

Un análisis económico del secreto comercial y de la protección legal y criptográfica del algoritmo

Anexo: Propuesta de un Registro Público Descentralizado de Secretos Comerciales y diseño de un nuevo software de encriptación para implementarlo

Por Tobías Rímoli
Universidad Torcuato Di Tella
tobiasrimoli@mail.utdt.edu

Sumario: El criterio del uso más óptimo de los recursos disponibles guía la administración de los activos de las empresas, así como la estrategia jurídica a implementar al momento de decidir con qué institutos proteger sus intangibles, e inclusive la tecnología criptográfica a utilizar para resguardar dichos activos. Con este marco en consideración, nos centraremos especialmente en el secreto comercial como estrategia y en el algoritmo como intangible, para concluir proponiendo dos formas de protegerlos, una exclusivamente informática a través del desarrollo de una extensión del explorador web y otra que importaría una reforma estructural del modo en que se resguardan aquellos secretos más valiosos por medio de la creación de un Registro Público Descentralizado y un software que genere un nuevo tipo de hash.

Palabras clave: Activos intangibles, criptografía, SaaS, nube, NFT, Google, hacking, big data, Teoría de juegos, hash, Blockchain, descentralización, audiencia judicial, BFA.

Contenido:

Un análisis económico del secreto comercial y de la protección legal y criptográfica del algoritmo

- I. Introducción: Precios, administración de la información e intangibles.
- II. El secreto comercial.
- III. El daño: requisito y eficiencia.
- IV. La protección del algoritmo
 - A. Caracterización
 - B. Vías legales
 - a. Patente de invención
 - b. Derecho de autor
 - c. Defensa de la competencia
 - d. Contrato
 - e. Secreto comercial
 - C. Vías informáticas

Anexo – Propuesta de un Registro Público Descentralizado de Secretos Comerciales y diseño de un nuevo software de encriptación para implementarlo

- A. Introducción
- B. Teoría de juegos y el costo computacional
- C. Concepto y mecánica
- D. Contraseñas y aleatoriedades
- E. Desarrollo del software y medidas de seguridad adicionales
- F. El Registro
- G. La hoja de ruta y la audiencia judicial
- H. Ejemplo de funcionamiento (con anotaciones)
 - a. Generación del hash e inscripción en el Registro
 - b. Control judicial ante un eventual litigio

Referencias

Un análisis económico del secreto comercial y de la protección legal y criptográfica del algoritmo

I. Introducción: Precios, administración de la información e intangibles

Si consideramos que el sistema de precios es un mecanismo para comunicar información (Hayek, 1945), y si atendemos a que las compañías que cotizan ven expresado su valor estimado por el mercado a través de precios, aquellos números -expresados en moneda- resumirían infinidad de datos de la compañía, de la industria y del mercado en general.

Aumentar el valor y, tarde o temprano, que se refleje en precios es el objetivo central de las compañías. En ese sentido, no todo lo que se comunica implica beneficios para las mismas: hay informaciones que, cuando se logran restringir al público y monopolizarlas, permiten valorizar la empresa o evitar su desvalorización.

Hay dos clases de este tipo de informaciones, aquellas que se apegan a los usos comerciales honestos y las que no. A modo de ejemplo, es legítimo que una empresa alimenticia oculte la receta de sus productos, pero no lo es que oculte sus ingredientes en tanto aquellos pueden llegar a perjudicar la salud de algunos consumidores. Desde otro plano, es legítimo que la empresa oculte su estrategia comercial pero no lo es que oculte el fracaso de la misma a sus inversores.

Sea el caso de no revelar ingredientes que pueden ser peligrosos para la salud o el caso del fracaso de la estrategia, se refleja que se ha incurrido en acciones u omisiones que generaron información errónea al mercado respecto de la compañía, impactando en su valorización. Algo que es repudiado por los usos comerciales honestos ya que implicarían una defraudación al mismo.

En cambio, aquellas informaciones que, por el contrario, si se ocultan no repudiarían los usos comerciales honestos, estando legítimamente bajo el control de la empresa, no sería cuestionable su monopolio. Por el contrario, en aquellos casos en que aquel sea de valor para la empresa (activos intangibles), si no se lo establece y gestiona correctamente, podría significar que el administrador no ha obrado con la diligencia de un buen hombre de negocios, haciéndoselo responsable por los daños de su omisión (art. 59 LGS).

Para Lev “los intangibles (empleados calificados, patentes, know-how, software, relaciones con los clientes, marcas, procesos y modelos organizacionales únicos, entre otros) generan la mayor parte del crecimiento empresarial y del valor para los accionistas. Asimismo, representan más de la mitad de la capitalización de mercado de las empresas que cotizan en bolsa y concretizan la ventaja competitiva de las empresas (Lev, 2003)” (González G, 2015).

En tanto el sistema de precios se basa en hechos más que en derechos, cuando aquí hablamos de monopolio nos referimos a una perspectiva práctica de aquel. En tanto existan monopolios de derecho, aquellos en la medida de que se correlacionen con la realidad, es decir en tanto que la coacción institucional del Estado, sea de oficio o a pedido de parte, logre corresponder en hechos aquel derecho (enforcement). En base a esta perspectiva práctica, y la imposibilidad de protegerlos legalmente en muchos casos, es que ciertos datos y productos se resguardan exclusivamente por medio de medidas tecnológicas de las propias empresas.

En los casos en que aquel monopolio legítimo sea violado, la ley reconoce acciones a la presunta víctima de para que, en la medida de que lo perjudique, propender su cese y reparación, así como la punición del responsable.

II. El secreto comercial

Juan M. Farina lo define de la siguiente forma (Farina, 1991):

" (...) Consiste en técnicas o procedimientos industriales descubiertos o creados por una empresa, que no llegan a tener entidad suficiente para ser tutelados mediante una patente de invención, modelo o diseño, pero que permiten a dicha empresa lograr determinada calidad, menores costos o imprimir a sus productos características especiales. (...)".

La ley de secretos comerciales (LSC) o Ley 24.766, o -como la misma se titula- la “*Ley de confidencialidad sobre información y productos que estén legítimamente bajo control de una persona y se divulgue indebidamente de manera contraria a los usos comerciales honestos*”, no lo define en forma expresa, sino que rige las condiciones que deberían reunirse para iniciar la acción, siguiendo la tradición regulatoria romanista. Así, establece:

Las personas físicas o jurídicas podrán impedir que la información que esté legítimamente bajo su control se divulgue a terceros o sea adquirida o utilizada por terceros sin su consentimiento de manera contraria a los usos comerciales honestos, mientras dicha información reúna las siguientes condiciones:

De la Ley de Secreto Comercial y el desarrollo de la doctrina se desprenden los requisitos que debe cumplir la información tutelable por el Secreto Comercial:

1. Ser secreta en el sentido de que no sea, como cuerpo o en la configuración y reunión precisas de sus componentes, generalmente conocida ni fácilmente accesible para personas introducidas en los círculos en que normalmente se utiliza el tipo de información en cuestión (artículo 1, inciso a, Ley 24.766).
2. Tener valor comercial por ser secreta (artículo 1, inciso b, Ley 24.766).
3. Haber sido objeto de medidas razonables, en las circunstancias, para mantenerla secreta, por la persona que legítimamente la controla (artículo 1, inciso c, Ley 24.766).
4. No ser susceptible de ser tutelada mediante una patente de invención, modelo o diseño (requisito de la doctrina, no todos los autores coincidentes en este punto (Herrera & Paludi, 2019)).
5. Encontrarse en un documento, medio electrónico, magnético, discos, ópticos, microfilmes, películas u otros elementos similares (artículo 2, Ley 24.766)
6. Si se tratase de información a la que se haya accedido con motivo de una relación de trabajo, empleo, cargo, puesto, desempeño de la profesión o relación de negocios, haber estado prevenidos de su confidencialidad (artículo 3, Ley 24.766).

La Ley 24.766 no consagra un derecho en concreto como sí sucede con el derecho de autor el cual se protege desde la materialización o exteriorización y a partir del que se desprenden las acciones de ley. En este caso, en cambio, lo que se repudia son las prácticas comerciales deshonestas, especialmente las que puedan causar daños. En efecto, el artículo 11 postula:

La protección conferida por esta ley no crea derechos exclusivos en favor de quien posea o hubiera desarrollado la información.

