

UNIDADE 11

PROPIEDAD INTELECTUAL E SEGURIDADE NO USO DÁS TIC

1.- CONCEPTO E BREVE HISTORIA DA PROPIEDAD INTELECTUAL.

1.1.- Historia.

1.1.1.- RENACEMENTO.

1.1.2.- A ILUSTRACIÓN FRANCESA E O DEBATE SOBRE A NATUREZA DO DEREITO.

1.1.3.- O SÉCULO XIX.

1.1.4.- O SÉCULO XX.

1.1.4.1.- Aspectos da Propiedade Intelectual segundo a OMPI.

1.1.4.2.- Propiedade industrial.

2.- DEREITOS SOBRE A PROPIEDAD INTELECTUAL.

3.- MECANISMOS DE PROTECCIÓN.

3.1.- Lei Orgánica de Protección de Datos de Carácter Persoal (LOPD).

3.1.1.- DEBER DE INFORMACIÓN.

3.1.2.- TIPOS DE CONSENTIMIENTO.

3.1.3.- COMUNICACIÓN DE DATOS.

3.1.4.- ACCESO AOS DATOS POR CONTA DE TERCEIROS.

3.1.5.- CRÍTICAS E PRINCIPAIS PROBLEMAS.

3.2.- Os virus e outro software mal intencionado. Programas Antivirus e Cortalumes.

3.2.1.- MÉTODOS DE PROPAGACIÓN.

3.2.2.- TIPOS DE VIRUS.

3.2.3.- MÉTODOS DE PROTECCIÓN E TIPOS.

3.2.3.1.- Activos.

3.2.3.2.- Pasivos (tamén coñecidos como Boas Prácticas).

3.3.- Certificados dixitais. As axencias certificadoras.

3.3.1.- CERTIFICADO DIXITAL.

3.3.2.- AXENCIAS CERTIFICADORAS.

3.4.- Software libre e propietario. Software de código aberto.

3.5.- Os distintos tipos de licenzas: GPL, BSD, etc.

3.5.1.- LICENZA COPYLEFT.

3.5.1.1.- Forte e débil.

3.5.2.- LICENZAS GPL.

3.5.2.1.- Licenza GNU GPL.

3.5.2.2.- Licenza Mozilla Public License.

3.5.3.- LICENZAS ESTILO BSD.

3.6.- A licenza Creative Commons.

3.6.1.- CREATIVE COMMONS.

3.6.2.- CREATIVE COMMONS INTERNATIONAL.

3.6.3.- OUTROS TIPOS DE LICENZAS.

PROPIEDAD INTELECTUAL E SEGURIDADE NO USO DÁS TIC

1.- CONCEPTO E BREVE HISTORIA DA PROPIEDAD INTELECTUAL.

A propiedade intelectual é un dereito patrimonial de carácter exclusivo que outorga o Estado, por un tempo determinado, para usar ou explotar en forma industrial e comercial as invencións ou innovacións, tales como un produto tecnicamente novo, unha mellora a unha máquina ou aparello, un deseño orixinal para facer máis útil ou atractivo un produto ou un proceso de fabricación novidoso; tamén ten que ver coa capacidade creativa da mente: as invencións, as obras literarias e artísticas, os símbolos, os nomes, as imaxes e privilexios.

O titular da propiedade intelectual ten facultade para evitar que calquera persoa teña acceso ou faga uso da súa propiedade sen o seu consentimento. Os dereitos de propiedade intelectual que outorga cada país son independentes entre si, polo que unha mesma idea, invención, obra ou carácter distintivo pode ser obxecto de protección nunha pluralidade de Estados, existindo tantos títulos de protección como Estados que a outorgaron.

