Una propuesta de mapeo entre puntos de pericia y preguntas de competencia derivadas de un modelo ontológico

Mirta del Carmen Peñalva
Universidad Tecnológica Nacional - Facultad Regional La Plata.
GIDAS - Grupo de Investigación & Desarrollo Aplicado a Sistemas informáticos y computacionales
penalvam@frlp.utn.edu.ar

Resumen

Actualmente la Forensia Digital se encuentra en un proceso de desarrollo y expansión apoyándose en las TCIs. En ella se integran espacios disciplinares muy diversos con lógicas y dinámicas particulares. En este artículo se propone contribuir al encuentro entre el lenguaje técnico jurídico y el ingenieril que se produce cuando Jueces y/o abogados expresan los requerimientos a los peritos. Las actividades realizadas se enfocaron en pericias digitales de correos electrónicos bajo el marco de la ontología OntoFoCE, que especifica a estos últimos y responde a un conjunto de preguntas de competencia. El trabajo incluyó el análisis de una muestra de puntos de pericia reales, a partir de los cuales se identificó el concepto de pieza de requerimiento. Se distinguieron dos hipótesis: la primera, se centró en la posibilidad de extender el proceso de concepción de la ontología mencionada para ser aplicado a otros objetos de estudio. La segunda, planteó la elaboración de un mapeo entre piezas de requerimiento y preguntas de competencia. Dicho instrumento dará soporte al perito informático en su labor como auxiliar de la Justicia, contribuyendo a su objetivo esencial de brindar información sustentada en evidencia científica.

1. Introducción

En el actual contexto de globalización e hiper-conectividad, el ciberespacio es la plataforma de ejecución de *casi* todas las actividades humanas. Con la irrupción de la pandemia del COVID-19 se aceleró la virtualización del trabajo, el estudio y demás servicios mudándolos fuera de las seguridades provistas por los contextos organizacionales. La metáfora "La tierra es plana" acuñada por Friedman T. [10], se encarna en un conjunto de fenómenos cuya difusión es inmediata y su alcance no reconoce fronteras. Este cúmulo de interacción humana se convierte en un campo propicio para la concreción de ciberdelitos, los cuales crecen en número [9] y en diversidad [1], citamos a modo de ejemplo, la duplicación de casos en España entre 2011 y 2018.

Para poder estudiarlos y esclarecerlos, la Forensia Digital cobra impulso apoyándose en recursos metodológicos provenientes de la Seguridad Informática y los integra al campo de la Criminalística. Se jerarquiza de esta manera, su objetivo primigenio de validar evidencia digital admisible y científicamente irrefutable, que sirva de soporte a la Justicia en su responsabilidad de conocer la verdad en ocurrencias de delitos informáticos.

En este trabajo se presenta una propuesta para acercar la expresión de los requerimientos a peritar desde el lenguaje técnico jurídico hacia el lenguaje técnico ingenieril. Se tomó como base una investigación enfocada en la aplicación de ontologías a la Forensia Digital para el caso de correos electrónicos. La misma contribuyó el modelo ontológico OntoFoCE y la herramienta de software ObE Forensic [15] que utilizados en el análisis forense, aseguran producir evidencia digital no repudiable. Este artículo está integrado en secciones, la sección 1 presenta el estado actual de los ciberdelitos, el desarrollo de la Forensia Digital como instrumento para develarlos y aspectos que motivan el presente trabajo, la sección 2 describe el marco teórico-conceptual de referencia, la sección 3 explica el trabajo propuesto y llevado a cabo y en la sección 4 se exponen las conclusiones.

2. Marco Teórico

La Forensia Digital se define como el *uso de métodos científicamente probados y derivados hacia la preservación, recolección, validación, identificación, análisis, interpretación, documentación y presentación de evidencia digital proveniente de fuentes digitales con el propósito de facilitar o promover la reconstrucción de eventos, que se consideran criminales, o ayudando a anticipar acciones no autorizadas que pueden ser perjudiciales para las operaciones planeadas.* [14]

Por otra parte, una definición de *delito informático* lo considera como *aquel que se da con la ayuda de la*

informática o de técnicas anexas [2], a lo que podemos adicionar el uso de hardware y/o software como medio o fin.

Gradualmente, la legislación argentina ha ido elaborando un conjunto de leyes referidas a estos delitos además de adherir en 2017 al Convenio sobre Ciberdelincuencia de Budapest [5], que promueve un marco común de tratamiento de estos delitos en las diferentes naciones.