Posteriormente continuaremos describiendo el secreto comercial cuando nos refiramos a la protección del algoritmo, antes urge profundizar en el lugar que ocupa el daño como punto de partida de la reacción institucional ante la violación de los secretos comerciales.

III. El daño: requisito y eficiencia

En cuanto a la necesidad de acreditar daños, ésta se plasma en las tres vías de ley, los cuales pasamos a analizar:

El artículo 11 continúa:

El acceso por terceros a la información de manera contraria a los usos comerciales honestos, dará derecho a quien la posea a ejercer las siguientes acciones: a) Solicitar medidas cautelares destinadas a hacer cesar las conductas ilícitas.

En efecto, al solicitar medidas cautelares conforme los requisitos generales de aquellas, debe acreditarse judicialmente el peligro en la demora por lo tanto aquel debe poner en riesgo algún derecho.

b) Ejercer acciones civiles destinadas a prohibir el uso de la información no divulgada y obtener la reparación económica del perjuicio sufrido.

A fin de iniciar acciones para prohibir el uso de información no divulgada además se debe requerir la reparación económica del perjuicio. Esto se desprende de una interpretación gramatical de la norma al usar la conjunción “y” entre “prohibir el uso de la información no divulgada” y “obtener la reparación económica del perjuicio sufrido”.

Desde el plano penal, aquella ley remite al Código Penal en cuanto dispone que:

Artículo 12: Quien incurriera en la infracción de lo dispuesto en la presente ley en materia de confidencialidad, quedará sujeto a la responsabilidad que correspondiera conforme con el Código Penal, y otras normas penales concordantes para la violación de secretos, sin perjuicio de la responsabilidad penal en que se incurra por la naturaleza del delito.

En consecuencia, aquel Código postula:

Artículo 156: Será reprimido (...) el que teniendo noticia, por razón de su estado, oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño, lo revelare sin justa causa.

Por lo tanto, uno de los extremos a demostrar en el delito es la posibilidad de causar daño. La acción por este delito, tal como dispone el artículo 73 inciso 2 es una acción privada, por lo que el afectado debe promoverla y además proseguirla.

Esta inclusión del delito como acción privada se sostiene en base a un sentido de eficiencia utilitarista. El proceso judicial y la eventual condena contra quien habría divulgado un secreto comercial podría causar una mayor difusión pública del hecho, por lo que la acción

podría multiplicar daños. En efecto, es la víctima quien está en mejor posición para juzgar si un proceso judicial de represión contra el dañador le genera más daño o no, y en consecuencia aquella solución sería la preferible para la sociedad.

Producida la fuga de información sobre secretos comerciales, es posible que el afectado se vea beneficiado en proseguir la sanción penal más allá de sus costos en patrocinio legal. Esto porque podría dejar un mensaje a propios y ajenos de que la empresa no permitirá este tipo de conductas, desincentivando nuevas violaciones, reduciendo riesgos de nuevas fugas y aminorando costos potenciales en pérdida del monopolio sobre activos intangibles de la compañía.

IV. La protección del algoritmo

A. Caracterización

Sobre códigos informáticos se sostiene la economía actual, las comunicaciones, la producción, generación, explotación, fabricación y distribución -directa o indirectamente- de prácticamente todas las materias primas, productos y servicios, la generación de documentos e instrumentos públicos y privados. Prácticamente ninguna novedad de la segunda década del Siglo XXI puede ser ajena a la intervención del algoritmo de alguna u otra forma. He ahí la importancia de comprenderlo, algo que -a mi juicio- se hace con una velocidad que no acompaña el crecimiento exponencial de su uso, lo que en la práctica deriva en asimetrías de poder en la sociedad. Profundizar en dicho análisis, propio de las ciencias políticas y sociales, no es el objetivo de esta nota. En este capítulo nos avocaremos a comprender alternativas legales de su protección a través del análisis económico del derecho.

B. Vías legales

a. Patente de invención

Para que algo sea patentable debe implicar una novedad mundial, una actividad inventiva y aplicabilidad industrial, tal como dispone el art. 33 inciso 1 del Tratado de Cooperación en materia de patentes (PCT). A ello además la doctrina ha añadido el estar descripto suficientemente y ser materia protegible (Vazquez D'Alvaré, 2015).

Sin embargo, el artículo 6 inc a) de la Ley de Patentes de Invención y Modelos de Utilidad -Ley 24.481-, asimismo, excluye a “los métodos matemáticos”, a los que podrían reducirse el código del algoritmo. Expresamente también el inciso c) agrega “los programas de computación”. No obstante, el artículo 17 permite la registración de grupos de invenciones “relacionadas entre sí de tal manera que integren un único concepto inventivo general”, de esta forma se admitiría la protección de algoritmos embebidos en un software que a su vez esté incluido en algún tipo de dispositivo que sí es patentable.

De todas formas, tal como expone Posner y cnia. dado que cuando se emite la patente se hace de su solicitud un documento público, divulgándose los pasos que constituyen la invención con suficiente detalle para permitir a los lectores fabricar el propio producto. Si bien legalmente no pueden utilizar la información para fabricar, utilizar o vender el producto o proceso patentado sin una licencia del titular, pueden “inventar alrededor” de la invención patentada, es decir sin duplicar los pasos particulares, obteniendo el mismo resultado sin infracción (Posner, Landes, & William, 2003). Esto demuestra lo inviable que es su aplicación al algoritmo ya que las pequeñas modificaciones son perfectamente posibles y sin mucho esfuerzo de lograría un algoritmo diferente.

En efecto, inclusive el requisito de novedad inventiva puede ser cuestionable dadas las características propias de la creación de software, del cual cada avance generalmente se da

en base a desarrollos anteriores, inclusive utilizando repositorios públicos como Github e infinidad de foros que hay en internet.

b. Derecho de autor

Si se considera al algoritmo como obra original en su materialización en lugar de atenerse a su formulación lógica, matemática, como diagrama de flujo o lenguaje de programación, podría protegerse por esta vía. Acreditados los requisitos de originalidad y el de ser susceptible de expresión, reproducción o divulgación, se lo consideraría una obra protegible por el derecho de autor (Morales Oñate, 2021).

Caso extremo de la consideración del algoritmo como obra original se da en los NFT, donde se han llegado a subastar como piezas originales. En la imagen siguiente puede verse cómo luce el sitio “Dusk” en la web oscura, el primer sitio creado en aquella red, en el que anuncian la subasta de la clave privada de su código en forma de token no fungible.



Apariencia del sitio Dusk (Duskgytldkxiuqc6.onion) al momento de entrega de esta investigación.

c. La defensa de la competencia

La apropiación ilegítima de informaciones bajo el poder de la competencia puede ser causal de competencia desleal, esto se da especialmente en caso de que ésta tenga como objeto o efecto la intención de fijar, concertar o manipular el precio de venta de bienes o servicios en el mercado, tal como reconoce el artículo 2 inciso a de la Ley 25.156.

Puede darse el caso en el que la competencia que haya accedido ilegítimamente al algoritmo de fijación de precios de la plataforma de e-commerce o al algoritmo de flash trading de una plataforma de intercambio y aproveche su funcionamiento para afectarla y excluirla del mercado. En esos casos la correlación anticipada del comportamiento entre ambas podría ser indicativo, aunque no demostraría la apropiación ilegítima.

d. Contrato

Esta forma de protegerlo podría ser una de las mejores alternativas ya que goza de un gran desarrollo jurisprudencial, así como bajos costos de implementarlo. Aunque ejecutarlos puede implicar costos legales y dificultad probatoria. En aquellos donde se fije confidencialidad se debería individualizar, en la medida de lo posible, la información sujeta al mismo.

Cláusula ejemplo:

Información no pública – Confidencial: *“El contratado” no podrá comunicar a persona alguna la información no pública o de carácter confidencial de que haya tenido conocimiento, con motivo de la ejecución de sus obligaciones emanadas del presente contrato, salvo que así lo requiera su cometido o que “La Contratante” lo hubiera autorizado expresamente a hacerlo. Esta obligación de reserva o confidencialidad seguirá en vigor aún después del vencimiento del plazo de rescisión o resolución del presente contrato. Haciéndose responsable “El Contratado” de los daños y perjuicios que pudiera irrogar la difusión de datos e informes no publicados.*

En cuanto a la autoría de lo creado, en los contratos de trabajo de creación de software o locación de servicios deberían incluirse cláusulas donde se cede toda creación y se renuncia a realizar reclamo alguno respecto a su propiedad o titularidad. El incumplimiento, apropiación o transferencia a un tercero habilitaría la acción por incumplimiento contractual.