A **propiedade intelectual** clasifícase en dúas categorías:

1. **Propiedade industrial:** A propiedade industrial é o dereito exclusivo que outorga o Estado para usar ou explotar en forma industrial e comercial as invencións ou innovacións de aplicación industrial ou indicacións comerciais que realizan individuos ou empresas para distinguir os seus produtos ou servizos ante a clientela no mercado. Esta inclúe as invencións, marcas, patentes, debuxos e modelos industriais, así como indicacións xeográficas de orixe.
2. **Dereitos de autor:** o recoñecemento que fai o Estado a favor de todo creador de obras literarias e artísticas, en virtude do cal outorga a súa protección para que o autor goce de prerrogativas e privilexios exclusivos de carácter persoal e patrimonial. Os primeiros integran o chamado dereito moral e os segundos, o patrimonial. Este refírese ás obras literarias e artísticas, é dicir, refírense aos dereitos que teñen os artistas sobre as súas obras, os dereitos dos intérpretes sobre as súas execucións e interpretacións, os dereitos dos autores de fonogramas sobre as súas gravacións e os dereitos das empresas de radiodifusión sobre os seus programas, tanto de radio como de televisión.

Ao termino do tempo que ten de vixencia o dereito da patente, ou no caso de que non se abonaran as coutas anuais pola mesma, pódese aproveitar a información contida na mesma sen o pago das regalías correspondentes aos titulares da patente.

A propiedade intelectual é o conxunto de dereitos que corresponden aos autores e a outros titulares (artistas, produtores, organismos de radiodifusión...) respecto das obras e prestacións froito da súa creación.

Ao Ministerio de Cultura correspóndelle propoñer as medidas, normativas ou non, para lograr a adecuada protección da propiedade intelectual.

1.1.- Historia¹.

1.1.1.- RENACEMENTO.

Coa extensión da imprenta na Europa Renacentista aparece o primeiro marco legal monopolista dos dereitos de propiedade intelectual, que era aínda un marco feudal e cuxos obxectivos fundamentais eran o control político da nacente empresa. O autor non aparecía como suxeito de dereitos, senón o impresor era o propietario destes.

Ese control estatal (en parte delegado na Igrexa no mundo católico), facilitou con todo a aparición das primeiras patentes. A primeira da que se ten constancia é unha patente de monopolio da República de Venecia de 1491 a favor de Pietro de Ravena que aseguraba que só el mesmo ou os impresores que el ditaminase tiñan dereito legal no interior da República a imprimir a súa obra "Fénix". A primeira patente deste tipo en Alemaña apareceu en 1501 e en Inglaterra en 1518, sempre para obras concretas e sempre como graza real de monopolio. Unha práctica esta, a da concesión de monopolios reais baixo forma de patente, que as monarquías europeas foron estendendo en distintos ámbitos como forma de remuneración dos seus colaboradores.

O século XVII coñeceu distintos intentos de regulación co obxecto de asegurar aos autores literarios unha parte das ganancias obtidas polos impresores. Ese era o sentido por exemplo das disposicións de 1627 de Felipe IV en España. O que movía a esta regulación é precisamente a ausencia de monopolio do autor respecto da obra. Dado que calquera impresor podía reeditar unha obra calquera, o lexislador buscaba manter os incentivos do autor ligándoo a compartir unha parte dos beneficios obtidos polo impresor.

Pero o primeiro sistema legal de propiedade intelectual configurado como tal xurdiu na Inglaterra Barroca. É o chamado Statute of Anne (polo nome do monarca en cuxo reinado promulgouse, Ana de Inglaterra) de 1710. A importancia desta norma veu dada porque por primeira vez aparecían as características propias do sistema de propiedade intelectual tal como coñécense actualmente

Establecía un sistema de monopolio temporal universal: todas as obras publicadas recibirían un prazo de copyright de 14 anos, renovable por unha vez si o autor mantíñase con vida (ou, sexa, un máximo de 28 anos de protección). Mentres que todas as obras publicadas antes de 1710 recibirían un prazo único de 21 anos a contar desá data.

O conflito veu cos impresores, os cales alegaban que unha vez encargadas e recibidas as obras, os beneficiarios do monopolio deberían ser eles e non o autor orixinal. Nacía así o sustento do que máis tarde sería a diferenza entre [copyright](#) e [dereitos de autor](#). **Mentres o primeiro converte a obra nunha mercancía máis facendo plenamente transmisibles os privilexios outorgados polo monopolio legal, o segundo reservará dereitos aos autores máis aló ata logo da venda.**

1.1.2.- A ILUSTRACIÓN FRANCESA E O DEBATE SOBRE A NATUREZA DO DEREITO.