La labor investigativa del perito informático se desarrolla desde que una huella es identificada, para luego ser considerada como indicio, posteriormente como evidencia y finalmente convertirse en prueba digital. Cabe aclarar estas consideraciones referidas a la consolidación de la fuerza probatoria, son responsabilidad de la autoridad del proceso judicial. Los procedimientos y actividades de investigación que realiza el perito informático conforman un proceso vivo y en constante mejora. En este sentido, se requiere ajustar su nivel de formalización, como así también asegurar una realización rigurosa, bajo un marco metodológico fundamentado científicamente, tal lo definido en el Art. 477 del Código Procesal Civil y Comercial de la Nación Argentina que especifica que la fuerza probatoria del dictamen pericial se sustenta en *"... los principios científicos o técnicas en que (se) funda, en concordancia de su aplicación con las reglas de la sana crítica..."*.

La formación ética y disciplinar continua del perito informático asegura procesos de mayor calidad, al mismo tiempo su involucramiento en actividades de I+d aportan innovaciones relacionadas a metodologías, técnicas, métodos y herramientas. La aplicación adecuada de estos recursos producirá información precisa dotando de solidez a las decisiones de la Justicia por estar fundamentadas en evidencia científica. De esta manera, se evita que las pruebas liberen o condenen a los imputados debido a inconductas o imparcialidades de los actores del sistema judicial.

El proceso que lleva adelante un perito informático contempla las siguientes actividades: preservación, recolección, validación, identificación, análisis, interpretación, documentación y presentación de evidencia digital. Su instanciación debe realizarse con el soporte de estructuras estandarizadas, reconocidas en el ámbito científico, reglamentadas, que aseguren su repetición e inalterabilidad del soporte físico y el material digital para que el proceso y por ende la prueba, sean incuestionables. En este sentido, existen modelos de referencia para la ejecución de las mencionadas actividades como la familia de normas ISO/IEC 27k [11] o el Proceso Unificado de Recuperación de Información (PURI) desarrollado por investigadores de la Universidad FASTA [8]. Debemos resaltar que durante el desarrollo de cada una de las actividades periciales se debe velar por el aseguramiento de la cadena de custodia del material a peritar, como por ejemplo la encriptación del material al momento de la recolección o la copia bit a bit que permita detectar posibles alteraciones.

Es fundamental el encuentro e integración del Servicio de Justicia y la Ingeniería Forense, inicialmente a través de un lenguaje común, para ir acercándose a un marco conceptual robusto, como por ejemplo una ontología que brinde uniformidad y consistencia de términos, conceptos y sus relaciones, involucrados en este dominio en particular.

Desde este punto de vista una ontología se define como *"la descripción conceptual y terminológica de un conocimiento compartido acerca de un dominio específico. Dejando de lado la formalización e interoperabilidad de aplicaciones, esto no es más que la principal competencia del término: hacer mejoras en la comunicación utilizando un mismo sistema en lo terminológico y conceptual"* [6].

Son varias las experiencias que aplican ontologías al dominio de la Justicia. A modo de ejemplo se puede citar una experiencia de aplicación de la plataforma METHONTOLOGY en el ámbito legal español [4] y otra de aplicación de ontologías para optimizar la recuperación de documentación legal [7].

3. Propuesta

Emplazados en la temática ya introducida, se presenta el siguiente trabajo de análisis, discusión y elaboración de propuestas referidas a la estructuración de los contenidos expresados en los puntos de pericia, que son solicitados a los peritos informáticos tanto en las designaciones para actuar como auxiliar de la Justicia como así también en investigaciones privadas o de partes.

El perito recibe una propuesta de designación para una actividad forense conjuntamente con la solicitud expresa del alcance de su actividad, estos son los puntos de pericia.

Para (Cafferata Nores & García, 2003) la pericia es un medio probatorio con el cual se intenta obtener, para el proceso, un dictamen fundado en especiales conocimientos científicos, técnicos o artísticos, útiles para el descubrimiento o la valoración de un elemento de prueba. Su regulación se encuentra definida de manera general en los códigos procesales de forma meramente enunciativa [3].

De una pericia interesa particularmente el objeto de la pericia o los puntos de pericia. Si bien no existe una definición doctrinaria del término, es posible explicarlo según sus características:

- Mediante ellos el Juez o solicitante define el alcance de la actividad pericial
- Son aquellos rubros que se solicita se determinen o aclaren a fin de ofrecer debidamente la prueba, que contribuye a abundar el conocimiento y criterio del Juez al momento de dictar sentencia sobre el caso sometido a su decisión.

