forenses informáticas que dan respuesta desde diferentes perspectivas a la formación de estos especialistas y auxiliares de la justicia, para que se tenga una vista medianamente clara y detallada de las habilidades y conocimientos que se deben tener frente al aseguramiento de la evidencia digital. (CANO 2009)

Finalmente y no menos importante, la norma hace énfasis en los siguientes puntos, que se deben observar todo el tiempo tanto por el DEFR como por el DES:

· Minimizar el manejo del dispositivo con la evidencia digital original o con la evidencia digital potencial
· Dar cuenta de cualquier cambio y documentar las acciones que se tomen (mientras el experto se hace una opinión sobre su confiabilidad)
· Cumplir con las leyes locales sobre el manejo de la evidencia
· No tomar acciones más allá de sus competencias.

Tipologías de dispositivos y entornos alcance de la norma
De acuerdo con la norma es alcance de la misma: (LOPEZ RIVERA 2012, pág.200)

· Equipos y medios de almacenamiento y dispositivos periféricos
· Sistemas críticos (alta exigencia de disponibilidad)
· Computadores y dispositivos conectados a la red
· Dispositivos móviles
· Sistemas de circuitos cerrados de televisión digital

Con este alcance, quedan fuera tecnologías recientes como las unidades de estado sólido, los sistemas de control industrial (por sus configuraciones y tecnologías especiales basadas en microcontroladores), servicios web, entre otros temas especializados, que si bien pueden utilizar los pasos naturales del proceso asociado con la informática forense (documentos y alcance de la norma identificación, recolección y/o adquisición, conservación y/o preservación), requiere una vista particular de aseguramiento que es propia e inherente a los avances tecnológicos previamente enunciados.

Si bien estas tipologías tratan de ser generales y genéricas frente a lo que se puede encontrar en una escena con dispositivos tecnológicos, es importante anotar que cada tecnología requiere un margen de especialidad que escapa al proceso general planteado y sus actividades previstas, toda vez que los cambios técnicos que se tienen, requieren un entendimiento particular de cómo funcionan y cuáles son las implicaciones frente a las

exigencias del proceso forense en informática, basado en el método científico, no para conocer la verdad, sino para dar respuesta a preguntas que se plantean en el contexto del caso en estudio.

Un ejemplo de esta condición es la realización de la imagen idéntica, la cual es un procedimiento que se aplica con software especializado para asegurar que el contenido digital del dispositivo informático (particularmente magnético) es fiel copia del original, en el que se aplica un hash sobre la imagen resultado, el cual puede ser verificado posteriormente para validar su inalterabilidad.

Sin embargo, aplicar el mismo procedimiento sobre unidades de estado sólido no genera el mismo resultado, toda vez que esta unidad funciona de manera diferente al medio magnético, es decir de manera general, constantemente por efectos de la confiabilidad del medio, se está cambiando de posición la información allí residente (CANO 2013), con lo cual se puede aplicar un hash un momento T y éste no será igual al que se aplique en T+1.

Así las cosas, las tipologías son sensibles a los cambios tecnológicos y nuevos retos emergentes de la informática forense, lo que necesariamente advierte que las técnicas descritas en el estándar deberán ser revisadas y ajustadas en el tiempo de manera periódica, con el fin de advertir cambios y ajustes que permitan mantener la confiabilidad de los procedimientos aplicados, como quiera que este documento es un referente de alcance global.

Reflexiones finales

El estándar ISO/IEC 27037:2012 es un avance relevante para el ejercicio de la práctica de la informática forense a nivel internacional que permite homogenizar una serie de prácticas claves para efectos de dar mayor confiabilidad a los resultados de los procesos aplicados, que previamente sólo estaban fundados en la buena práctica internacional o referentes particulares a instituciones o entidades reconocidas por sus logros en este campo.

Este documento cubre tres etapas de la actuación forense digital como son identificación, recolección y/o adquisición y conservación y/o preservación, detallando prácticas y consideraciones de actuación relevantes que responden a los mínimos que el “Especialista en Evidencia Digital” debe cubrir y asegurar para mantener la confiabilidad de sus resultados frente al tratamiento y aseguramiento de la evidencia digital.