Con distintas formas e matices o sistema estendíase aos poucos por Europa. Dinamarca e Suecia tiveron a súa primeira lexislación en 1741 e España en 1762, por lei outorgada polo rei Carlos III. Pero o debate sobre a natureza destas patentes seguiu aberto. Mentres o copyright tendía a

¹Inclúese este apartado como información sobre o desenvolvemento dos conceptos ao longo da historia.

homologar o privilexio cunha forma máis de propiedade, o dereito de autor requiría un fundamento que ao final o equiparase cun dereito natural, non nacido dunha concesión real, senón directamente esixibles de forma evidente... o cal, dado o recente da súa aparición non era, nin moito menos, unha argumentación teórica fácil, como mostraba, por exemplo, a **Lettre sur le commerce des livres** de Diderot.

1.1.3.- O SÉCULO XIX.

Con todo, a arrasadora expansión do capitalismo e a necesidade de incentivos para manter o acelerado desenvolvemento tecnolóxico, tralas guerras napoleónicas, consolidarían a lóxica da propiedade intelectual e estenderían as lexislacións protectoras.

De feito, a propiedade intelectual estivo historicamente supeditada, na práctica, ás necesidades sociais de innovación. Cando Eli Whitney inventou a desmotadora de algodón en 1794 a ninguén -e moito menos a el mesmo- ocorréuselle suscitar demandas malia que a houbese patentado. A desmotadora era un invento sinxelo, que permitía reducir o prezo do algodón drasticamente e converteu a EE.UU., na década de 1830, no gran provedor das nacentes manufacturas téxtiles británicas. E o algodón -ata entón equivalente ao lino en prezo e limitado xa que logo ás clases altas- transformouse nun ben de consumo de masas de prezo asumible. EE.UU. e Gran Bretaña pasaron, grazas á industria da manufactura algodoeira, de ser países en desenvolvemento a ser países desenvolvidos.

Outro aspecto destacable foi a internacionalización espontánea dos pagos aos autores por parte dos editores. Ao parecer, durante o século XIX os autores estadounidenses recibiron máis pagos dos editores británicos que dos do seu propio país, malia que legalmente os privilexios eran estatais e non podían ser reclamados legalmente noutros países. Parece que, como volve suceder hoxe en día, a parte principal dos ingresos dunha obra producíanse na primeira edición, o que incitaba aos editores británicos a pagar por acceder aos contidos antes que os seus competidores, sen necesidade de que estes fixesen valer os seus privilexios legais.

Malia iso, a *Convention de Berne pour la protection des œuvres littéraires et artistiques*, convocada en 1886 por iniciativa de Víctor Hugo -autor dos primeiros éxitos de vendas internacionais marcou un momento decisivo na globalización do dereito de autor ao obrigar á reciprocidade no recoñecemento de dereitos aos autores por parte dos países signatarios. Aínda que eran orixinalmente tan só media ducia de países exclusivamente europeos (EE.UU. non se sumou ata 1989) sentáronse as bases do panorama actual.

1.1.4.- O SÉCULO XX.

O século XX foi o século do copyright, os dereitos de autor e as patentes. Trala convención de Berna fúndase o BIRPI (*Bureaux internationaux réunis pour la protection du propriété intellectuelle*), hoxe OMPI (Organización Mundial da Propiedade Intelectual). Aparecen xa as primeiras sociedades de dereitos como a SAE (hoxe SGAE) en 1898 e farmacéuticas e empresas tecnolóxicas consolidaron, sobre o sistema de patentes, o seu modelo de negocio.

A segunda metade do século, co estalido industrial da música popular e a universalización do mercado audiovisual, concentrado en EE.UU., levaron á formación dun gran mercado cultural mundial dependente da homologación internacional da propiedade intelectual.

1.1.4.1.- ASPECTOS DA PROPIEDAD INTELECTUAL SEGUNDO A OMPI.

