Propiedad intelectual, apuntes y retrospectiva

Durante esta serie de artículos hemos ido viendo el valor de las propiedades intelectuales, los riesgos y el valor del proceso de auditoría. En este artículo pretendo sintetizar el trabajo realizado en los anteriores. A la vez que complementar algunas cuestiones que creo que pude pasar por alto.

El viaje comenzó identificando que consideramos propiedad intelectual y cuales son las diferentes formas en las que se manifiesta. Hablamos de que estos activos en la era digital y de servicios en la que nos encontramos son los que más valor y diferenciación aportan a las empresas. Identificamos, patentes, modelos de utilidad, derechos de autor, propiedad industrial, *trademarks*, imagen comercial, secretos comerciales, … También vimos que la ley protege especialmente aquellas que se pueden vender, pero nosotros debemos considerar un espectro más amplio e incluir toda aquella información que sea relevante para la empresa.

En el siguiente artículo seguimos indagando las categorías que contemplaban las leyes, que sí y que no se puede proteger con las herramientas legales del estado. Y mencionamos algunos marcos y estándares dirigidos a las propiedades intelectuales. Es interesante descubrir que no aparecen los típicos marcos que aparecen casi en cualquier otro tema de auditoría, sino que en este ámbito el referente es WIPO (*World Intellectual Property Organization*). Intuyo que esto se debe a que la gestión de las propiedades intelectuales está íntimamente relacionada con la seguridad en general. Así que supongo que podría añadir a aquel artículo la ISO 27000 a la lista de marcos.

Después pasamos a identificar los riesgos a los que se enfrenta cualquier organización en los que a propiedades

intelectuales se refiere. En este apartado identificamos 3 grandes categorías en las que podíamos incluir un montón de riesgos: *olvidarse de las PI*, *perder o que nos roben PI* e *infringir las PI de otros*. Me aventuro a decir que las más comunes son la primera y última categoría. Entiendo que la segunda es una preocupación más dirigida a grandes empresas multinacionales que manejan cientos de propiedades intelectuales en equipos enormes y las diferencias en tecnología o procesos son importantísimas.

Y en el último post se esquematiza el proceso de una auditoría y los controles que se podrían implantar en una organización para securizar la PI. El proceso de la auditoría comienza por identificar todas las propiedades intelectuales de las que dispone la organización, haciendo un inventario, identificando a la gente con acceso a las PI, e investigando otras fuentes que nos digan que cosas hay a nombre de la empresa, como los dominios de internet que tenga comprados. Después hay que comprobar quienes tienen acceso a la información sensible y que no se este haciendo un uso indebido de alguna PI de terceros.

Como ya he dicho la mayoría de estos controles pertenecen a la seguridad. Desde el punto de vista TI los controles generales y de personas se extienden también al mundo digital. Por lo que además debemos aplicar los controles de segregación de funciones, controles de acceso, registro de actividad, etc. a todos los sistemas de información que contengan información sensible, es decir, prácticamente todos. Particularmente en cuanto a las personas y terceros que puedan tener acceso los contratos de confidencialidad son indispensables.

En conclusión, la propiedad intelectual tiene un valor tremendo en cualquier organización, es lo que diferencia y más valor aporta. Afortunadamente existen herramientas legales que ayudan a proteger estos. (Des)afortunadamente, las empresas tienen que gestionar estos activos de manera adecuada y para ello necesitan el servicio que prestan los auditores y

consultores. Para esto lo esencial es identificar todas aquellas propiedades intelectuales que sean de valor para la empresa y protegerlas o sacarles el mayor partido posible.

Enlaces

[1] <<Propiedad intelectual, introducción y contexto>>, PublicaTIC, https://blogs.deusto.es/master-informatica/propiedad-intelectual-introduccion-y-contexto/

[2] <<Propiedad intelectual, relevancia>>, PublicaTIC, https://blogs.deusto.es/master-informatica/propiedad-intelectual-relevancia/

[3] <<Propiedad intelectual, riesgos>>, PublicaTIC, https://blogs.deusto.es/master-informatica/propiedad-intelectual-riesgos/

[4] <<Propiedad intelectual, controles y auditoria>>, PublicaTIC, https://blogs.deusto.es/master-informatica/propiedad-intelectual-controles-y-auditoria/

Propiedad intelectual, controles y auditoría

En el artículo anterior comentamos los riesgos a los que se exponen las empresas en cuanto a la propiedad intelectual. Identificamos 3 categorías: No olvidarnos de nuestra PI, que no nos roben nuestra PI y no infringir la PI de otros.

Para cada uno de estos posibles riesgos existen distintos

controles que podemos implementar para reducir la probabilidad de que ocurran. Asegurando de esta manera el correcto funcionamiento de la empresa y asegurando el uso y aprovechamiento de estos activos tan importantes.

Empecemos por lo más básico, tener controlado cuales son las PI de las que disponemos. Para evitar que se olvide cuales son las PI de las que dispone la organización hay algunos controles obvios que hay que implementar.

Como auditores nuestro trabajo comienza por *identificar las propiedades intelectuales*. Hay muchísimas maneras de descubrir toda la información que puede ser de importancia para la organización. Algunas de las técnicas en las que podemos pensar son:

- Realizar un inventario periódico de las PI de las que dispone la empresa.
- Identificación de la documentación relacionada con las PPII.
- Clasificación de las PI. Según tipo, importancia, …
- Descubrir e investigar licencias a nombre de la empresa.
- Validar que las licencias de PPII que hace uso la empresa son válidas.
- Investigar acuerdos con terceros sobre PI.
- Procedimientos investigación y flujos de trabajo bien documentados.
- Identificación de los principales generadores de PI. Seguramente el equipo de investigación o desarrollo.
- Análisis de repositorios de documentos.
- Descubrir nombres de dominios de internet relacionados con la organización.
- Si la organización opera internacionalmente, análisis del estado de las patentes, marcas, … en todos los países en los que opera.

Además queremos evitar perder estos datos por lo que necesitaremos establecer controles que eviten la pérdida de

información. Aquí entrarían varias técnicas de *seguridad de la información*, como copias de seguridad o replicación de documentos.

Una vez tenemos identificado aquello que queremos proteger nos fijamos en los controles que nos ayudan a evitar que manos u ojos indeseados se hagan con nuestros activos. Esta parte se solapa mucho con la gestión de la *seguridad.*

- Controles de acceso.
- Restricciones de acceso.
- Segregación de responsabilidades.
- Identificación de usuarios.
- Registro de actividad.
- Ciberseguridad.
- Concienciación de los empleados acerca de la PI.
- Investigación de los contactos y pasado de los empleados.
- Contratos de confidencialidad.
- Marcar como confidencial la información o documentos para que no haya dudas.
- Expresar claramente en los contratos de los empleados la confidencialidad y las consecuencias en caso de incumplimiento.