- Conforman el grupo de preguntas iniciales o incógnitas legales que debe responder el perito al momento de realizar la actividad pericial.

- Estos elementos usualmente se expresan en términos de acción *"verificar… constatar… informar… explicar…"*, en la cual el perito recurre al conocimiento científico de su área, para responder a la solicitud del Juez, atendiendo a las normas y buenas prácticas de cada disciplina.

- Son consignas totalmente restrictivas de la actuación pericial, y marca el espacio dentro del cual el perito debe realizar su tarea.

Para poder responder de forma consistente, los peritos deben comprender lo que se les solicita, sin ambigüedad en: tareas, precisión, granularidad y alcance, entre otras. Una dificultad que se presenta en los puntos de pericia es que son escritos por Jueces o abogados, quienes en muchos casos, no tienen competencias de saberes sobre tecnologías. Cuando esta situación no les permite formularlos adecuadamente se requieren instancias para aclarar, detallar y redactar el contenido con el perito.

En este sentido, y tomando como ejemplo un caso de objeto de estudio, se hace referencia a la Tesis Doctoral *"Una Ontología del Correo Electrónico y su Trazabilidad como Soporte para la Forensia Digital"* [15]. En ella se propone un modelo ontológico específico que representa el proceso de transmisión del correo electrónico permitiendo derivar su trazabilidad, respondiendo a preguntas de competencia relativas a los puntos de pericia más habituales cuando se trata de correos electrónicos. Esta ontología permite comprobar la autenticidad del correo electrónico como prueba digital lo que la convierte en no repudiable.

Se recopilaron 86 ejemplos de puntos de pericia referidos al objeto de estudio *"correo electrónico"* correspondientes al período 2001-2017 y en su mayoría pertenecientes al foro laboral. Los mismos fueron provistos por peritos informáticos, que cumplieron el rol de validar la ontología por considerarse "usuarios expertos". Los textos se informaron sin mención alguna que pudiera identificar causa, personas, empresas, organizaciones o juzgados intervinientes en la acción judicial. Tras la lectura de los mismos se advirtió: uso de lenguaje libre, escasa reutilización de texto, ausencia de plantillas aplicadas en su formulación. Consecuentemente, pudieron adolecer de imprecisión, ambigüedad, vaguedad, alcance indefinido del pedido, utilización incorrecta de términos técnicos, lo que puede generar confusión o cambio del sentido del objetivo, omisiones, etc. Pero también se encontraron similitudes, que lograron sintetizarse en 46 puntos de pericias representativos de la muestra. En base a ellas se especificó una lista de 21 preguntas de competencia, que con una estructura, terminología y sintaxis definidas, constituyen un set de preguntas regulares que responden las solicitudes formuladas por los puntos de pericia.

La Figura 1 muestra la ontología definida sobre el objeto de estudio "correo electrónico". Esta especificación semántica y exhaustiva de las características del objeto y sus relaciones, representa el dominio sobre el cual se pueden inferir las preguntas que se puedan requerir. Sobre esta ontología se desarrolló la aplicación web ObE Forensic, que a través de un lenguaje específico, automatiza la obtención de respuestas, brindando precisión, (ya que dado un conjunto de datos, la respuesta a una pregunta es única) y ahorros de procesamiento.