Segundo a **Organización Mundial da Propiedade Intelectual** (OMPI), a propiedade intelectual é un tipo de propiedade, isto significa que o seu propietario ou titular pode dispoñer desta como lle pareza e que ningunha outra persoa física ou xurídica poderá dispoñer legalmente da súa propiedade sen o seu consentimento. Naturalmente, o exercicio deste dereito está suxeito a limitacións.

- **Propiedade industrial:** Enténdese por propiedade industrial un conxunto de dereitos exclusivos que protexen tanto a actividade innovadora manifestada en novos produtos, novos procedementos ou novos deseños, como a actividade mercantil, mediante a identificación en exclusiva de produtos e servizos ofrecidos no mercado.
- **Dereitos de autor:** que comprende as obras literarias e artísticas, tales como as novelas, os poemas, as obras de teatro, as películas, as obras musicais, as obras de arte, os debuxos, pinturas, fotografías, esculturas, e os deseños arquitectónicos.
- **Dereitos conexos:** comprende as interpretacións ou execucións dos artistas, a produción de fonogramas e as actividades dos organismos de radiodifusión.

1.1.4.2.- PROPIEDAD INDUSTRIAL².

Ao tratarse dun tipo de propiedade intelectual, esta garda unha estreita relación con creacións do enxeño humano como as invencións e os debuxos e modelos industriais. As creacións estéticas que determinan a aparencia de produtos industriais. Ademais, a propiedade industrial inclúe as marcas de fábrica ou de comercio, as marcas de servizo, os nomes e designacións comerciais, incluídas as indicacións de procedencia e denominacións de orixe, e a protección contra a competencia desleal. Aquí, a característica de creación intelectual, aínda que existente, é menos prominente, pero o que importa é que o obxecto da propiedade industrial conste de signos que transmitan unha información aos consumidores, concretamente, sobre os produtos e os servizos que se ofrecen no mercado.

A protección vai dirixida contra o uso non autorizado de tales signos, o cal é moi probable que induza aos consumidores a erro, e contra as prácticas enganosas en xeral.

2.- DEREITOS SOBRE A PROPIEDAD INTELECTUAL.

Polo que respecta aos dereitos que conforman a propiedade intelectual distínguense os dereitos morais e os dereitos de carácter patrimonial:

- **Dereitos morais:**

Fronte aos sistemas de corte anglosaxón, a lexislación española é claramente defensora dos dereitos morais, recoñecidos para os autores e para os artistas, intérpretes ou executantes.

² Non confundir propiedade industrial con patentes. Unha patente é un dereito exclusivo concedido a unha invención, é dicir, un produto ou procedemento que aporta, en xeral, un novo xeito de facer algo ou unha nova solución técnica a un problema. Para que sexa patentable, a invención debe satisfacer determinados requisitos.

Estes dereitos son irrenunciabes e inalienabes, acompañan ao autor ou ao artista intérprete ou executante durante toda a súa vida e aos seus herdeiros ao falecemento daqueles. Entre eles destaca o dereito ao recoñecemento da condición de autor da obra ou do recoñecemento do nome do artista sobre as súas interpretacións ou execucións, e o de esixir o respecto á integridade da obra ou actuación e a non alteración das mesmas.

- **Dereitos de carácter patrimonial:**

Hai que distinguir entre:

- **Dereitos relacionados coa explotación da obra ou prestación protexida**, que á súa vez se subdividen en **dereitos exclusivos** e en **dereitos de remuneración**:
 - Os **dereitos exclusivos** son aqueles que permiten ao seu titular autorizar ou prohibir os actos de explotación da súa obra ou prestación protexida polo usuario, e a esixir de este unha retribución a cambio da autorización que lle conceda.
 - Os **dereitos de remuneración**, a diferenza dos dereitos exclusivos, non facultan ao seu titular a autorizar ou prohibir os actos de explotación da súa obra ou prestación protexida polo usuario, aínda que si obrigan a este ao pago dunha cantidade monetaria polos actos de explotación que realice, cantidade esta que é determinada, ben pola lei ou na súa falta polas tarifas xerais das entidades de xestión.
- **Dereitos compensatorios**, como o dereito por copia privada que compensa os dereitos de propiedade intelectual deixados de percibir por razón das reproducións das obras ou prestacións protexidas para uso exclusivamente privado do copista.