Y por otro lado, debemos asegurar que las propiedades intelectuales están adecuadamente protegidas haciendo uso adecuado de las *herramientas legales* de las que se dispone.

- Patentes
- Modelos de utilidad
- *Copyright*
- Marcas
- Diseños industriales
- Derechos de autor
- Secretos comerciales
- Seguros
- …

También debemos asegurar que la estrategia en cuanto a la PI se alinea con la estrategia de la empresa.

El último problema al que nos podemos enfrentar es a estar infringiendo la propiedad intelectual de terceros. En estos casos nuestro trabajo como auditores es reportarlo a la dirección para que tomen las acciones necesarias para resolver el problema.

Referencias

[1] <<Intellectual Property Process Audit Report>>, KnowleadgeLeader, consultado el 20/11/2020, https://www.knowledgeleader.com/knowledgeleader/content.nsf/web+content/au/ditreportintellectualpropertyprocess

[2] <<Intellectual Property Management and Auditing>>, consultado el 20/11/2020, https://www.innovation-asset.com/the-audit-and-management-of-intellectual-property

[3] <<IP Audit Check-list>>, consultado el 21/11/2020, https://www.southeastasia-iprhelpdesk.eu/sites/default/files/publications/EN_Audit.pdf

[4] <<Law and Internal Auditing>>, consultado el 21/11/2020, https://na.theiia.org/training/Public%20Documents/Intellectual%20Property.pdf

[5] <<Fact Sheet IP audit: Uncovering the potential of your business>>, consultado el 22/11/2020, https://www.iprhelpdesk.eu/sites/default/files/newsdocuments/Fact-Sheet-IP-Audit-Uncovering-Potential-Your-Business-EN.pdf

Propiedad intelectual, Riesgos

Riesgos, riesgos, riesgos, … De eso va la auditoría, no?

Hemos visto durante los primeros artículos la enorme importancia que tienen las propiedades intelectuales. Cómo son la base sobre la cual las empresas se apoyan, las distingue y las hace competitivas frente al resto. Es lo que marca la diferencia entre los mejores y el resto.

Como todo lo que es valioso, a las empresas les interesa protegerlo y cuidarlo. Las empresas u organizaciones al estar compuestas por personas los riesgos de los que se debe proteger a las propiedades intelectuales se pueden distribuir en dos categorías básicas: Que no la roben y que no se pierda.

Un riesgo muy habitual en organizaciones de cualquier tamaño es la infrautilización de alguna PI. Es común encontrarse que se está pagando un servicio al que no se le está dando uso; perder documentos al marcharse la gente del equipo; olvidar donde se encuentran ciertos documentos; olvidar que se tiene un dominio web porque no se le da uso; no hacer uso de las herramientas legales para proteger las PI; o, directamente, no saber que se tiene alguna PI.

Estos son riesgos internos de la organización. Son cuestiones que normalmente perjudican a la organización por no aprovechar bien sus recursos, pero el impacto suele ser pequeño en comparación con los riesgos externos.

Los riesgos externos de la PI es que sea robada. Hablamos de casos en los que la competencia logra información delicada o consigue cierta tecnología eliminando la ventaja competitiva con la que contaba la primera empresa. Cuando se trata de información delicada en vez de tecnología esta puede ser usada para adelantarse y perjudicar las estrategia de la primera

empresa.

La mayoría de los robos no se suelen dar mediante planes muy sofisticados, basta con que haya algún empleado descontento con acceso a los documentos de interés.

Cuanto más puntera y más grande sea una empresa más cuidado tiene que tener una empresa. A estos niveles la competencia y los participantes en estas artimañas empiezan a tener escala internacional, países que para mejorar su competitividad usan recursos del país para robar tecnología y otros datos a grandes organizaciones para potenciar empresas del país.

Aunque parezca de película no es tan raro encontrarse noticias como la siguiente [1] en la que grupos de hackers organizados por un gobierno se dedican a robar información y tecnología a empresas para tener esa tecnología en el país sin tener que adherirse a las leyes internacionales y de esa manera poder competir con potencias extranjeras.

Las cuestiones que dificultan el buen estado de las PI dentro de una organización son principalmente el tamaño de esta. Empresas grandes, internacionales, se encuentran con una complejidad enorme a la hora de gestionar sus PIs y las PIs de las que hacen uso. Cada país tiene leyes ligeramente distintas en cuanto a las PIs, y mantener el control y gestionar las interacciones de todas estas leyes se puede volver infernal.

Lo más habitual es que cuanto mayor es la organización, mayor sea el número de propiedades intelectuales que maneja. Además de tener más PIs, disponer de una plantilla mucho mayor aumenta la superficie de ataque considerablemente. Sinceramente la mayor fuente de riesgos en las organizaciones son las personas.

Por ejemplo, pensemos en una empresa que se dedica a la producción de software. El equipo de desarrollo tendrá seguramente todo el código y conocimientos en un repositorio privado al que solo unas pocas personas tengan acceso. De esta

manera controlar quien puede y no puede acceder a esa información es sencillo.

Sin embargo, si la PI de una empresa son los procesos, contenido creativo, planos, o documentación que no está en un lugar controlado, sino que la información está a la vista o en los portátiles personales de los empleados, que no están gestionados por la empresa, cuanto más difuso sea qué constituye una PI más complicado es gestionar y protegerla.

A esto hay que añadir que cuanta más gente tenga acceso a la información más difícil es protegerla. La probabilidad de empleados descontentos o poco concienciados aumenta. Y las personas son fácilmente influenciables, basta con un poco de ingeniería social para robar información privilegiada, no hace falta ni que el ataque sea especialmente sofisticado. El sistema es tan seguro como el eslabón más débil.

La explosión combinatoria del número de empleados, gente con acceso a la PI y la dificultad para definir y limitar el acceso a las PI hace que la superficie de ataque y consecuentemente el riesgo que corren las PI sea enorme.

Referencias

[1] <<An Unfair Advantage: Confronting Organized Intellectual Property Theft>>, ASIS, consultado el 01/11/2020 https://www.asisonline.org/security-management-magazine/articles/2020/07/an-unfair-advantage-confronting-organized-intellectual-property-theft/

[2] <<Intellectual Property Protection High Tech’s Crown Jewels>>, ISACA, vol 3 (2018): 39-44

[3] <<Intellectual Property Theft/Piracy>>, FBI, consultado el 02/11/2020 https://www.fbi.gov/investigate/white-collar-crime/piracy-ip-theft

[4] <<Five insights on cyberattacks and intellectual property>>, Deloitte, consultado el 02/11/2020 https://www2.deloitte.com/us/en/pages/advisory/articles/five-insights-on-cyberattacks-and-intellectual-property.html

---

Propiedad intelectual, relevancia

En el post anterior hemos hablado sobre qué es la propiedad intelectual y algunas de las maneras mediante las cuales podemos proteger derechos que tenemos sobre estas. Es innegable el valor que aportan las PIs a las empresas. Es más, son los elementos que más valor aportan actualmente.