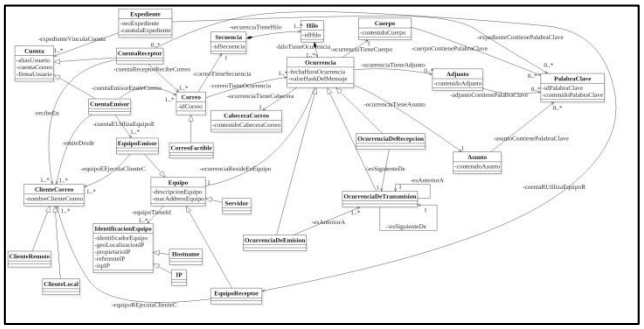

Figura 1. Modelo Conceptual de OntoFoCE

Una idea emergente del modelo ontológico de *"correo electrónico"*, es la posibilidad extenderlo a otros objetos como se describe en la Figura 2. Dado un objeto de estudio, se lo puede conocer utilizando diversas técnicas de elicitación discutidas en [13] y [16] y aplicadas en Ingeniería de Requerimientos. El proceso de elicitación de requerimientos se compone de los siguientes subprocesos secuenciales: obtención del conocimiento del dominio o problema, análisis, especificación y validación por parte de expertos de dicho dominio. A través de la aplicación de la técnica "lectura en perspectiva" sobre un conjunto de causas, se extraen puntos de pericia habituales relacionados al objeto de estudio. Se analizan, clasifican y con dicho cuerpo del conocimiento se modela una versión de ontología que representará las características del objeto de estudio y sus relaciones con otras entidades del dominio. Luego, podrá conocerse el universo de preguntas que responderá el modelo, formuladas en base a los atributos de las clases definidas.

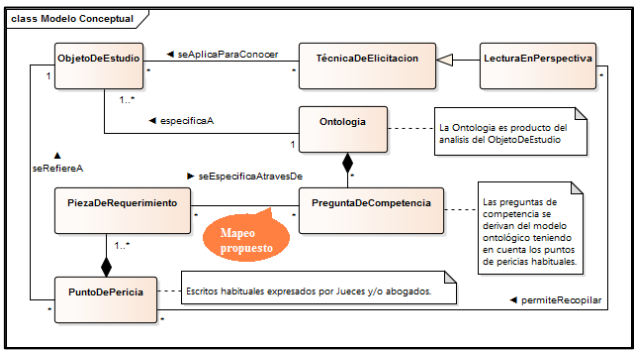

Figura 2. Modelo Conceptual para vincular PiezaDeRequerimiento con PreguntaDeCompetencia.

Las preguntas de competencia que actualmente responde OntoFOCE se detallan a continuación en Tabla 1. La definición de un set de preguntas específicas y validadas permitirá a los Jueces y abogados, disponer de un repositorio para escribir los requerimientos periciales sin ambigüedad, estableciendo el alcance necesario y suficiente, usando terminología técnicamente correcta, que le asegure una solicitud de puntos de pericia eficaces que no tengan que ser sometidos a ciclos de explicación y reescritura.

Tabla 1. Preguntas de Competencia derivadas de OntoFoCE

PC01: Dado un correo CE ¿Cuál es la fecha, hora y dirección IP de emisión del correo electrónico?
PC02: Dado un correo CE ¿Cuál es la fecha, hora y dirección IP de recepción del correo electrónico?
PC03: Dado un correo CE ¿A qué cuentas se remitió el correo?
PC04: Dado un correo CE ¿Cuál es el alias de usuario y dirección de e-mail del emisor?
PC05: Dado un correo CE ¿Cuál es el alias de usuario y dirección de e-mail del Receptor?
PC06: Dado un correo CE ¿Cuál fue el cliente de correo utilizado por cada usuario?
PC07: Dado un correo CE ¿Cuál fue el equipo desde el cual se emitió el correo?
PC08: Dado un correo CE ¿Cuál fue el equipo en el que se recibió el correo?
PC09: Dado un correo, un emisor y un receptor ¿cuál es la secuencia de equipos por los que pasó ese correo?
PC10: Dado una cuenta C ¿cuáles son los correos que emitió?
PC11: Dado una cuenta C ¿cuáles son los correos que recibió?
PC12: Dado una cuenta C1 ¿se ha emitido un correo hacia la cuenta C2?
PC13: Dado una cuenta C1 ¿se ha recibido un correo desde la cuenta C2?
PC14: Dada una dirección IP ¿cuál sería la localización geográfica del mismo?
PC15: ¿Cuáles son los correos que han pasado por el dispositivo que posee una IP dada?
PC16: ¿Cuáles son los mails enviados desde una determinada cuenta en una fecha dada?
PC17: ¿Cuáles son los mails recibidos por una determinada cuenta en una fecha dada?
PC18: Dada una palabra clave ¿Figura en el asunto de un correo?
PC19: Dada una palabra clave ¿Figura en el cuerpo de un correo?
PC20: Dada una palabra clave ¿Figura en el adjunto de un correo?
PC21: ¿Cuáles son los correos intercambiados entre las cuentas C1 y C2 en un rango de fechas dado?