Sin embargo, los temas relacionados con el análisis e interpretación de la evidencia digital no son cubiertos por esta norma y se espera que la anunciada ISO/IEC 27042, sugiera los

campos de acción en estos temas, los cuales tendrán retos importantes como se establece su reciente borrador:

"*El análisis e interpretación de la evidencia digital puede ser un proceso complejo. En algunas circunstancias, puede haber varios métodos que se pueden aplicar y los miembros de equipo de investigación tendrán que justificar la selección de determinado proceso y mostrar cómo es equivalente a otro utilizado por otros analistas. En otras circunstancias, los investigadores tendrán que idear nuevos métodos para el examen de la evidencia digital que previamente no ha sido tenido en cuenta y deben ser capaz de demostrar que el método de producción es "adecuado".*"

Así las cosas, contar con el estándar ISO/IEC 27037:2012 nos permite avanzar en la unificación de lenguajes y acciones propios de la práctica de la informática forense, que junto con iniciativas especializadas por tipo de dispositivos y tecnologías novedosas, permitan desarrollar una monitorización abierta y efectiva de la práctica de sus especialistas, incrementando los niveles de excelencia y madurez tanto de los profesionales en esta área como en el desarrollo de herramientas que soporten los más altos estándares de confiabilidad.

Referencias

ISO/IEC 27037:2012. Tecnología de la información – Técnicas de seguridad – Directrices para la identificación, recolección, adquisición y preservación de la evidencia digital.

ISO/IEC 27042 - Tecnología de la información – Técnicas de seguridad – Directrices para el análisis e interpretación de la evidencia digital. (En desarrollo)

HB171-2003 Guidelines for the Management of IT Evidence. Australia Standard.

LOPEZ RIVERA, R. (2012) *Peritaje informático y tecnológico. Un enfoque teórico-práctico*. ISBN 978-84-6160-895-9.

NIST (2007) Guidelines on cell phone forensics. Disponible en: http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf (Consultado: 15-09-2013)

NIST (2010) Forensics web services. Disponible en: http://csrc.nist.gov/publications/nistir/ir7559/nistir-7559_forensics-web-services.pdf (Consultado: 15-09-2013)

NIJ (2004) Forensic Examination of Digital Evidence: A Guide for Law Enforcement. Disponible en: https://www.ncjrs.gov/pdffiles1/nij/199408.pdf (Consultado: 15-09-2013)

NIJ (2008) Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition. Disponible en: http://www.ncjrs.gov/pdffiles1/nij/219941.pdf (Consultado: 15-09-2013)
CANO, J. (2009) *Computación forense. Descubriendo los rastros informáticos*. Ed. Alfaomega. México.
CANO, J. (2013) Unidades de estado sólido. El reto de la computación forense en el mundo de los semiconductores. *Blog IT-Insecurity*. Disponible en: http://insecurityit.blogspot.com/2013/06/unidades-de-estado-solido-el-reto-de-la.html (Consultado: 15-09-2013)

RFC 3227

La RFC (*Request For Comments*) 3227 es un documento que recoge las principales directrices para la recolección y el almacenamiento de evidencias digitales, constituyendo un verdadero estándar para la recopilación y almacenamiento de evidencias. La RFC 3227 define un proceso para la recolección de evidencias que ayuda al perito informático a adquirir y catalogar las evidencias digitales.

Así pues, el proceso definido incide en la adquisición de una *imagen* del sistema que debe adquirirse lo más fidedigna posible, realizando notas detalladas que incluyan fechas e indicando si se está utilizando la hora local o el horario UTC, minimizando los cambios en la información que se está recolectando (eliminando si es posibles los agentes externos que pudieran ejecutar dichos cambios), priorizando la recolección sobre el análisis, recogiendo la información por orden de volatilidad (es decir, recopilando primero la información de las memorias *cachés* y de la memoria principal -RAM- y, posteriormente, recolectando la información de la memoria secundaria -discos duros-, seguidamente de las memorias USB y, finalmente, de las unidades ópticas, *logs* de sistemas y documentos.

El perito informático, según este estándar, deberá intentar por todos los medios que se pierda la mínima información posible, tomando la mejor decisión con respecto a si se deben extraer las evidencias de los ordenadores encendidos que han sido intervenidos (siempre ante fedatario público o autoridad que levante acta del proceso), o desconectar la máquina de la red a fin de evitar que se active cualquier programa informático diseñado para eliminar la información de las unidades físicas conectadas al ordenador, bien a distancia (botón de pánico), bien de forma programada. Es necesario señalar que esta desconexión provocará la desmagnetización de las *cachés* y de la memoria principal, cuya información se perderá

irremediablemente, razón por la cual es necesario analizar y decidir in situ cuál es la mejor opción en función de lo que el perito informático perciba en los diferentes sistemas intervenidos.