Es difícil cuantificar el valor de una PI, pero el valor de estas se vuelve muy claro cuando se realiza la venta de alguna de estas. Por ejemplo, fue muy sonado el desorbitado precio que pagó Disney por una de las sagas de películas más queridas de la historia. Star Wars se vendió por 4.050 millones de dólares. Un juego que seguro que también os suena se vendió por 2.500 millones de dólares. La marca Harry Potter, el mayor fenómeno literario de los últimos años, tiene un valor estimado de 25.000 millones de dólares.

En el mundo de la informática, empresas que se dediquen al desarrollo de software deben prestar mucha atención a las diferentes licencias que tienen las librerías, frameworks u otro software que utilicen. Algunas de estas licencias no son compatibles entre sí y es posible que haya grupos de herramientas que no se puedan usar conjuntamente en el mismo proyecto, o que en caso de hacerlo nos exijan licenciarlo de una manera específica.

Hay que tener mucho cuidado también con cómo son esas licencias. Es posible que partes de una tecnología tengan una licencia y otras partes tengan otra distinta. Por ejemplo, es bastante sonado el caso Google vs Oracle [4], en el que Google intenta defenderse de de una acusación de violación de copyrights por haber usado la librería estandar de Java para Android. En este caso Oracle, Sun en su día, promocionan el lenguaje como abierto o libre, sin embargo, la librería estándar de Java está protegida por copyright. Esto de licenciar de manera distinta partes de una tecnología hace muy confuso entender si se está haciendo un uso correcto del código o no. Lo mejor en estos casos es conocer bastante bien la legislación vigente. En resumidas cuentas se puede decir que la cuestión que va a determinar el tribunal superior de justicia de los Estados Unidos es si las APIs se pueden copiar o no.

Si bien su relevancia es cada vez mayor, no he encontrado muchos marcos, guías o estándares para gestionarlas. Tenemos algunas ISOs [3] y un montón de estándares por la WIPO (World Intellectual Property Organization) [2]. Casi todo gira entorno a identificar toda la propiedad intelectual que haya en una empresa, porque es bastante complicado saber qué se tiene, y sobre cómo sacarle valor a esta.

Una parte importante de la auditoría es conocer la legislación. Como en todos los casos, este es un tema complicado. Hay muchos organismos que se encargan de gestionar los derechos de las Propiedades Intelectuales. Varían entre países y en ocasiones pueden ser contradictorias. Para simplificar un poco el tema vamos a echarle un vistazo a la ley española a ver qué dice sobre la propiedad intelectual [1].

Los primero artículos definen qué es la propiedad intelectual y qué derechos se le atribuyen a su o sus creadores, quienes se les considera autores de una obra y, las diferentes clasificaciones básicas de tipos de propiedades intelectuales.

Es especialmente interesante para nosotros los informáticos y programadores el Título VII, del artículo 95 al 105 excluido, en los que se tratan los programas de ordenador en particular. Ahí se nos dice que tanto el software como toda la documentación técnica, manuales de usuario y otros documentos asociados al software están protegidos por la ley de propiedad intelectual. También debemos conocer en qué casos podemos realizar ingeniería inversa de un código de forma legítima. Podría resumirse en que solo se puede realizar si queremos crear otro programa que vaya a interoperar con el primero. Recomiendo que le echéis un vistazo al menos a esta sección que trata los programas de ordenador en particular. Una pregunta que me hago es, ¿cómo se deben interpretar estas leyes ahora que la mayoría del software está transicionando hacia un modelo de servicio?

Todo este embrollo legal es complicado, hay múltiples legislaciones que no tienen porque seguir las mismas directrices o clasificar las PI de la misma manera. Pero tan complicado como esto es identificar todas las propiedades intelectuales de las que dispone una empresa y el valor que estas aportan, identificar los riesgos y controlar las PI que maneja.

Referencias

[1] <<BOE>> núm. 97, de 22/04/1996.
Entrada en vigor:23/04/1996
Departamento: Ministerio de Cultura
Referencia: BOE-A-1996-8930
Permalink ELI: https://www.boe.es/eli/es/rdlg/1996/04/12/1/con

[2] <<List of WIPO Standards, Recommendations and Guidelines>>, consultado 20/10/2020
https://www.wipo.int/standards/en/part_03_standards.html

[3] <<03.140 PATENTS. INTELLECTUAL PROPERTY>>, consultado el 20/10/2020

https://www.iso.org/ics/03.140/x/

[4] << Oracle vs Google: en juego el derecho de autor y el desarrollo de software>>, consultado el 20/10/2020 https://www.brandsprotectionnews.com/oracle-vs-google-en-juego-el-derecho-de-autor-y-el-desarrollo-de-software/

Propiedad intelectual, introducción y contexto

La propiedad intelectual es uno de los mayores activos de las empresas actuales. La edad de la información se caracteriza principalmente por otorgar mucho valor a los datos y las ideas que surgen de las personas. Estos elementos intangibles incluyen: dibujos, formas, nombres, imágenes, obras literarias y artísticas, símbolos, modelos, fórmulas, etc. Manejar y controlar el uso y conocimiento de estas es muy complicado. ¿Cómo controlas algo que no se puede tocar?

Para proteger la explotación de estos recursos existen leyes que categorizan y otorgan ciertos derechos según el tipo de propiedad intelectual. Estas leyes varían según el organismo gubernamental. En general nos podemos encontrar con los siguientes [1]:

- Patentes: El gobierno otorga el derecho de explotación exclusiva de un producto, generando un monopolio artificial para la empresa o creador de la invención, a cambio de la divulgación del producto.
- Modelo de utilidad: Es un derecho que otorga el estado a una invención. Es muy similar a una patente, con la diferencia de que un modelo de utilidad no tiene que ser tan “novedoso” u “original” como una patente. Versiones, actualizaciones o extensiones de un producto que suponen una ventaja competitiva entran en esta categoría. A cambio la exclusividad sobre el producto es menor que en la patente.
- Derechos de autor: Son unos derechos que obtiene el autor de una obra artística, científica o didáctica, por el simple hecho de ser el autor. Aquí podemos

encontrarnos los derechos de copia (copyright) que especifican quién y cómo puede realizar copias de las obras. Expiran o pasan al dominio público después de muchos años. En la mayoría de los países ocurre pasados los 50 años, en muchas partes de Europa son 70 años y en México 100.