Cláusula ejemplo:

Derechos de propiedad: *Los derechos de propiedad de autor y reproducción, así como cualquier derecho intelectual de cualquier naturaleza que sea, sobre cualquier informe, estudio y obra producida como consecuencia de este contrato por parte de “El Contratado”, pertenecerá exclusivamente a “La Contratante”.*

e. El Secreto comercial

Esta vía, antes desarrollada en esta nota, es la más utilizada para proteger al algoritmo, la cual ha vivido un resurgimiento como instituto desde la expansión de internet. Sin embargo, es sumamente frágil ya que no protege un derecho sino, como antes desarrollamos, brinda acciones ante el daño. Esto implica que una vez que la información haya sido divulgada empieza a integrar el dominio público y desde entonces no hay marcha atrás. Asimismo, es susceptible a de que se realicen simulaciones de los procesos de generación de informaciones similares, lo que sería difícil de desacreditar por quien padeció la violación.

Por otro lado, trae como ventajas que como no requiere inscripción. Si se adoptan medidas como por ejemplo incorporar la palabra “Confidencial” en forma de inevitable lectura a cada documento a proteger, se puede ahorrar importantes costos en trámites. Asimismo, atento a que no es necesario realizar registración alguna, tampoco requiere renovaciones, protegiendo en forma ilimitada en el tiempo y omitiendo costos administrativos y legales que implicaría una registración.

Sin embargo, la producción probatoria puede resultar sumamente difícil. Las empresas precisan de una forma en la cual acreditar la entrega de información confidencial y la existencia en el tiempo del Secreto, sin por ello incurrir en costos como los de los trámites de patentes.

En efecto, la redes blockchain pueden aportar una solución en cuanto permiten acreditar con una seguridad incomparable la existencia en el tiempo del secreto, siempre que éste se encuentre en un archivo o se pueda volcar en uno. El archivo podría reducirse a un código hash y éste anotarse en la red descentralizada, produciendo una marca de tiempo que posteriormente -ante su consulta- devuelva la existencia o no del archivo y la fecha en que fuera inscripto. Dados los bajos costos, el sistema podría ser provisto por el Estado para su

generación automática desde un sitio web, sin trámites o costes adicionales que impongan trabas al usuario. En el Anexo de este trabajo desarrollará esta idea.

C. Vías informáticas

Más allá de las consideraciones legales, no debe omitirse observar alternativa informática que es central ya que, como hicimos referencia en la introducción y al desarrollar los secretos comerciales en el punto anterior, lo relevante en el ámbito del comercio son los hechos. Y, si existen alternativas para que el enforcement sea menos costoso por vía tecnológica que la legal, ésta será la mejor alternativa.

En ese sentido, los controles sobre el derecho de autor son usuales, plataformas como Netflix han implementado bloqueos para evitar las capturas de pantalla y plataformas como YouTube aplican algoritmos sobre los videos antes de ser publicados en búsqueda de material protegido.

Los secretos comerciales, en cambio, atento a sus características particulares pueden estar contenidos en conversaciones entre el personal y en infinidad de documentos de la compañía, pudiendo presentar gran desestructuración y heterogeneidad. Al efecto, las soluciones tecnológicas pueden ser la mejor alternativa en muchos o la mayoría de los casos. En otros, en cambio, dada la relevancia económica del intangible, las opciones legales serían indispensables para complementar su protección tal como desarrollaremos en el Anexo.

Más allá de la encriptación y certificación que trajo la implementación del protocolo Hhttps, el uso de comunicación encriptada de punta a punta, implementada en 2014 por Whatsapp, puede ser una solución ante ataques ‘man in the middle’, el ojo no deseado del distribuidor de internet o los gobiernos. Sin embargo, las compañías normalmente no los utilizan y dejan sus mensajes expuestos al servidor o -en los casos en que el proveedor declara encriptar- confían ciegamente en que efectivamente lo haga y no haya dejado puertas traseras. En esos casos los mensajes podrían quedar expuestos a eventuales hackers, a empleados descontentos y a los miles de empleados de seguridad y servicios de inteligencia que acceden a los datos, muchas veces sin orden judicial alguna, algo que no debería pasar -por lo menos en los EE.UU.- desde la derogación de la Ley Patriot en el 2015.

Las compañías exponen sus secretos en forma diaria al redactar sus mails, cargar archivos adjuntos y utilizar la nube. Inclusive en el Estado -caso que excede esta nota-, por ejemplo, el Ministerio Público Fiscal de la Nación se provee de mails oficiales de Outlook y diversas oficinas del Gobierno de la Provincia de Buenos Aires utilizan servicios de Google Drive; en ninguno de estos casos se encripta desde el usuario.

Urge tomar medidas, no obstante, el abaratamiento de los costos de uso de este tipo de plataformas ha estimulado su implementación. Es que justamente la minería de datos sobre las comunicaciones y archivos de los usuarios genera importantes ingresos económicos al proveedor, permitiéndole ofrecerlos gratuitamente en muchos casos. En efecto, un extracto de las políticas de privacidad de Google ([Policies.google.com/privacy](https://policies.google.com/privacy)) menciona:

“Recopilamos información sobre su actividad en nuestros servicios (...) También recopilamos el contenido que crea, carga o recibe de otras personas. Este contenido incluye los correos electrónicos que escribe y recibe, las fotos y videos que guarda, los documentos y las hojas de cálculo que crea, y los comentarios que hace en videos de YouTube. (...) es posible que recopilemos información de

registro de los mensajes y las llamadas (...) Proporcionamos información personal a nuestros afiliados u otras empresas o personas de confianza para que la procesen por nosotros.”

Otro factor que influye sobre estos costos son los desarrollos que explica la “Ley” de Moore, que postula que cada 24 meses la potencia de los ordenadores se duplicaría, al permitir que los transistores ocupen menos espacio. Se pudo advertir en la práctica durante décadas que el postulado se correspondía con la realidad. Tras llegar a los límites de la física se desarrolló la tecnología de los núcleos o ‘core’, permitiendo seguir elevando la potencia. Todo esto ha permitido que año a año los servidores sean más potentes, generando un abaratamiento de costos y consecuente procesamiento en origen de los datos.

| | Small – Linux – N. Virginia (m1.small) | Quadruple Extra Large (/cgl.4xlarge/c3.4xlarge) |
|------------------|---|--|
| 1/1/2010 | \$0.09 | \$3.16 |
| 3/12/2012 | \$0.08 | \$2.50 |
| 12/1/2012 | \$0.07 | \$2.10 |
| 4/14/2014 | \$0.04 | \$1.50 |

Precios históricos de Cloud Computing para dos tipos de casos populares.

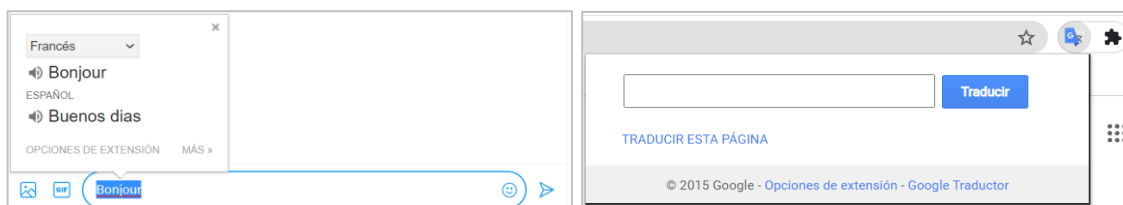
Fuente: Phox, Sherin, Schmahmann, & Niles, 2017.

Al implementar esta infraestructura también se pueden beneficiar los proveedores al reducir el acceso del dispositivo cliente a su algoritmo, reduciendo posibilidades de que se aplique ingeniería inversa -pretender copiar el código fuente desde el código objeto- o crackeos -parches no autorizados que cambian las características originales y/o quita bloqueos comerciales-. A su vez genera mayor velocidad en la carga y también es más seguro dado que no interviene el dispositivo del usuario en el procesamiento, habiendo pasado sus archivos al servidor por rigurosos controles. Esto se puede advertir en el nuevo paradigma de computación en la nube. A través de la idea del Software como servicio (SaaS) se han desarrollado incluso sistemas operativos, es el caso de Chrome OS.