A modo de ejemplo, se muestran en la Tabla 2, un extracto de los 46 puntos de pericia referidos previamente:

Tabla 2. Extracto de puntos de pericia habituales

Tabla II-2: Puntos de Pericia Resultantes

N°	PUNTO DE PERICIA
1)	¿Quién es el titular de la casilla salta@yahoo.com.ar? , ¿Cuándo se habilitó la misma?, si en el período de la causa fue el sistema de contacto del actor con la demandada o sus casillas de email; persona1@dominio.com.ar, usuario@yahoo.com.ar, persona2@dominio.com.ar, persona3@dominio.com.ar y persona4@dominio.com.ar e imprimir ó transcribir los mails recepcionados y emitidos desde esa bandeja de servicios entre esos sujetos y fecha.
2)	Acceder al equipo y extraer toda información de la que pudieran surgir los correos electrónicos en los que la casilla "xxxxxxx@xxxx.com.ar" figure como remitente o destinatario.
3)	Agregue al informe los correos electrónicos enviados y recibidos desde esas cuentas entre su creación y MES de AÑO inclusive.

En dicha tabla se observa, remarcado en color, el punto 2) al cual se le aplicaron las siguientes preguntas de competencia:

Dado un correo CE

PC01:¿Cuál es la fecha, hora y dirección IP de emisión del correo electrónico?

PC02:¿Cuál es la fecha, hora y dirección IP de recepción del correo electrónico?

PC04:¿Cuál es el alias de usuario y dirección de e-mail del emisor?

PC05:¿Cuál es el alias de usuario y dirección de e-mail del Receptor?

PC07:¿Cuál fue el equipo desde el cual se emitió el correo?

PC08:¿Cuál fue el equipo en el que se recibió el correo?

Por ejemplo, para poder responder la pregunta de competencia *PC01:¿Cuál es la fecha, hora y dirección IP de emisión del correo electrónico?* Se interroga al modelo de la Figura 1 vinculando las clases: Correo, CuentaEmisor, EquipoEmisor, Equipo, IdentificacionEquipo hasta obtener el contenido de los atributos deseados. En la Figura 3 se detalla la consulta SPARQL que permite responder la pregunta de competencia PC01.

```
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX oc: <http://www.semanticweb.org/beatr/ontologies/2018/0/ontologia_correos#>
SELECT DISTINCT ?fechaEmision ?direccionIP
WHERE { ?correo oc:correoTieneSecuencia ?s.
        ?s oc:secuenciaTieneHilo ?h.
        ?h oc:hiloTieneOcurrencia ?o.
        ?o rdf:type oc:OcurrenciaDeEmision.
        ?o oc:fechaHoraOcurrencia ?fechaEmision.
        ?o oc:ocurrenciaResideEnEquipo ?q.
        ?q oc:equipoTieneId?ip.
        ?ip oc:identificadorEquipo ?direccionIP.
```

Figura 3. Consulta SPARQL correspondiente a la pregunta de competencia PC01

La aplicación web ObE Forensic responde siempre las preguntas sobre los datos ingresados. Luego el perito debe seleccionar las respuestas que aplican al requerimiento para armar el informe final. A este respecto, si previamente se procesara el punto de pericia y lograra algún nivel de interpretación al vincularlo con preguntas de competencia correspondientes, podría facilitar la labor del perito enfocándolo en las preguntas específicas. De esta manera, surge la idea de una interfaz de mapeo sugerida como vinculante tal se visualiza en la Figura 2.

De la lectura en perspectiva de la muestra de 86 puntos de pericia disponible en [15], se observó que un punto de pericia podía contener uno o varios requerimientos, por lo cual se procedió a identificar estos casos y disponerlos como unidades independientes a las cuales se denominó *pieza de requerimiento*.

Dicha información se migró a una base de datos en SQL Server para facilitar su procesamiento y se aplicó una metodología semi-estructurada ad-hoc.

Tomando como base los conceptos vertidos en [12] referidos a cómo expresar competencias y/o resultados de aprendizaje en el Modelo de Formación por Competencias y Aprendizaje Centrado en el Estudiante, se definió una estructura gramatical para expresar todos los requerimientos contenidos en los puntos de pericia:

Verbo en infinitivo + ***objeto*** + *condición*

El *verbo*, acción concreta y observable, que sintetiza la finalidad del punto de pericia, el *objeto* **es primordial**, es sobre lo que recae la acción del verbo, es lo que deberá informar el perito y la *condición* representa referencias de contexto, criterios de ejecución, puede contener filtros, restricciones, limitaciones del alcance o formatos específicos de presentación, como por ejemplo: "texto" contenido en un asunto de un correo, período en el cual se

haya enviado una pieza de correo, pertenencia a una cuenta de origen o destino (o varios), etc.