- Propiedad industrial: Una propiedad industrial puede ser una marca, símbolo, patente, dibujo o diseño industrial. Sobre estas el estado otorga el derecho decidir quién puede utilizar la invención, diseño o signo distintivo y a prohibir que un tercero lo haga.
- Marcas registradas o *trademarks*: Estas están compuestos por formas, dibujos, símbolos, iconos, logotipos, música, (olores en algunos países). Son elementos principalmente gráficos que un consumidor asocia a una marca. Y las instituciones gubernamentales otorgan a su titular, la posibilidad de autorizar o prohibir el uso de la misma a terceras personas.

También hay otros tipos de PI que son curiosas y/o destacables:

- Variedades vegetales: Como se puede intuir por el nombre, este tipo de propiedad otorga derechos de de uso comercial sobre una variedad de plantas.
- Imagen comercial: La imagen que proyecta una marca o empresa. La sensación, estilo, *feeling* que percibe un cliente también se puede considerar propiedad intelectual. Pero esta no está protegida por ninguna ley y, el cuidado de esta es puramente de la empresa. Tiene mucho valor, se puede dañar fácilmente y tiene mucho impacto en los clientes.
- Secreto comercial: Son fórmulas, prácticas, procesos, diseños, instrumentos, patrones o compilaciones de información que no se conoce o no se puede determinar de manera razonable, mediante la cual una empresa puede obtener una ventaja económica. Estos conocimientos se

podrían proteger mediante una patente pero en ese caso se deben publicar los detalles y en unos 20 años se perdería la exclusividad.

Cómo gestionar y controlar las ideas y la información es difícil, hay que tener localizada e identificada toda aquella información que sea relevante para la empresa. Lo que un trabajador aprende durante su jornada laboral, ¿le pertenece a él o a la empresa? Si este empleado se marcha a la competencia, ¿qué les puede contar? ¿Cómo de parecidos tienen que ser dos cosas para considerarse plagio? ¿Cuánto para que sea un producto distinto? ¿Cómo estimar cuánto vale una PI?

Si bien las leyes se centran especialmente en productos que se pueden vender las propiedades intelectuales también incluyen documentos internos de las empresas como las buenas prácticas, formularios u hojas de procesos entre otros. Todo el conocimiento implícito de una organización procesos, organización, experiencia y habilidades de los empleados es conocimiento y puede suponer un valor muy elevado.

Para que nos hagamos una idea del volumen que suponen las propiedades intelectuales durante el año 2018 en España se realizaron más de 80.000 solicitudes. Más de 50.000 de marcas, 18.000 diseños industriales, 12.000 nombres comerciales y 5.000 modelos de utilidad, patentes y expedientes [2].

[1] <<¿Qué es la propiedad intelectual?>>, OMPI, consultado el 30/09/2020, https://www.wipo.int/edocs/pubdocs/es/intproperty/450/wipo_pub_450.pdf

[2] <<La OEMP en cifras>>, OEMP, consultado el 02/10/2020, https://www.oepm.es/export/sites/oepm/comun/documentos_relacionados/Publicaciones/Folletos/La_OEPM_en_Cifras_2018.pdf

Cloud Computing, riesgos a considerar

En este post, y tal como adelanté en el anterior, me voy a dedicar a ofrecer una visión general sobre los **riesgos** asociados al Cloud Computing.

Lo primero que debemos entender, si queremos listar o categorizar los riesgos asociados a este paradigma, es que **dependiendo del modelo** de servicio o del modelo de despliegue que elijamos (las diferencias quedaron claras en los anteriores posts) podemos encontrarnos con **diferentes tipos de riesgos** [1].

Por ejemplo, no es lo mismo desarrollar una nube privada y mantener todo dentro de nuestra organización que contratar a un proveedor de servicios y externalizar nuestra capacidad de cómputo y almacenamiento a una nube pública. Igualmente, no podemos considerar que existen los mismos riesgos si estamos consumiendo un modelo de servicio PaaS (Platform as a Service) que SaaS (Software as a Service). En el primero solo tenemos fuera de la empresa el hardware y los sistemas de soporte (las aplicaciones son nuestras, o al menos las ponemos nosotros) y en el segundo, no tenemos dentro de casa ni un -maldito- trozo de código [2]. ¿Se ve a lo que me refiero?

Y si a eso le añadimos que lo normal no es adoptar un único modelo de servicio o un único modelo de despliegue (por ejemplo, la nube híbrida es la combinación de los dos modelos de despliegue principales junto a soluciones on-premise) estamos ante un **escenario de riesgos complejo** de analizar. ¡No sé ni por donde se va a desmontar mi negocio!

Pero bueno, no todo es tan negativo. La industria se ha

preocupado por este tema y ha solucionado parte de la complejidad. De hecho, hoy en día, a 2019, contamos con **categorizaciones** bastante **exhaustivas** y tenemos a nuestra disposición **marcos de trabajo** que, en mayor o menor medida, nos pueden ayudar a detectar y mitigar los riesgos asociados a este paradigma de manera metódica.

Una categorización que considero suficientemente completa es la que he leído en [1]. En este artículo, se listan **seis esferas o áreas de riesgo** que puede llegar a presentar el Cloud. Voy a tratar de resumirlas, pero recomiendo leer el artículo original:

- **Autenticación.** Todo lo relativo al control y el aseguramiento de la correcta autenticación de usuarios. El Cloud Computing presenta retos en este ámbito, o mejor dicho, magnifica los retos que ya existían en modelos de computación tradicionales. La confidencialidad de la información está en el punto de mira cuando todos nuestros sistemas residen en la nube. Sobre todo, si residen en la nube pública, cuya gestión y buen gobierno dependen de un tercero.
- **Seguridad y privacidad.** Otro frente es garantizar que los datos con lo que se opera en la nube se mantienen seguros y privados. Y de nuevo, los riesgos relativos a esta esfera tienen que ver precisamente con la irrupción de un nuevo agente: el proveedor de servicios. Cuando se contrata a un proveedor, se debe asegurar que este sigue los estándares y controles oportunos, o que tiene las certificaciones necesarias.
- **Compatibilidad con sistemas internos.** Una serie de riesgos asociados al Cloud Computing tienen que ver con que la mayoría de compañías no pueden migrar todos sus sistemas a la nube. Por ejemplo, aquellos que son parte esencial de la estrategia de la organización, que son considerados propiedad intelectual o que son tan diversos que no son compatibles con la infraestructura

de ningún proveedor. Existen dificultades y peligros en la interoperabilidad de sistemas, así como en la integridad de los datos que manejan. De nuevo, debido al factor de externalización.