Esta forma de funcionamiento, así como le hace imposible al usuario el auditar el software, también le hace casi imposible el poder controlar los datos que la terminal comparte con el servidor, más aún en sistemas que para su normal funcionamiento requieren de una interacción constante con la central.

Entonces, en definitiva, las empresas que utilicen estos sistemas están exponiendo sus datos y secretos comerciales a su proveedor de alojamiento y/o procesamiento en la nube, pero antes de eso a todos los intermediarios de internet sobre los que pasó el paquete entre que salió del cliente hasta que encontró al servidor siempre que hayan logrado romper el protocolo Https, algo que puede realizar por cualquier aficionado con herramientas como Bettercap.

He ahí la importancia de que en esa interacción quien desee proteger sus secretos comerciales depositados en la nube trabaje con documentación encriptada a cotidiano antes de su alojamiento; una ocupación que sería sumamente costosa si no se cuenta con softwares que codifiquen y decodifiquen automáticamente la información en el usuario antes de su carga a la red. Un funcionamiento similar al de las extensiones de traducción en los exploradores web sería sumamente práctico, de modo que permita operar sobre la página web pero que antes realice una triangulación de los datos, de forma tal que la mera escritura sobre un cuadro de texto no implique envío de datos al servidor sin antes pasar por el codificador.



Ejemplo de extensión de traducción en explorador web: Google Translate en Chrome.

En efecto, si se cuenta con un cifrado lo suficientemente fuerte, aumentaría los costos de aquellos que quieran acceder a los datos y generaría un dilema del prisionero inhibiendo a actuar a quienes quieran acceder a ellos. Estos efectos serían aún mayores y el esquema tendría gran solidez si para todo dato se utilizara encriptación a fin de evitar el señalamiento que implicaría la información encriptada como información importante en contraste con el resto, logrando de esta forma ocultar lo relevante en un mar de información no relevante, multiplicando costos si se desea acceder a algún dato valioso.-

Anexo

Propuesta de un Registro Público Descentralizado de Secretos Comerciales y diseño un nuevo software de encriptación para implementarlo

A. Introducción

La publicidad del sistema actual impide el depósito de los secretos comerciales en registros públicos ya que el acto administrativo quitaría el velo de secretismo sobre el intangible. No obstante, un régimen que deposite versiones codificadas podría ser viable. Al respecto el acto podría ser eliminado a fin de realizar un mero hecho de la administración como sería el funcionamiento automático de un sistema web que recepte un código hash anotado por el usuario para su posterior anotación en una red descentralizada. Esto implicaría el reconocimiento del procedimiento iniciado por el peticionante en forma anónima y a su mero interés, sin convalidar derecho alguno sobre el contenido de la registración. Se seguiría con el mismo criterio actualmente vigente de que quien hace uso del secreto comercial, y en este caso del Registro, es quien por razones económicas le es conveniente. A su vez, quien es poseedor del documento, de la marca de tiempo y de la hoja de ruta podría exigir las acciones que actualmente le reconoce la ley.

Como mencionamos anteriormente, el secreto se presentaría codificado en forma de hash, de esta manera se quitaría del conocimiento de los funcionarios y de cualquiera que vulnere la seguridad del Registro la posibilidad de acceder al contenido del mismo.

Con base a los avances planteados por (Dyrhovden, 2017), en orden al concepto de funcionamiento de Blockchain y diversas técnicas criptográficas que podido estudiar y experimentar, planteo la propuesta tecnológica que paso a desarrollar.

B. Teoría de juegos y el costo computacional

El gráfico siguiente indica el tiempo necesario para descifrar una contraseña mediante la fuerza bruta en función de la entropía (complejidad) de la contraseña, utilizando el sistema Diceware. Sobre esta lógica económica de costos computacionales está asentada buena parte de la criptografía y, en definitiva, la seguridad informática de las empresas, gobiernos y ciudadanos; inclusive lo que nos compete, los secretos comerciales y los algoritmos.

| Entropy (n bits) Entropy = $\log_2(S^L)$ L is pass length S is symbol pool (i.e. if your password has lowercase and numbers, your symbol pool is 26+10+36) | Length of password approximately equivalent to a given entropy Note: First three columns are rounded to a max of +/- 0.2 Fourth column is rounded to a max of +/- 0.05 | | | | Time until guaranteed brute-force password crack Based on attacker's guesses per second vs. password strength Formula: (Seconds to guaranteed crack) = $(2^{\text{entropy}}) \div (\text{guesses per second})$ Result then converted from seconds to more reasonable units of time such as years Note: By definition, it takes half of the guaranteed crack time on average to crack a password | | | | | | Entropy (n bits) Entropy = $\log_2(S^L)$ L is pass length S is symbol pool (i.e. if your password has lowercase and numbers, your symbol pool is 26+10+36) |
|--|---|---|---|--|--|-----------|---------------|-----------------|-------------------|---------------------|--|
| | Lowercase (26 symbols, 4.7 bits ea) | UPPER + lower + 0-9 (62 symbols, 5.95 bits ea) | UPPER + lower + 0-9 + special characters (94 symbols, 6.55 bits ea) | Pass phrase with an average of 4.3 letters per word (12.93 bits per word) Column's value = words in phrase | Attacker's brute force guesses per second | | | | | | |
| | | | | | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | |
| 120 | | 20 | | | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 120 |
| 118 | 25 | | 18 | | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 118 |
| 116 | | 19 | | 9 | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 116 |
| 114 | | | | | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 114 |
| 112 | 24 | | 17 | | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 112 |
| 110 | | | | | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 110 |
| 108 | 23 | 18 | | | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 108 |
| 106 | | | 16 | | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 106 |
| 104 | 22 | | | 8 | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 104 |
| 102 | | 17 | | | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 102 |
| 100 | | | | | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 100 |
| 98 | 21 | | 15 | | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 98 |
| 96 | | 16 | | | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 96 |
| 94 | 20 | | | | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 94 |
| 92 | | | 14 | | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 92 |
| 90 | 19 | 15 | | 7 | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 90 |
| 88 | | | | | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 88 |
| 86 | | | 13 | | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 86 |
| 84 | 18 | | | | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 84 |
| 82 | | 14 | | | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 82 |
| 80 | 17 | | | | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 80 |
| 78 | | 13 | | | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 78 |
| 76 | 16 | | 12 | 6 | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 76 |
| 74 | | | | | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 74 |
| 72 | | 12 | | | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 72 |
| 70 | 15 | | 11 | | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 70 |
| 68 | | | | | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 68 |
| 66 | 14 | 11 | 10 | | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 66 |
| 64 | | | | 5 | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 64 |
| 62 | 13 | | | | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 62 |
| 60 | | 10 | 9 | | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 60 |
| 58 | | | | | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 58 |
| 56 | 12 | | | | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 56 |
| 54 | | 9 | | | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 54 |
| 52 | 11 | | 8 | 4 | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 52 |
| 50 | | | | | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 50 |
| 48 | 10 | 8 | | | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 48 |
| 46 | | | 7 | | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 46 |
| 44 | | | | | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 44 |
| 42 | 9 | 7 | | | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 42 |
| 40 | | | 6 | 3.1 | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | 40 |
| Entropy (n bits) Entropy = $\log_2(S^L)$ L is pass length S is symbol pool (i.e. if your password has lowercase and numbers, your symbol pool is 26+10+36) | Length of password approximately equivalent to a given entropy Note: First three columns are rounded to a max of +/- 0.2 Fourth column is rounded to a max of +/- 0.05 | | | | Time until guaranteed brute-force password crack Based on attacker's guesses per second vs. password strength Formula: (Seconds to guaranteed crack) = $(2^{\text{entropy}}) \div (\text{guesses per second})$ Result then converted from seconds to more reasonable units of time such as years Note: By definition, it takes half of the guaranteed crack time on average to crack a password | | | | | | Entropy (n bits) Entropy = $\log_2(S^L)$ L is pass length S is symbol pool (i.e. if your password has lowercase and numbers, your symbol pool is 26+10+36) |
| | Lowercase (26 symbols, 4.7 bits ea) | UPPER + lower + 0-9 (62 symbols, 5.95 bits ea) | UPPER + lower + 0-9 + special characters (94 symbols, 6.55 bits ea) | Pass phrase with an average of 4.3 letters per word (12.93 bits per word) Column's value = words in phrase | Attacker's brute force guesses per second | | | | | | |
| | | | | | 10,000 | 1,000,000 | 1,000,000,000 | 100,000,000,000 | 1,000,000,000,000 | 100,000,000,000,000 | |

Fuente: HelmedHorror, 2015.