Se realizó un estudio sintáctico, semántico y morfológico del conjunto de requerimientos contenidos en puntos de pericias, se eliminaron expresiones tales como:

- *"Todo **otro dato de interés** para un total esclarecimiento de los hechos"*
- *"...verosimilitud de las **personas**..."* (la información siempre se refiere a una cuenta de correo que tiene un titular, no se puede informar nada acerca de la/s persona/s que gestiona/n dicha cuenta)
- *"...Indique si era **habitual** y **frecuente** la comunicación entre..."*
- *"Informe si resulta **habitual** la comunicación..."*
- *"... Manifieste **si puede** precisar..."* (se está consultando sobre las competencias del perito)
- *"Proceda al copiado digital de los correos **que contengan la información vinculada a la causa**..."*
- *"...puerto de entrada y salida y **todo otro dato de interés**."*
- *"...remitidos entre **PADRE e HIJO**..."*

No es función del perito indicar qué datos se debe informar, aunque puede brindar asesoramiento en la reformulación del texto.

Se excluyeron los casos sin enunciación apropiada. Del conjunto restante se listaron los objetos correspondientes a los requerimientos de puntos de pericia. Seguidamente, con la lista de verbos se realizaron agrupamientos por similitud y sinonimia (ejemplo: *informar y agregar al informe*). Se eliminaron verbos improcedentes por su amplitud o imprecisión, como: "*practicar*", "*analizar*", "*imprimir*" requiere disponer de hardware e insumos, "*transcribir*" implica actividad manual, inviable si se tratase de grandes volúmenes de datos y expuesta a riesgos de introducir errores involuntarios. Se computó la frecuencia de verbos, la misma se describe en Tabla 3.

Tabla 3. Frecuencia de uso de verbos

Verbo del requerimiento	Ocurrencias	% Participación	% Participación acumulada
determinar	24	30%	30%
indicar	13	16%	47%
informar/agregar al informe	12	15%	62%
constatar	5	6%	68%
identificar	5	6%	75%
extraer/copiar	4	5%	80%
comprobar	3	4%	84%
dictaminar	3	4%	87%
verificar	3	4%	91%
certificar	2	3%	**94%**
detallar	1	1%	95%
detectar	1	1%	96%
precisar	1	1%	97%
recabar	1	1%	99%
señalar	1	1%	100%

Se observa que los diez primeros verbos (frecuencia >1), acumulan el 94% de los casos, lo que indicaría que esta lista de verbos podría cubrir el alcance de la actividad inherente a las pericias sobre correos electrónicos, aunque como se dijo anteriormente el verbo que los engloba a todos ellos es *informar*.

En referencia a la lista de objetos se procedió a clasificar los tipos de requerimientos en cuatro categorías:

1) Consistencia: refiere a verificación, constatación, posibles adulteraciones.

2) Existencia: refiere a certificación de existencia o no de alguna condición.

3) Contenido parcial: refiere a consulta de contenido de algún atributo del objeto.

4) Contenido total: refiere a consulta de todos los atributos de un objeto.

Como resultante del análisis, se arribó al modelo que expresa los metadatos de una pieza de requerimiento y sus relaciones, el mismo se presenta en la Figura 4.

Una pieza de requerimiento tiene como objeto una cuenta de correo, un correo electrónico o a una dirección física. Además especifica si el requerimiento trata datos sobre emisión, recepción, ambas o incluso la trazabilidad de las ocurrencias de transmisión. Puede definir un filtro temporal, una cadena de caracteres a buscar en el asunto o adjunto o cuerpo del mail y puede hacer referencia a otras cuentas de correo vinculadas.

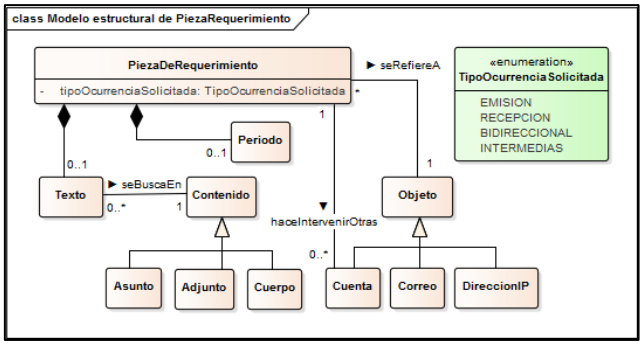

Figura 4. Modelo estructural (metadatos) de una pieza de requerimiento

Se identificaron las palabras clave para describir los contenidos a instanciar, correspondientes a cada una de las piezas de acuerdo al modelo ilustrado en Figura 4. Este conjunto preliminar de términos se expone en la Tabla 4. A posteriori se debieron someter a comprobación de consistencia por parte del experto.