- **Disponibilidad.** Existen también riesgos relativos a la disponibilidad de los sistemas que residen en la nube. Hoy en día, dicha disponibilidad debe ser garantizada en todo momento, ya que los sistemas han comenzado a ser parte esencial de cualquier organización. En la nube, dada la complejidad del paradigma, se deben realizar controles, mecanismos y procedimientos de redundancia y testing muy exhaustivos, lo que expone a una organización a mayores costes y amenazas.
- **Continuidad de negocio.** Si una organización adopta el Cloud (principalmente si hace uso de nubes públicas), está delegando su continuidad de negocio a un tercero: el proveedor de servicios. Si el proveedor sufre un ataque o una catástrofe, la empresa cliente también.
- **Propiedad intelectual y aspectos legales.** Hay riesgos asociados con la dificultad de decidir quién posee realmente los datos en un entorno Cloud. ¿El proveedor? ¿El cliente? Las complicaciones legales entorno a este tema deben ser un riesgo a considerar. Asimismo, el Cloud Computing presenta riesgos a nivel de cumplimiento. Por ejemplo, leyes o reglamentos tales como el GDPR obligan a las empresas a considerar aspectos relativos a la protección de datos personales. Su incumplimiento puede acarrear multas millonarias. Si el proveedor no las cumple, el cliente tampoco.

Otra categorización que he encontrado interesante es la presente en [3] (apartado: *Cloud Adoption – key risks and how to mitigate them*), más centrada en las preguntas que debe realizarse toda organización que quiere migrar su infraestructura TI al Cloud. No obstante, no vamos a entrar en más detalles. La categorización anterior ya nos da una visión suficiente para hacernos una idea de los riesgos que presenta

el Cloud. De hecho, podemos observar que la mayoría de riesgos tienen que ver con **dos factores**: la **complejidad inherente al paradigma** y la puesta en escena de un nuevo agente, el **proveedor de servicios**.

Visto los tipos de riesgos, puede ser buena idea priorizarlos. Y por supuesto, esta **priorización** debe estar **ligada a la naturaleza y objetivos de nuestra organización**. Si somos una empresa de servicios, póngase Netflix, debemos considerar la disponibilidad y la continuidad del negocio como factores de máxima prioridad. Sin embargo, si somos una empresa farmacéutica con un alto número de patentes, quizá sea más prioritario para nosotros los mecanismos de autenticación de nuestros sistemas y la privacidad y seguridad de nuestros datos, así como los aspectos relativos a propiedad intelectual. La disponibilidad quizá no sea crítica, o al menos no en la misma medida. Con esto quiero decir, que la priorización debe ser relativa a nuestras necesidades y no debemos caer en el error de intentar priorizar todos los riesgos de la misma manera.

A modo de anécdota, y para que veáis que esto no es palabrería, deciros que hace apenas unas semanas, Amazon Web Services (AWS), probablemente el mayor proveedor de servicios Cloud, sufrió un **ataque DDoS** que tumbó durante 8 horas muchos de sus servicios (EC2, RDS, ELB…) [4]. Los clientes que dependían de dichos servicios, paralizados. Al final, si quiero atacar a una empresa, puedo atacar directamente a su proveedor de servicios Cloud. ¡Easy peasy! Por ello, es esencial elegir al proveedor adecuado.

Pero como decíamos con anterioridad, existen marcos de trabajo que nos van a permitir evitar este tipo de escenarios. Si queremos cubrir, o al menos considerar, todos los posibles riesgos asociados al Cloud (imaginad que sois el encargado de la gestión de riesgos TI en vuestra empresa), necesitamos herramientas, guías y muchas tablas. Sí, muchas tablas, si no queremos morir en el intento. Con esto quiero decir que no se debe reinventar la rueda. Podemos apoyarnos en marcos de trabajo que incluyan todos los controles y procedimientos oportunos a considerar. Y para nuestra suerte, existen muchos de ellos [5]. Además, ya existen otro tipo de esfuerzos (documentación, pautas, artículos) para permitir a los profesionales centrar el tiro [6].

En el siguiente post, trataremos de profundizar en dicho ámbito: los **controles** y **marcos de trabajo** asociados al Cloud Computing.

¡Gracias por leerme y nos vemos en el siguiente post!

[1] «Risk Landscape of Cloud Computing», ISACA, acceso el 2 de noviembre de 2019, https://www.isaca.org/Journal/archives/2010/Volume-1/Pages/Risk-Landscape-of-Cloud-Computing1.aspx

[2] «Entendiendo la nube: el significado de SaaS, PaaS y IaaS», Genbeta, acceso el 2 de noviembre de 2019, https://www.genbeta.com/desarrollo/entendiendo-la-nube-el-significado-de-saas-paas-y-iaas

[3] «Moving to the cloud – key considerations», KPMG, acceso el 2 de noviembre de 2019, https://assets.kpmg/content/dam/kpmg/pdf/2016/04/moving-to-the-cloud-key-risk-considerations.pdf

[4] «AWS customers hit by eight hours DDoS attack», Info Security, acceso el 2 de noviembre de 2019, https://www.infosecurity-magazine.com/news/aws-customers-hit-by-eighthour-ddos/

[5] Alosaimi Rana, Alnuem Mohammad. «Risk Management Frameworks for Cloud Computing: a critical review», *International Journal of Computer Science & Information Technology* 8 4 (2016), acceso el 2 de noviembre de 2019, https://pdfs.semanticscholar.org/6c88/c8f09a734317a611d4bcc566225907cbda31.pdf

[6] «Managing Cloud Risk: Top Considerations for Business Leaders», ISACA, acceso el 2 de noviembre de 2019, https://www.isaca.org/Journal/archives/2016/volume-4/Pages/managing-cloud-risk.aspx

¿Cómo nos afecta la nueva ley de copyright?

En este último blog os voy traer una noticia reciente que me ha parecido bastante interesante relacionada con la propiedad intelectual y que nos afecta a todos, tanto como consumidores como creadores de contenido en Internet.

Hace unos meses saltaba la noticia cuando el parlamento europeo aprobaba una reforma de la ley de copyright actual. Los artículos más polémicos han sido el 11 y 13 que ponen en peligro la libertad de expresión y el acceso a la información como lo conocemos hoy en día. [1]

Con el artículo 11 se pretende proteger a los medios de comunicación y creadores de contenido. Dentro de este artículo se contempla los siguientes puntos:

- Los usuarios de redes sociales u otras plataformas de Internet no podrán compartir fragmentos de noticias y ningún tipo de contenido con derechos de autor durante 20 años contando desde la creación del contenido. [2]
- Se contempla el pago de licencias para la utilización de fragmentos protegidos por derechos de autor. [2]

Por otra parte, el artículo 13 propone regular el uso de contenidos protegidos por parte de proveedores de servicios de la sociedad de la información como pueden ser redes sociales, motores de búsqueda como Google o plataformas de contenido como YouTube. [2] Concretamente se contemplan los siguientes puntos:

- La responsabilidad de los contenidos pasa a ser de quien los hospeda, no del que los produce. [3]

- Se contempla también el pago de licencias a los propietarios de los derechos para permitir el uso de su contenido en la plataforma. [2]

Con esta medida plataformas como YouTube serán responsables de los vídeos subidos y deberán implementar sistemas que se encargan de detectar y eliminar todo aquel contenido que se suba a la plataforma y este protegido por derechos de autor. [3]

Con la instalación de estos sistemas surge un nuevo problema ya que no son del todo fiables. Si tomamos como ejemplo YouTube, su sistema hace lo siguiente: [4]

1. Los propietarios de los derechos envían a YouTube archivos sonoros y visuales sobre sus contenidos.
2. YouTube crea una huella digital del contenido y la almacena en su base de datos.
3. Un sistema se encarga de comparar los vídeos subidos con las huellas almacenadas con el objetivo de detectar si se ha utilizado contenido protegido. En caso positivo el contenido será eliminado inmediatamente.