Con la teoría de juegos en miras, se deben diseñar sistemas criptográficos tal que los costos en capacidad de procesamiento sean tan altos que la función de utilidad del hacker sea no actuar. La teoría de la complejidad computacional se dedica al estudio de la dificultad que deriva a estos costos, todo lo que puede traducirse a cantidades de dinero.

No obstante, hay varios motivos para postular que con la tecnología actual los diseños existentes pronto pueden ser insuficientes, a saber:

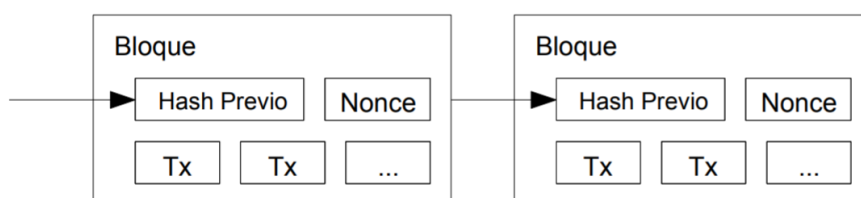
- Se puede prever que la computación en la nube siga bajando sus costos *-tal como expusimos anteriormente-*, lo que podría ser un problema debido a que sus clientes -además de los propietarios y sus asociados- pueden usarlo para romper hashes, como demuestra el caso del investigador Thomas Roth.
- Los Estados y grandes empresas pueden destinar importantes recursos para lograr intentar romper las codificaciones, algo no menor dadas las guerras comerciales existentes y la anonimidad de los ataques cibernéticos.
- La mejora continua de algoritmos de pools de trabajo en sistemas distribuidos (poder computacional descentralizado). Inclusive los casos de expansión de malwares que utilizan la capacidad de procesamiento de sus víctimas, como parásitos.
- Los avances en el desarrollo de la computación cuántica que acercan cada vez más el deadline de cambio del paradigma en la materia.

En efecto, profundizar la complejidad, es decir, aumentar los costes potenciales del atacante, se vuelve indispensable antes de implementar cualquier sistema que pretenda proteger secretos importantes. Ya que una vez que éstos estén codificados en el hash y cargados en la red no habría marcha atrás si un destinatario no deseado se hace con ellos. Dado que hay secretos comerciales que pueden llegar a guardarse hasta por más de 100 años y tener valores económicos sumamente altos, prever lo máximo posible de los avances tecnológicos que vendrán se vuelve indispensable.

Es necesario entonces adoptar medidas de seguridad aún más altas que las que implementa en general las empresas de tecnología Blockchain, lo cual es necesario ya que como en aquel sistema las transacciones fluyen por un corto período de tiempo antes de que se anote la transacción en el libro de contabilidad, el hacker debería actuar rápidamente. En nuestro caso, si la empresa ha codificado su secreto y el pirata ha logrado hacerse del mismo, no estaría limitado en tiempo para intentar romperlo. Por ello con un solo hash no sería suficiente y urge necesario un esquema complejo como el que describiremos a continuación.

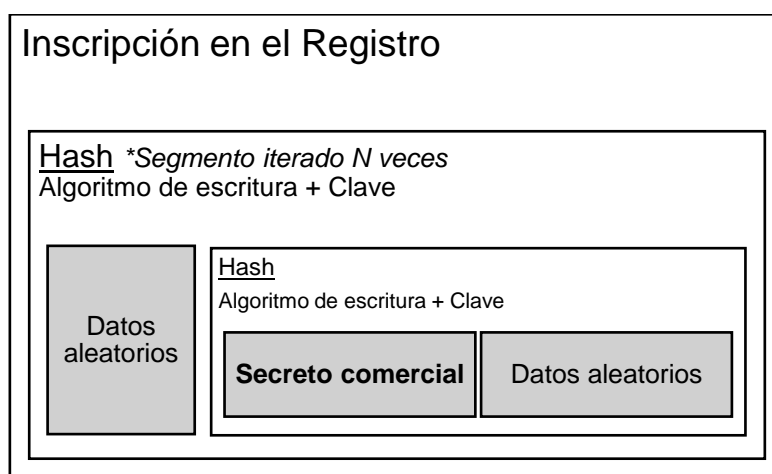
C. Concepto y mecánica

En Blockchain, dado que al alterar un bloque de datos cambiaría su hash, como el siguiente bloque tiene el código del anterior deberían romperse y modificarse todos los siguientes de la cadena, una hazaña que aún no se ha logrado o por lo menos anunciado. Por lo tanto, esta tecnología nos enseña que su fuerza consiste no tanto en el hash, ya que han existido experimentos -versiones anteriores a la actual- en que se han logrado romper, sino en la dificultad criptográfica de la sucesión de dichos códigos.



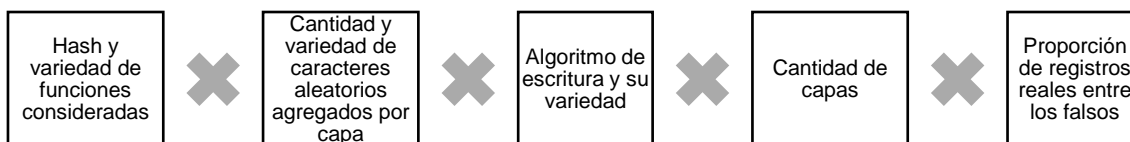
Esquema de funcionamiento de Blockchain. Fuente: Nakamoto, 2008.

En un esquema similar se basa nuestra propuesta que consistiría, en lugar de una cadena, en una sucesión de capas. De tal manera, se realizaría un hash del archivo del secreto comercial, tras lo cual se agregarían datos aleatorios y realizaría un nuevo hash de la conjunción de ambos. Tras obtener el nuevo código se agregarían más datos aleatorios y se hashearía otra vez. Este proceso se iteraría un número N de veces, agregando capa tras capa y alternando aleatoriamente el tipo de hash aplicado (*SHA-256, SHA-512, etc.*).



Esquema de funcionamiento del sistema propuesto.

Al agregar más capas se haría aún más difícil el trabajo al hacker, quien deberá tener un poder computacional suficiente para romper un hash multiplicado por la cantidad de iteraciones realizadas, todo multiplicado a su vez por la cantidad de algoritmos hash posibles utilizados, la cantidad de algoritmos de escritura por su clave y la proporción de registros reales entre los falsos. Cada una de estas variables serán oportunamente explicadas.



Este grado de dificultad es relevante sólo si ignoráramos lo siguiente: Que el elemento del algoritmo de escritura combinado con la generación de más de una capa le provee al sistema de una solidez prácticamente infranqueable. Esto es así porque si bien pasar la primera capa sería algo esperable, pasar la segunda ya sería una hazaña dado que el algoritmo escribiría cada carácter del hash y de la aleatoriedad en un orden determinado por una clave. De esta manera, al estar mezclado el hash con la aleatoriedad, una vez roto el primero tendría que encontrar la fórmula matemática que decodifique el algoritmo de escritura sin un parámetro predeterminado de cómo sería el output ya que como hay más de una capa no habrá un archivo fácilmente identificable sino más código. Si encontrara alguna vez la respuesta del primer hash, el hacker siquiera sabría del éxito de su trabajo ya que no tendría forma de corroborarlo.