Tabla 4. Palabras clave de rastreo de metadatos de una pieza de requerimiento

Elemento	Palabras clave
1.Objeto	
Cuenta	cuenta/casilla/dirección de mail/dirección de correo/usuario/dominio/@
Correo	correo/mail/email/e-mail/correo electrónico/mensaje
DireccionIP	dirección ip/ip/dirección física/dispositivo/móvil/pc/computadora/equipo
2.Emisión	emisión/emitido/emisor/enviado/envío/envían/remitido/remite/origen/salida/intercambio/intercambiado/comunicación entre
3.Recepción	recepción/recibido/receptor/destinado/destinatario/entrada/intercambio/intercambiado/comunicación entre/ remitido/remite
4.Trazabilidad	trazabilidad/rastreo/intermedio/servidores/enlace/transmisión
5.Desde	fecha/desde/período/entre/intervalo/tiempo/día/durante
6.Hasta	fecha/hasta/período/entre/intervalo/tiempo/día/durante
7.Texto de búsqueda	texto/contiene/contenga/conteniendo/contenido/" "/texto adjunto
8.Asunto	asunto/
9.Cuerpo	contenido/
10.Adjunto	adjunto/archivo/
11.Menciona otras cuentas	entre casilla/entre cuenta/intercambio/comunicación/@

Conjuntamente se elaboró una propuesta de mapeo (Tabla 5) con posibles respuestas ante la presencia concreta de los metadatos/elementos que pueden encontrarse en una pieza de requerimiento.

Tabla 5. Mapeo entre PiezaDeRequerimiento y PreguntaDeCompetencia

Objeto	*Tipo Ocurrencia Solicitada*			*Período*		*Búsqueda en Contenido*				*Menciona otras cuentas*	*Aplicar Pregunta de Competencia*
	Emisión	*Recepción*	*Intermedias*	*Desde*	*Hasta*	*Texto de búsqueda*	*Asunto*	*Cuerpo*	*Adjunto*		
Cuenta	X									X	**PC12**
		X								X	**PC13**
	X										**PC10**
		X									**PC11**
	X	X		X	X					X	**PC21**
	X			X	X						**PC16**
		X		X	X						**PC17**
Correo	X										**PC01,04,06,07**
		X									**PC02,05,06,08**
	X									X	**PC03**
	X	X	X								**PC09**
						X	X				**PC18**
						X		X			**PC19**
						X			X		**PC20**
DireccionIP											**PC14**
	X	X	X								**PC15**

A modo ilustrativo se interpreta la primera fila de esta tabla. Partiendo de una cuenta definida, si lo que se desea solicitar es lo que se emitió desde ella, y si se menciona una segunda cuenta indicando que se filtre además a ésta como cuenta destino, entonces se puede responder con la pregunta de competencia *PC12: Dado una cuenta C1 ¿se ha emitido un correo hacia la cuenta C2?*

4. Conclusiones

Partiendo del abordaje teórico de la Criminalística mediada por las TICs, se realizó una revisión de aspectos y conceptos dominantes en el campo de la Forensia Digital, para finalmente focalizarse en la lectura e interpretación de la ontología del objeto de estudio "*correo electrónico*" denominada OntoFoCE, que expresa una semántica a través de la exhaustiva especificación de las características del objeto y relaciones. Como resultado del mismo se identificaron dos hipótesis. La primera se centra en la posibilidad de reutilización o extensión del proceso llevado a cabo para la concepción de OntoFoCE, para aplicarlo a otros objetos de estudio como por ejemplo mensajería instantánea y lograr modelos ontológicos propios. En este sentido, se presentó un modelo preliminar que podrá ser punto de partida de futuras iniciativas de investigación. La segunda, se refiere al mapeo entre punto de pericia y preguntas de competencia correspondientes a OntoFoCE. Se logró identificar una estructura de metadatos de cada una de las piezas de requerimientos que puede contener un punto de pericia y de su análisis, se arribó a un instrumento que en base a ellos sugiere la/s pregunta/s de competencia que lo responde. Se evaluó el desempeño del proceso de análisis y si la/s pregunta/s sugeridas eran pertinentes. Este proceso ejecutado con baja automatización resultó ser dificultoso, consumió mucho tiempo por lo que se prevé a futuro aplicar una herramienta de *parsing* que automatice el análisis de los puntos de pericia y separe sus componentes. Si bien, la primera evaluación indicó consistencia en un alto número de casos, coincidió con que eran los más sencillos o directos y su expresión era clara. Se deberá realizar una prueba de concepto sobre una muestra de mayor tamaño y diversidad de escritura para poder medir la robustez de la propuesta. Estos resultados deberán ser expuestos ante los usuarios expertos (peritos informáticos) y los actores del ámbito judicial para contribuir al uso de un lenguaje común y generar aprendizajes que mejoren el uso de terminología específica, reduzcan la ambigüedad, brinden precisión y claridad del alcance de los puntos de pericia, entre otros.