El problema de estos algoritmos es que no son capaces de entender muy bien el contexto. Por ejemplo, si una persona sube un cover de una canción protegida por derechos de autor, el sistema es probable que detecte que está incumpliendo la propiedad intelectual del autor de la canción, ya que puede pensar que la está cantando el propio autor. Evidentemente un cover es totalmente legal, aunque se pueden dar casos de vídeos con un cover que quedarían eliminados por este motivo. Del mismo modo, también es posible que el algoritmo no detecte correctamente los casos realmente ilegales. [5]

Hasta ahora, la baja fiabilidad de estos sistemas no era problema para las plataformas como YouTube ya que no eran responsables del contenido subido por terceros y hay muchas otras plataformas que ni siquiera utilizan este tipo de

sistemas. Con la llegada de la nueva ley, todas las plataformas se van a ver obligadas a implementar sistemas mejorados de este tipo para evitar que se suba ningún contenido protegido. Estos algoritmos mejorados probablemente sean capaces de detectar al 100% los casos de infringimiento de la propiedad intelectual. Sin embargo, el número de veces que el sistema detecta contenido legal como ilegal también aumentará.

Evidentemente, en los casos que el algoritmo detecte como ilegal un contenido totalmente legal, se puede enviar una reclamación a la plataforma (si tiene los recursos y cuenta con este tipo de servicios) para demostrar que el contenido es legal. Esto implica más trabajo y recursos tanto para la plataforma como para los usuarios. Al fin y al cabo, ¿quién va a perder el tiempo enviando una reclamación para intentar recuperar un "meme" que publicó en Twitter por ejemplo? Y en caso de hacerlo, lo más probable es que se tarde horas o incluso días en poder tener tu contenido publicado de nuevo cuando ya probablemente no tenga ningún sentido.

Aparte de los propios usuarios, los principales perjudicados de todo esto serían las pequeñas plataformas que no cuentan con los recursos económicos necesarios para poner en marcha sistemas de monitorización que permitan comprobar que contenido infringe la ley y cuál no, por lo que probablemente tengan que cerrar. [3]

En definitiva, la nueva ley de copyright propone un aumento de la persecución de los delitos contra la propiedad intelectual, pero a mi parecer a un coste demasiado elevado, limitando nuestro derecho a la libertad de expresión en Internet.

Referencias:

[1]https://www.elconfidencial.com/tecnologia/2018-09-12/ley-copyright-parlamento-europeo-link-tax-upload-filter_1614760/

[2]https://www.adslzone.net/2018/09/12/articulos-11-13-directiva-derechos-autor/

[3]https://hipertextual.com/2018/07/articulo-13-reforma-derechos-autor-afecta-internet

[4]https://marketing4ecommerce.net/lo-debes-saber-la-politica-copyright-youtube/

[5]https://www.youtube.com/watch?v=ilEsBgbm7Fo

Controles en la propiedad intelectual

En el post anterior hable sobre los riesgos relacionados con la propiedad intelectual, concretamente sobre las fuentes de las que pueden surgir estos riesgos. El objetivo de este post es comentar los controles que un auditor tendría que implementar para tratar los diferentes tipos de riesgos.

Como mencionamos en el post anterior los riesgos pueden proceder de varias fuentes diferentes que suelen ser internas o externas a la organización. En función de esto aplicaremos unos controles u otros.

Entre los riesgos externos encontramos como más importantes (mayor probabilidad de que ocurran y mayor impacto para la empresa) los relacionados con temas de robo de información como puede ocurrir a través de ataques cibernéticos. Para tratar estos riesgos se recomienda usar los controles del estándar ISO 27002 [1] que se encarga de temas relacionados con la protección de datos. Algunos que podemos implementar

son:

- **10.1 Controles criptográficos:** asegurar el uso apropiado y efectivo para proteger la confidencialidad, autenticación y integridad de la información.
- **11.2.4 Mantenimiento de los equipos:** asegurarse de que los equipos tienen todas las ultimas actualizaciones para evitar brechas de seguridad.
- **12.2.1 Controles contra el código malicioso:** implementar controles para la detección, prevención y recuperación ante afectaciones de malware.
- **13.1 Gestión de la seguridad en las redes:** implantar estándares, directrices y procedimientos de seguridad técnicos para redes y herramientas de seguridad de red como IDS/IPS (detección y prevención de intrusiones).
- **13.2.1 Políticas y procedimientos de intercambio de información**: Deberían existir políticas, procedimientos y controles formales de transferencia para proteger la información que viaja a través del uso de todo tipo de instalaciones de comunicación.
- **15.1 Seguridad de la información en las relaciones con suministradores:** se debe controlar el acceso de terceros a los sistemas de información de la organización.

Otro conjunto de riesgos bastante importante son los que pueden provenir de dentro de la organización. Los riesgos más comunes aquí se producen simplemente por descuido y debido a la poca educación de los propios empleados en materia de seguridad. En este caso podemos implementar los siguientes controles del ISO 27002 [1]:

- **7.1.1 Investigación de antecedentes:** asegurarse al contratar que la persona contratada no es un posible espía de otra organización como el caso Ferrari comentado en el post anterior. [2]
- 7.2.2 Concienciación, **educación** y **capacitación** en

seguridad de la información: es importante presentar a los trabajadores una guía de buenas prácticas que deben lleven a cabo para asegurarnos la protección de la información.

- **9.1 Requisitos de negocio para el control de accesos:** establecer políticas de acceso a la información para evitar que nadie que no deba acceda a información confidencial.
- **11.1.2 Controles físicos de entrada:** evitar que personas no autorizadas accedan a lugares de acceso restringido.
- **11.2.9 Política de puesta de trabajo despejado y bloqueo de pantalla:** evita que personas sin acceso autorizado puedan visualizar en el ordenador información confidencial cuando el responsable del ordenador no está en su puesto de trabajo.
- **12.3 Copias de seguridad:** asegurar de tener siempre disponibles copias de la información en caso de que alguien borre de forma voluntaria o por accidente información.
- **12.6.2 Restricciones en la instalación del software:** evitar que los usuarios puedan instalar software malintencionado con el que puedan robar información.
- **13.2.4 Acuerdos de confidencialidad y secreto:** firmar acuerdos de confidencialidad con los empleados para evitar que puedan divulgar en el futuro información confidencial. En caso de hacerlo se podría denunciar.