D. Contraseñas y aleatoriedades

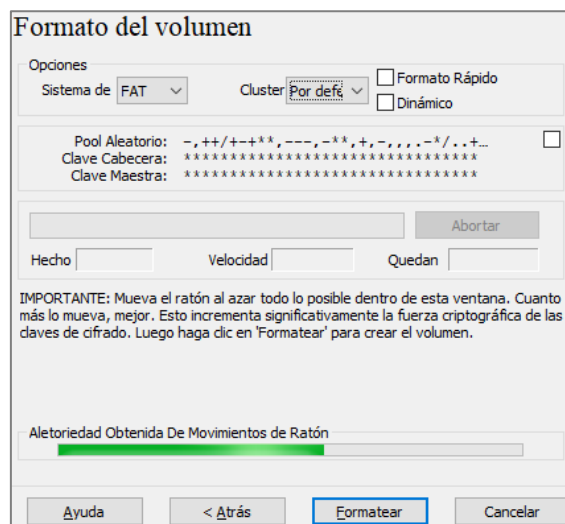
Toda aleatoriedad y contraseña utilizada sería generada por el sistema ya que las personas somos propensas a generarlas con poca entropía, es decir, con pocos valores, con uso de poca cantidad de caracteres respecto de la totalidad de los posibles (uso de muchas vocales por ejemplo), con gran aversión a los caracteres no alfanuméricos e inclusive solemos utilizar las estructuras predeterminadas del lenguaje (palabras, frases, etc). El siguiente gráfico realiza un análisis comparativo de los resultados de diferentes investigaciones al respecto, donde se puede advertir lo señalado.

| year | study | length | % digits | % special |
|------|------------------------|--------|----------|-----------|
| 1989 | Riddle et al. [15] | 4.4 | 3.5 | — |
| 1992 | Spafford [5] | 6.8 | 31.7 | 14.8 |
| 1999 | Wu [12] | 7.5 | 25.7 | 4.1 |
| 1999 | Zviran and Haga [18] | 5.7 | 19.2 | 0.7 |
| 2006 | Cazier and Medlin [14] | 7.4 | 35.0 | 1.3 |
| 2009 | RockYou leak [19] | 7.9 | 54.0 | 3.7 |

Atributos comunes estimados de las contraseñas. Fuente: Bonneau, 2012.

Cualquier usuario curioso puede acceder en internet a la big data de las filtraciones masivas de contraseñas, incluso con detalle de país, edad y demás características del titular, lo que se puede analizar estadísticamente para generar diccionarios acordes a la víctima en orden a la probabilidad de uso. De hecho, recientemente se ha publicado en el sitio Rfmirror.com el diccionario más grande de contraseñas de los que se alguna vez se hayan difundido públicamente, con 100 Gb de datos en Txt; con un listado tan abundante luego un hacker podría usarlo como materia prima para lanzar ataques de fuerza bruta desde programas como Hydra.

Por todo esto, es indispensable eliminar la intervención de la voluntad humana en la generación de contraseñas y generar claves sólidas. Además, es necesario evitar la implementación de algoritmos de generación automática, dado que pueden tener fallas haciéndolos previsibles y que nunca se tiene certeza de si sus desarrolladores no ocultaron puertas traseras. Para ello nuestro sistema incorporaría como input en la generación de contraseñas y aleatoriedades de los movimientos del mouse, tal como utiliza el software Veracrypt.



Captura de Veracrypt en proceso de recolección de datos de los movimientos del mouse.

Aleatoriamente se definiría la cantidad de capas. Al respecto se fijaría un número mínimo para garantizar rigidez, pero también un valor máximo para que el software tenga plazos razonables de funcionamiento y que el proceso no colapse el dispositivo.

Para romper nuestro sistema una posible forma sería utilizar un algoritmo de inteligencia artificial que pretenda generar uno a uno los outputs posibles, para el que fuera anteriormente entrenado, como por ejemplo el nombre de formatos (.txt, .docx, .exe, .jpg, etc.). Al hacer esto se estaría asumiendo una codificación perfecta. A modo esquemático, si el archivo del secreto comercial es el destino, el hash inscripto en el Registro serían las coordenadas de una de las escalas de la ruta hacia él, pero que sin las demás indicaciones de la ruta no habría forma de encontrarlo más que calcular todos los inputs hasta que alguno genere el primer output, y luego generar todas las combinaciones posibles y las combinaciones entre combinaciones que tengan como base el output del primer hash, a fin de encontrar en alguna de todas ellas algo que se parezca a un archivo comercial. Estimo que algo así sería inviable por los fundamentos expuestos. El dilema del prisionero, entonces, tendría reglas infranqueables.

E. Desarrollo del software y medidas de seguridad adicionales

El código fuente de nuestro software sería público, de código abierto y gratuito, adoptando el modelo de desarrollo del bazar de Babel (Raymond, 1999). De esta forma se motivaría su adopción por doble vía, por un lado, garantizando la auditoría de seguridad por la comunidad y admitiendo colaboraciones para robustecerla; y por el otro, al eliminar costos de uso se restringirían barreras y ampliaría la comunidad que lo utiliza y colabora tal como indica la ley de oferta-demanda. Al ser de código abierto podría modificarse para admitir otros usos además del que fuera diseñado originalmente, contribuyendo inclusive a la comunidad cypherpunk.

El usuario también puede dividir en varias registraciones el archivo o texto, registrando una parte en uno y otra en otro de modo de distribuir aún más los riesgos ante un ataque.

Para mayor seguridad, el software se utilizaría en un dispositivo offline sin placa de red, preferiblemente nunca conectado a internet desde su compra a nuevo. Se instalaría en el computador a través de un pen drive previamente formateado y también preferiblemente nunca usado anteriormente, al que se agregaría el archivo instalador utilizando una metodología de guardado similar a la del sistema operativo Tails. Dicho sistema operativo sería el recomendado.

El hash final se anotaría manualmente en otro dispositivo, sin conexión con el primero, para inscribirse en una red descentralizada de un Registro de secretos comerciales.

F. El Registro

Con este Registro luego se podría acreditar en juicio que quien alega la titularidad del secreto, efectivamente lo tuvo en su poder en un tiempo determinado, para lo que necesitaría un segundo archivo que demuestre la marca de tiempo.

El uso de un sistema de registración ante el Estado proveería al secreto comercial de seguridad y prueba legal que hoy no tiene, a su vez la utilización de una red Blockchain para almacenar los hashes finales de nuestro software proveería de la seguridad propia de la descentralización imposibilitando la alteración de los registros realizados anteriormente ya que deberían atacarse todos los nodos al mismo tiempo para lograr el cometido.

Una medida de seguridad sería adicionada por la entidad pública administradora: se anotaría entre registración y registración, cantidades aleatorias de hashes con información basura, de modo que entre medio de todas las registraciones reales la gran mayoría sean registros que no tienen ningún valor. De esta forma, el hacker que acceda al listado de hashes debería destinar un poder computacional exponencialmente más alto tan solo para encontrar un hash que le sirva para iniciar su trabajo.

En Argentina se ha creado Blockchain Federal Argentina (BFA), que es una red que tiene participación de entidades públicas y privadas, inclusive sectores de la industria, el comercio y de la sociedad civil, por lo que si bien no es conveniente para un sistema estrictamente secreto, servirá su plataforma cuando posteriormente en este texto ejemplifiquemos el proceso. En la práctica, podría crearse una red descentralizada del Registro de la Propiedad Intelectual para registrar los hashes.

G. La hoja de ruta y la audiencia judicial

Tras realizar la encriptación, el programa emitiría un archivo codificado que tras su decodificación indicaría a modo de hoja de ruta el detalle capa por capa de los datos aleatorios adicionados, el orden de ellas, el algoritmo hash y el de escritura utilizado, junto con sus contraseñas.

Ante un eventual litigio en el que la titularidad del secreto comercial desee ser probada, quien alega presentaría a la autoridad judicial el archivo hoja de ruta que sería decodificado anotando la contraseña en secreto durante la audiencia por el actor y permitiría que el programa repita el proceso en base a las órdenes predeterminadas, indicando en consecuencia si el hash resultante es coincidente o no con el registrado oportunamente. El archivo original del secreto comercial también podría reservarse por el actor hasta el momento de la audiencia y por imperativo legal podría limitarse excepcionalmente el derecho de la contraparte de controlar esta prueba. Todo esto a fin de reducir la exposición del documento secreto ante contrapartes o terceros que puedan participar en el juicio o acceder a las actuaciones.

H. Ejemplo de funcionamiento (con anotaciones)

**En este ejemplo no consideré el algoritmo de escritura ya que su inclusión podría dificultar la comprensión del funcionamiento.*

a. Generación del hash e inscripción en el Registro

1) Texto del secreto comercial:

Ingredientes de la torta Pasta Frola de Doña Marta S.A. (10 raciones): 125 gr. manteca de cabra, 125 gr. azúcar negra, 5 huevos de codorniz, esencia de vainilla extraído de orquídeas cubanas, ralladura de 1/2 limón, 250 gr. harina leudante, 600 gr. dulce de membrillo, 10 gr. de esencia de banana, 10 gr. de esencia de frutos rojos.