Referencias

[1] Andrés, M. M. C. (2016). Los desarrollos tecnológicos y su influencia en el crecimiento de los ciberdelitos en Colombia (Bachelor's thesis, Universidad Piloto de Colombia).

[2] Callegari, N. (1985). Delitos informáticos. Revista de la Facultad de Derecho y Ciencias Políticas.

[3] Cafferata Nores, J. I., & García, G. (2003). La prueba en el proceso penal. (LexisNexis, Ed.) (5a Edición). Buenos Aires: Depalma.

[4] Corcho, O., Fernández-López, M., Gómez-Pérez, A., & López-Cima, A. (2005). Construcción de ontologías legales con la metodología METHONTOLOGY y la herramienta WebODE. Law and the Semantic Web. Legal Ontologies, Methodologies, Legal Information Retrieval, and Applications, 142-157.

[5] Convenio sobre Ciberdelincuencia, Serie de Tratados Europeos N° 185, Consejo de Europa, Budapest, 23-11-2001.

[6] De Reuver, M., & Haaker, T. (2009). Designing viable business models for context-aware mobile services. Telematics and Informatics, 26(3), 240-248.

[7] Dehner, G. A., Eckert, K. B., Lezcano, J. M., & Ruidías, H. J. (2019). Modelo de recuperación de información jurídica basado en ontologías y distancias semánticas. In XIX Simposio Argentino de Informática y Derecho (SID 2019)-JAIIO 48 (Salta).

[8] Di Iorio, A. H., Curti, H., Greco, F., Iturriaga, J. I., Ruiz De Angeli, G., Podestá, A., ... & Constanzo, B. (2015). Proceso Unificado de Recuperación de Información (PURI) en redes informáticas. In Simposio Argentino de Informática y Derecho (SID 2015)-JAIIO 44 (Rosario, 2015).

[9] Domínguez, A. I. C., & Cornejo, R. G. (2020). La ciberdelincuencia en España: Un estudio basado en las estadísticas policiales. Revista Electrónica de Estudios Penales y de la Seguridad: REEPS, (6), 2.

[10] Friedman, T. L. (2006). The world is flat [updated and expanded]: A brief history of the twenty-first century. Macmillan.

[11] ISO/IEC. (2014). INTERNATIONAL STANDARD ISO / IEC 27000. Information technology -Security techniques - Information security management systems - Overview and vocabulary (Vol. 2014).

[12] Kowalski V., Morano D., Erck I., Cirimelo S., Enriquez H. (2020). "¿Qué se debe cambiar para orientarse a un Enfoque Basado en Competencias? Formación por Competencias, Aprendizaje Centrado en el Estudiante y Estándares de Acreditación de Segunda Generación para Ingeniería". Laboratorio MECEK y Confedi.

[13] Loucopoulos, P., & Karakostas, V. (1995). System requirements engineering. McGraw-Hill, Inc..

[14] Palmer, G. A. (2001, November). Roadmap for Digital Forensic Research Technical Report DTR-TOO I-01DFRWS. In Report from the First Digital Forensic Workshop (DFRWS) 2001.

[15] Parra de Gallo, H. B. (2019). "Una Ontología del Correo Electrónico y su Trazabilidad como Soporte para la Forensia Digital ". ISBN 978-987-86-3560-6

[16] Pohl, K. (2010). Requirements engineering: fundamentals, principles, and techniques. Springer Publishing Company, Incorporated.