Por último siempre es importante actuar de acuerdo a lo que la ley establece. En caso de empresas internacionales será necesario cumplir con la ley vigente en cada uno de los países en los que se opera, que en temas de propiedad intelectual suele variar de unos a otros. En caso de que el país está englobado dentro de una organización superior como puede ser la UE también será necesario tener en cuenta su legislación. Para este caso se pueden implementar los siguientes controles del punto 18.1 que se encarga de cumplir con los requisitos legales:

- **18.1.1 Identificación de la legislación aplicable: se deberá estar al corriente de todos los cambios que se pudieran producir en la legislación.**
- **18.1.2 Derechos de propiedad intelectual (DPI):** se deberían implementar procedimientos adecuados para garantizar el cumplimiento con los requisitos legislativos, normativos y contractuales relacionados con los derechos de propiedad intelectual y utilizar productos software originales.
- **18.1.5 Regulación de los controles criptográficos.**

Referencias:

[1]http://www.iso27000.es/

[2]https://lat.motorsport.com/f1/news/analisis-nace-un-nuevo-caso-de-spygate-en-la-f1/1594861/

Gestión de riesgos en propiedad intelectual

En este tercer post hablaré sobre los diferentes riesgos relacionados con la propiedad intelectual que pueden surgir dentro de un entorno empresarial. Un riesgo es la probabilidad de que un peligro ocurra y tengan consecuencias negativas para la organización. Para llevar a cabo una buena gestión de riesgos como auditores, es importante conocer las diferentes fuentes de las que pueden surgir para posteriormente listar una serie de riesgos potenciales y poder actuar en consecuencia para intentar evitarlos. Algunas de las fuentes más importantes a tener en cuenta a la hora de buscar riesgos

son [1]:

- **Dentro de la propia organización:** esta es una de las principales fuentes de riesgo. En algunos casos es debido a la falta de educación de los empleados de la empresa en cuanto a propiedad intelectual se refiere. En otros casos es debido a actos deliberados de los propios empleados. Este último caso es el más común y suele darse al abandonar un empleado la empresa. Esto es debido a que la propiedad intelectual está en muchas ocasiones en el propio conocimiento de la gente y cuando se va hay que tener en cuenta que se puede transmitir a gente externa a la organización. Si esto ocurre, se pueden tomar acciones legales como hizo Mercedes Benz hace unos años al enterarse de que un ex-ingeniero suyo estaba transmitiendo información confidencial a un equipo de la competencia que en este caso era Ferrari. [2]
- **Entidades cercanas a la organización:** en este apartado están incluidas todas aquellas entidades que tienen alguna relación con la organización pero que no pertenecen a la misma. Algunos ejemplos pueden ser distribuidores, proveedor, clientes, partners o personas subcontratadas. Todas estas entidades presentan un riesgo siempre y cuando tengan a acceso a aquello que esté protegido.
- **Competidores:** cualquier empresa que se encarga de manufacturar, crear y distribuir productos o servicios similares a nuestra empresa presenta un riesgo potencial. Un claro ejemplo de este tipo de riesgos está presente en la industria de los teléfonos móviles, donde hasta la simple forma de interactuar con la pantalla está protegido por patente en algunos países. Esto suele provocar múltiples demandas por infringir la propiedad intelectual entre empresas pioneras como sucedió hace unos años entre Apple y Samsung. [3]
- **“3rd parties” independientes:** en este apartado se

encuentran las conocidas entidades no practicantes (NPE) [4] que se dedican a amasar una gran cantidad de patentes pero no a llevar a cabo su desarrollo. El objetivo de la mayoría de estas entidades es buscar posibles infringimientos contra la propiedad intelectual y poner demandas para así poder obtener beneficios económicos. A este tipo de patentes se las conoce como "patentes troll". [5]

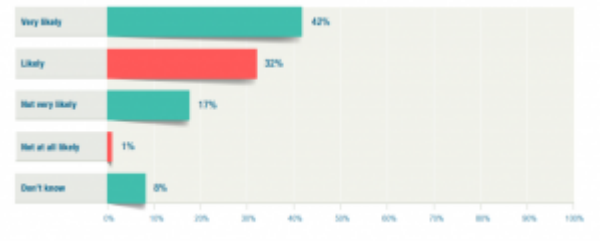
- **Entidades de gobierno:** es importante tener en cuenta que la ley de propiedad intelectual no es la misma en todos los países y que esta puede cambiar. Por lo tanto hay que estar al corriente de estos cambios para evitar posibles infracciones.
- **Entidades ilegales:** en este apartado se encuentra principalmente la piratería y los hackers informáticos. Un hacker puede ser una persona individual, una organización criminal o incluso entidades patrocinadas por un gobiernos con el objetivo de obtener información de rivales u otros países. Es un aspecto a tener bastante en cuenta ya que en España el 32 % de las empresas admite que ha sufrido algún ataque por hackers. [6] Como piratería nos referimos a toda copia falsa de un producto que tenga derechos de propiedad intelectual. Se estima que alrededor del 8% de productos que se obtienen en el mundo son copias falsas lo que supone una pérdida estimada de unos 512 millones de dólares en pérdidas para las entidades propietarias del producto original.
- **Proveedores de servicios y soluciones IP:** en muchas ocasiones las empresas deciden subcontratar empresas especializadas para llevar a cabo la gestión de su propiedad intelectual. Hay que tener en cuenta que siempre que la propiedad intelectual pasa a entidades externas supone un potencial riesgo para la empresa.

Una vez que sabemos donde buscar los riesgos, debemos hacer un listado de todos los riesgos posibles y analizarlos en función

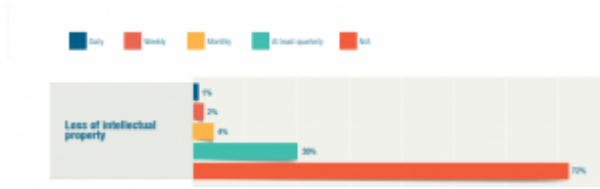
de varias variables como pueden ser:

- Probabilidad: probabilidad de que surja el riesgo.
- Impacto: impacto económico que tendría en la empresa en caso de que ocurra.

En función de estas variables conoceremos aquellos riesgos que debemos tener más en cuenta. Por lo general los principales riesgos suelen provenir de imitadores, piratería y sobre todo ciberataques. [7] Como muestra la siguiente encuesta realizada por ISACA, la mayoría de las empresas considera como muy probable el riesgo de un ataque cibernético. [8]



La misma encuesta también nos muestra la frecuencia con la que las empresas pierden activos protegidos por propiedad intelectual.