2) Hash del texto del secreto comercial

Ejemplo con función SHA512/256.

40552306c595b8e1b2dd192b0dec9e5807aa0659c8df2d56e397015ab28663b2

3) Hash + Aleatoriedad

Adicionar una aleatoriedad es necesaria porque si el proceso se itera, lograría evitarse la repetición del mismo hash. Es decir, tras haber hecho un hash sobre un hash, si se realiza un tercero éste repetiría el código del segundo y así sucesivamente. Adicionar una aleatoriedad que cambie con cada iteración modifica el input por lo que el output sería diferente. A su vez, mientras mayor sea el tamaño de la aleatoriedad más complejo sería resolver el hash ya que deberían introducirse más datos para obtener el código y sería más complejo resolver el algoritmo de escritura.

En los ejemplos siguientes se utiliza " - " para separar el hash de la aleatoriedad a mero sentido expositivo pero el algoritmo no introduciría aquel señalador ya que podría indicarle al hacker el éxito de su trabajo.

40552306c595b8e1b2dd192b0dec9e5807aa0659c8df2d56e397015ab28663b2 - HG1DF65SD5F1D35F1SD35GFSF53A4F65EAC65SDHG6J4JRT5H4df4gdfgdf53gdsf5gf5dg1fd53gdfg53df4g35dfg4fd53g4fdg31fg53fdg53dfgs53g153g1d35a1132sd1g3g1a351g53dfg15df3g1df53gdf5g1df5gdf5g151QF5EFFDG53DF531GFD35G1DF35G1DF3G1DF3G1

4) Hash de (hash + aleatoriedad), adicionado con una nueva aleatoriedad

Esta etapa se iteraría un número N de veces, generando nuevos hashes en base a clase funciones aleatorias de entre las posibles y códigos aleatorios adicionados al output anterior.

Ejemplo con función SHA3-256.

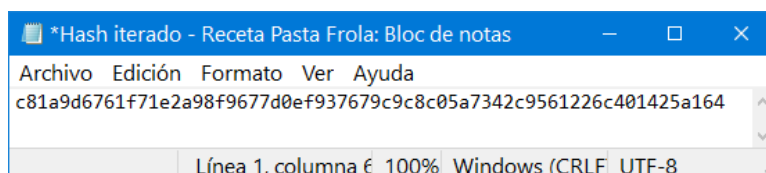
fb3d15acf127f98af42942d29f0c0849e15c28882f41abdd0e5d2bc86fdd09f0 - DFH4GDagfdhDSsffd4hdhdF5dfhdSFtfma56GSDDsfdg5FdhfgmhsD5Fgfd4gfsa6515SG6SA6s6A1G51g5d1h5d1515DF15DF51df5151SD5G1ED5V1S53D4HSGS654GS454G6RS65G1SDS6RT4Rdfgs6fh5t1d53r1d35aaf35ef1sf5gwe51g35DF5kmvF5A4FS5F44DS5F4SD5

5) Último hash

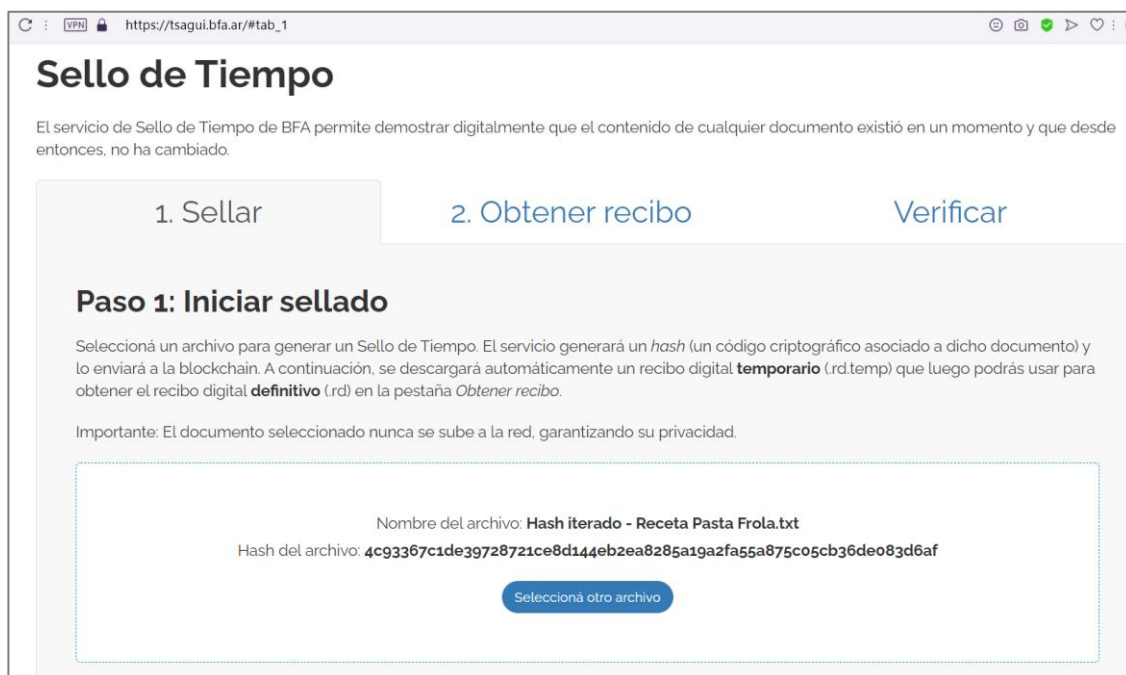
Ejemplo con función Keccak-256.

c81a9d6761f71e2a98f9677d0ef937679c9c8c05a7342c9561226c401425a164

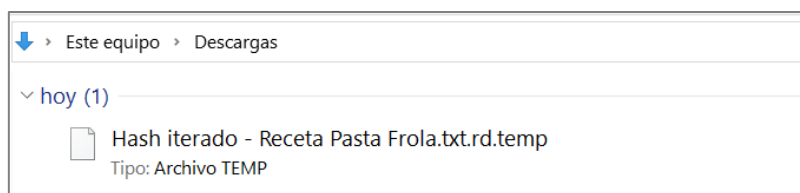
6) Adición del código a un archivo en formato .txt



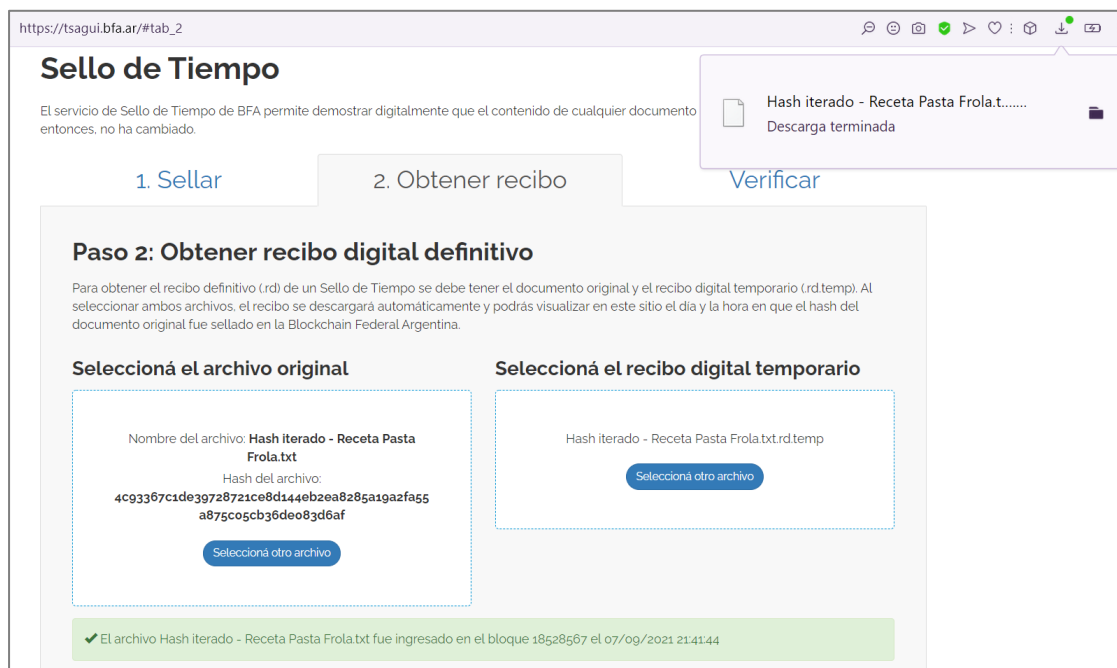
7) Registro del archivo en BFA y generación de la marca de tiempo provisoria