Se deberán obviar también las informaciones proporcionadas por los programas del sistema, ya que éstos pueden haberse visto comprometidos. Tampoco deben ejecutarse programas que modifiquen los metadatos de los ficheros del sistema.

Asimismo, el perito informático deberá prestar especial atención a no vulnerar, bajo ningún concepto, la privacidad de las personas, cumpliendo en todo momento con la Constitución, que protege la privacidad del individuo en su artículo 18, así como con las leyes que desarrollan dicho artículo. Es necesario prestar también especial cuidado sobre la información comprometida de la organización, puesto que puede darse el caso que se hallen almacenadas fórmulas, planos, o cualquier otro tipo de activos sometidos a las leyes de la propiedad industrial.

Por tanto, la recolección de la evidencia debe seguir los principios de:

- Admisibilidad: la prueba debe ser admisible por un Tribunal de Justicia
- Autenticidad: debe ser posible vincular la prueba al incidente o delito
- Completitud: la prueba debe ser completa, no parcial
- Confiabilidad: no se debe poner en duda el proceso de recolección de la prueba, por lo que debe conservarse de forma absolutamente escrupulosa la cadena de custodia, al objeto de evitar que el Tribunal inadmita la prueba
- Credibilidad: la prueba debe ser fácilmente comprensible por el Tribunal que vaya a evaluarla

El estándar define igualmente un procedimiento de recolección de evidencias, que debería ser lo más detallado posible, inequívoco y reduciendo al mínimo la cantidad de toma de decisiones necesaria durante el proceso de recolección. Así pues, se define que el proceso debe ser transparente, de tal forma que todos los métodos utilizados para la recolección de la prueba deben ser reproducibles, lo que significa que el procedimiento debe ser *forense* (del latín *forensis*, "público y notorio"), así como el deber de la utilización de métodos estándares.

Se debe crear un listado con todos los sistemas involucrados en el incidente, al objeto de recoger posteriormente la prueba, estableciendo una relación de las evidencias que es más

probable que sean admitidas, pecando por exceso, en lugar de por defecto, si fuese necesario, en la toma de precauciones para la recolección de la evidencia.

Para cada sistema informático, se debe obtener el correspondiente orden de volatilidad en cada una de sus memorias, desconectando cada sistema del exterior para evitar alteraciones en las evidencias, reuniendo posteriormente las evidencias con las herramientas forenses necesarias. Es necesario, asimismo, registrar el grado de sincronización del reloj del sistema y, a la vez que se van recolectando evidencias, indagar en la posibilidad de qué otros elementos pueden llegar a considerarse evidencias. Además, es necesario documentar cada paso y recoger en un documento las personas involucradas en el procedimiento, tomando nota de quién estaba allí y de qué estaba haciendo cada uno, así como de sus observaciones y reacciones. Finalmente, es necesario calcular los resúmenes o códigos *hash* para cada una de las evidencias, sin alterar éstas, al objeto de iniciar un procedimiento de cadena de custodia de las pruebas.

Por otra parte, el procedimiento de archivo de las evidencias define cómo deben almacenarse las pruebas. La evidencia debe estar claramente protegida y, además, debidamente documentada. Así pues, el perito informático necesitará, muy probablemente, la ayuda de un fedatario público (en España, un notario o un secretario judicial), que otorguen fe pública al acto de generación de la cadena de custodia mediante el cálculo del código *hash* correspondiente a la prueba. Además, se debe generar documentación conducente a la descripción clara de cómo se encontró la evidencia, cómo se manipuló y quién tiene bajo la custodia de quién está la evidencia en cada momento, detallando los cambios que se produzcan en la custodia de ésta.

El acceso a las evidencias almacenadas deberá ser limitado y deberán documentarse también las personas que tendrán permiso para acceder a las mismas, así como los cambios de custodia que se produzcan en las pruebas. Sería conveniente, asimismo, implementar un mecanismo que detecte accesos no autorizados a las pruebas.

Todos los programas que el perito informático necesite para realizar el análisis forense de las pruebas, deberá ser preparado con anterioridad en medios ópticos de “sólo lectura”, como CDs o DVDs, debiendo incluir, al menos, un programa de cada una de las siguientes tipologías:

- Un programa para el examen de los procesos
- Un programa para examinar el estado del sistema
- Un programa para realizar copias bit a bit

- Un programa para calcular sumas de verificación o códigos *hash*
- Un programa para la generación de imágenes básicas y para analizar éstas
- Una secuencia de comandos para automatizar la recopilación de pruebas.

Además, se deberá estar preparado para garantizar la autenticidad y fiabilidad de las herramientas que se utilicen.