Por último, aunque podemos pensar que las empresas están protegidas por la ley, la realidad es que en muchos países no se lucha activamente contra estos infringimientos lo que supone un alto coste económico para la empresa.[7]

En el siguiente post os comentaré los controles que se pueden llevar a cabo para tratar los diferentes riesgos comentados previamente.

Referencias:

[1]https://www.ipeg.com/ip-risk-management-how-to-deal-with-it

-part-1/

[2]https://lat.motorsport.com/f1/news/analisis-nace-un-nuevo-caso-de-spygate-en-la-f1/1594861/

[3]https://www.forbes.com/sites/connieguglielmo/2012/08/23/apple-samsung-patent-war-puts-future-of-innovation-at-risk/#6f5b250d6c76

[4]https://whatis.techtarget.com/definition/non-practicing-entity-NPE

[5]https://whatis.techtarget.com/definition/patent-troll

[6]https://www.abc.es/tecnologia/redes/abci-32-por-ciento-empresas-espanolas-admiten-haber-recibido-menos-ciberataque-ultimo-201705121805_noticia.html

[7]https://info.knowledgeleader.com/bid/164620/What-is-Intellectual-Property-Risk

[8]https://www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf

---

Cómo integrar la propiedad intelectual en una empresa

En el post anterior hablé sobre los diferentes derechos de protección que contempla la propiedad intelectual actualmente. En este me centraré en explicar la influencia que esta tiene en el negocio y cómo se debería integrar dentro de la empresa.

Debido al entorno competitivo en el que se mueven las empresas hoy en día, la innovación se hace casi imprescindible.

Identificar, desarrollar y el aprovecharse de nuevos productos o servicios innovadores es lo que llevará a la empresa a alcanzar el éxito. [1] Es aquí donde entra la utilidad de la propiedad intelectual a través de la protección mediante patentes, marcas u otras formas para tener protegidos estos nuevos servicios o productos de la competencia.

La creación de una nueva empresa comienza tras una idea innovadora sobre un producto o servicio. Tras esto tienen lugar numerosos procesos (diseño, desarrollo, pruebas) hasta la comercialización del mismo. El uso de la propiedad intelectual es imprescindible en cada una estas fases si se quieren obtener los mejores resultados económicos. [2] Por ejemplo, en la fase de diseño es probable que se diseñe el logo del producto, el cual habría que proteger.

Una vez que empecemos a desarrollar nuestros productos o servicios nos deberíamos hacer la siguiente pregunta, ¿cómo podemos implementar la propiedad intelectual? Para dar respuesta a esta pregunta la OEPM (Oficina española de patentes y marcas) ofrece una interesante guía de buenas prácticas para integrar la propiedad intelectual en la empresa a través de 10 consejos [3]:

1.Sea consciente de su capital intelectual: haga una lista con todos los activos que considere que deben estar protegidos.

2.Conozca qué es la propiedad intelectual: conocer las diferentes categorías en las que se divide la propiedad intelectual como pueden ser patentes, marcas y diseños industriales.

3.Proteja sus activos intangibles: indispensable proteger tus activos para evitar que terceros se beneficien de tu trabajo.

4.Elija la mejor protección para sus activos intangibles: elegir cuidadosamente aquellos activos a proteger. Hay que evaluar los diferentes países en los que se quiere obtener protección y tener en cuenta el coste económico de obtenerla.

5.Obtenga la protección: rellenar la solicitud y enviarla a la oficina nacional de registro oportuna. En caso de que se desee comercializar en otros países será necesario enviar una solicitud a la oficina de registro de cada país o hacer uso de los tratados acordados por la OMPI.

6.Integre la propiedad intelectual en su estrategia: una buena estrategia debería al menos poner en marcha un mecanismo para identificar los activos de la empresa que pueden ser protegidos, analizar su valor y decidir si protegerlos o no en función de esto.

7.Utilice la información sobre propiedad intelectual: conocer las diferentes patentes registradas por los competidores puede ser una fuente valiosa de información para tu empresa, ya que permite conocer el nuevo producto que van a sacar a la venta antes de que se produzca. Del mismo modo, es necesario antes de diseñar un nuevo producto llevar a cabo una comprobación de que no infringe la ley de propiedad intelectual para evitar posibles demandas y pérdida de tiempo. La mejor manera de comprobar esto es a través de las siguientes cuatro reglas [5]:

- No existe ningún otro producto del mismo tipo con la misma marca registrada.
- El producto no hace uso de una patente registrada.
- No se infringen derechos de autor o de indicación geográfica.
- No se utiliza ningún diseño ya registrado.

8.Cree valor con sus derechos sobre propiedad intelectual: es imprescindible obtener un retorno económica tras la inversión económica realizada para obtener la protección. Una forma podría ser la venta de licencias para la explotación de la propiedad intelectual.

9.Haga valer sus derechos sobre su propiedad intelectual: buscar a posibles infractores y buscar una solución. En primer

lugar se puede intentar negociar con el infractor con el objetivo de que remueva sus productos, los cambie o obtener una suma de dinero a través de la venta de una licencia de uso. Si esto no tiene éxito, el siguiente paso es acudir a los tribunales y exigir la retirada del producto así como una compensación económica. [5]

10.Consulte a expertos: debido a la complejidad de la ley y sus constantes cambios es necesario contar con abogados expertos en la materia. En caso de que la empresa opere en varios países, es necesario tener en cuenta que la ley no es igual en todos, por lo que es recomendable contar con asesoría legal dentro de cada uno de ellos. Cabe destacar también otras organizaciones a las que se puede consultar como las Oficinas de la Propiedad Intelectual o Centros de información sobre la Propiedad Intelectual.

En definitiva, la empresa debería ser capaz de usar la propiedad intelectual a su favor para obtener el máximo beneficio posible, usando los menos recursos económicos posibles. Es necesaria una estrategia que tenga en cuenta la propiedad intelectual desde la creación de la empresa hasta la venta de sus productos o servicios y la expansión internacional. [4]

Referencias:

[1]https://economictimes.indiatimes.com/small-biz/legal/relevance-of-intellectual-property-for-business/articleshow/49563911.cms

[2]http://www.innovaccess.eu/importance-of-ip-in-business

[3]http://www.oepm.es/export/sites/oepm/comun/documentos_relacionados/Publicaciones/Folletos/Guia_Buenas_practicas.pdf

[4]https://www.wipo.int/export/sites/home/blogsdeusto/public_html/sme/en/documents/wipo_magazine/01_2002.pdf

[5]http://www.innovaccess.eu/importance-of-ip-in-business?t=how-ip