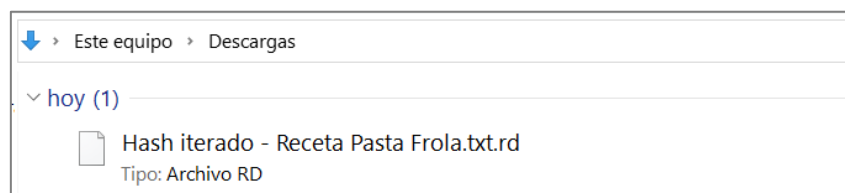
8) Marca de tiempo provisoria generada



9) Generación de la marca de tiempo definitiva

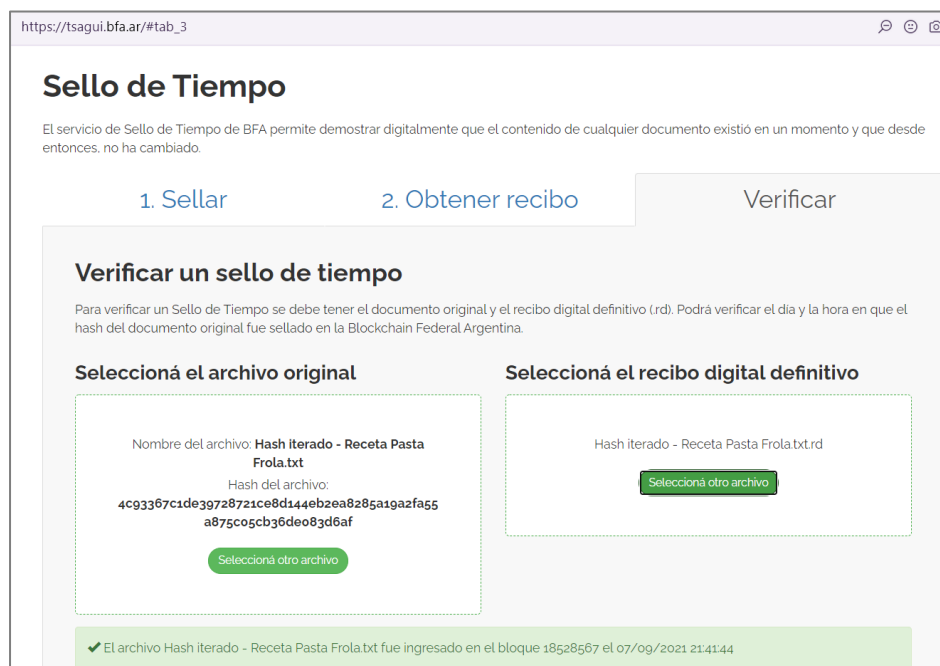


10) Marca de tiempo definitiva generada



b. Control judicial ante un eventual litigio

1) Verificación en BFA de la existencia de la oportuna registración del archivo que contiene el hash iterado del documento del presunto secreto comercial



2) Control sobre el contenido del archivo

Se reproducirían los pasos realizados oportunamente por el software codificador. El programa debería proporcionar una herramienta para realizar la tarea incorporando el archivo de hoja de ruta ya que serían recomendables números elevados de iteraciones lo que haría inviable el trabajo manual del operador.

Ejemplo de hoja de ruta en base al ejemplo que antecede:

1) SHA512/256

- Input

Ingredientes de la torta Pasta Frola de Doña Marta S.A. (10 raciones): 125 gr. manteca de cabra, 125 gr. azúcar negra, 5 huevos de codorniz, esencia de vainilla extraído de orquídeas cubanas, ralladura de 1/2 limón, 250 gr. harina leudante, 600 gr. dulce de membrillo, 10 gr. de esencia de banana, 10 gr. de esencia de frutos rojos.

- Output

40552306c595b8e1b2dd192b0dec9e5807aa0659c8df2d56e397015ab28663b2

2) SHA3-256

- Input

40552306c595b8e1b2dd192b0dec9e5807aa0659c8df2d56e397015ab28663b2 - HG1DF65SD5F1D35F1SD35GFSF53A4F65EAC65SDHG6J4JRT5H4df4gdfg df53gdsf5gf5dg1fd53gdfg53df4g35dfg4fd53g4fdg31fg53fdg53dfgs53g1d35a1132sd1g3g1a351g53dfg15df3g1df53gdf5g1df5gdf5g151QF5EFFFDG53DF531GFD35G1DF35G1DF3G1DF3G1

- Output
fb3d15acf127f98af42942d29f0c0849e15c28882f41abdd0e5d2bc86fdd09f0
- 3) Keccak-256
- Input
fb3d15acf127f98af42942d29f0c0849e15c28882f41abdd0e5d2bc86fdd09f0 - DFH4GDagf
dhDSsffd4hdhdF5dfhdSFtfma56GSDDsfdgf5FdhfgmhSD5Fgfd4gfSa6515SG6SA6s6A1G51
g5d1h5d1515DF15DF51df5151SD5G1ED5V1S53D4HSGS654GS454G6RS65G1SDS6RT4Rd
fgs6fh5t1d53r1d35aaf35ef1sf5gwe51g35DF5kmvF5A4FS5F44DS5F4SD5
 - Output
c81a9d6761f71e2a98f9677d0ef937679c9c8c05a7342c9561226c401425a164

Referencias

- Bonneau, J. (2012). The science of guessing: analyzing an anonymized corpus of 70 million passwords. *Computer Laboratory - University of Cambridge*.
- Dyrhovden, S. (2017). Blockchain and Trade Secrets: A Match Made in Heaven? King's College London.
- Farina, J. M. (1991). Transferencia de Tecnología. *Revista de Derechos intelectuales*, 259.
- González G, P. (2015). Propuesta de un modelo para medir activos intangibles en empresas de software a partir de una herramienta multicriterio. *Estudios Gerenciales*, 31 (135), ISSN: 0123-5923, 191-201.
- Hayek, F. A. (1945). El Uso del Conocimiento en la Sociedad. *American Economic Review*, XXXV, N° 4, 519-30.
- HelmedHorror, U. (2015). Time required to brute-force crack a password depending on password entropy (strength) [OC]. [Reddit.com/r/dataisbeautiful/comments/322lbn/time_required_to_bruteforce_crack_a_password/](https://www.reddit.com/r/dataisbeautiful/comments/322lbn/time_required_to_bruteforce_crack_a_password/).
- Herrera, E., & Paludi, P. (2019). Jornadas sobre vinculación tecnológica y Protección del conocimiento en las universidades argentinas. *Programa Nacional de Gestión de la Propiedad Intelectual y de la Transferencia Tecnológica*.
- Lev, B. (2003). Remarks on the measurement, Valuation and Reporting of Intangible Federal Reserve Bank of New York. *Economic Policy Review*, 17-22.
- Morales Oñate, D. A. (2021). Implicaciones jurídicas del algoritmo: derechos intelectuales y privacidad. *Revista de Derecho*, ISSN 1390-2466, ISSN-e 2631-2484, N°. 35, 111-130.
- Nakamoto, S. (2008). Bitcoin: Un Sistema de Efectivo Electrónico Usuario-a-Usuario.
- Phox, M., Sherin, Z., Schmahmann, A., & Niles, A. (2017). Computational Security and the Economics of Password Hacking. 15.
- Posner, Landes, R., & William, M. (2003). La estructura económica de la ley de propiedad intelectual. *The Belknap Press of Harvard University Press*, 295.
- Raymond, E. S. (1999). The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary.
- Vazquez D'Alvaré, D. (2015). Los requisitos de patentabilidad: Conceptos generales. Los requisitos de patentabilidad en el procedimiento del Tratado de Cooperación en materia de Patentes (PCT). *OMPI/PCT/15/6*.