3.- MECANISMOS DE PROTECCIÓN.

3.1.- Lei Orgánica de Protección de Datos de Carácter Persoal (LOPD).

Lei Orgánica 15/1999, de 13 de decembro, de Protección de Datos de Carácter Persoal.

Esta Lei Orgánica ten por obxecto garantir e protexer, no que concirne ao tratamento dos datos persoais, as liberdades públicas e os dereitos fundamentais das persoas físicas, e especialmente do seu honor e intimidade persoal e familiar.

O seu obxectivo principal é regular o tratamento dos datos e ficheiros, de carácter persoal, independentemente do soporte no cal sexan tratados, os dereitos dos cidadáns sobre eles e as obrigacións daqueles que os crean ou tratan.

O órgano de control do cumprimento da normativa de protección de datos dentro do territorio español, e con carácter xeral é a Axencia Española de Protección de Datos (AEPD), existindo outras Axencias de Protección de Datos de carácter autonómico.

As sancións teñen unha elevada contía, sendo España o país da Unión Europea que ten as sancións máis altas en materia de protección de datos. Ditas sancións dependen da infracción cometida.

Divídense en:

As **sancións leves** van desde **601,01** a 60.101,21 €

As **sancións graves** van desde **60.101,21** a 300.506,05 €

As **sancións moi graves** van desde **300.506,05** a 601.012,10 €

Pese ao elevado importe das sancións, existen moitas empresas en España que aínda non se adecuaron á mesma, ou o fixeron de forma parcial ou non revisan de forma periódica a súa adecuación; polo que resulta esencial o mantemento e revisión da adecuación realizada.

No sector público, a citada Lei regula igualmente o uso e manexo da información e os ficheiros con datos de carácter persoal utilizados por todas as administracións públicas.

A Axencia Española de Protección de Datos (AEPD) foi creada en 1994. Esta atópase en Madrid, aínda que algunhas comunidades autónomas crearon as súas propias axencias de carácter autonómico.

3.1.1.- DEBER DE INFORMACIÓN.

Os datos persoais clasifícanse en función do seu maior ou menor grado de sensibilidade, sendo os requisitos legais e de medidas de seguridade informáticas máis estritos en función do devandito maior grado de sensibilidade. Sendo obrigatorio, en todo caso a declaración dos ficheiros de protección de datos á "Axencia Española de Protección de Datos".

Os interesados aos que se soliciten datos persoais deberán ser previamente informados de modo expreso, preciso e inequívoco:

1. Da existencia dun ficheiro ou tratamento de datos de carácter persoal, da finalidade da recolleita destes e dos destinatarios da información.
2. Do carácter obrigatorio ou facultativo da súa resposta ás preguntas que lles sexan suscitadas.
3. Das consecuencias da obtención dos datos ou da negativa a dalos.
4. Da posibilidade de exercer os dereitos de acceso, rectificación, cancelación e oposición.
5. Da identidade e dirección do responsable do tratamento ou, no seu caso, do seu representante.

Permítese con todo, o tratamento de datos de carácter persoal sen ser solicitados directamente do afectado ou interesado, aínda que non se exige da obrigaón de informar de forma expresa, precisa e inequívoca, por parte do responsable do ficheiro ou o seu representante, dentro dos tres meses seguintes ao comezo do tratamento dos datos.

A excepción a todo isto faise dicindo que non será necesaria a comunicación en tres meses de devandita información si os datos foron recollidos de fontes **"accesibles ao público"**, e destínanse á actividade de publicidade ou prospección **comercial**, neste caso "en cada

comunicación que se dirixa ao interesado informaráselle da orixe dos datos e da identidade do responsable do tratamento, así como dos dereitos que lle asisten".

Existen datos cuxo tratamento está prohibido, que son os relativos a infraccións "penais ou administrativas" que só poderán ser incluídos nos ficheiros das **Administracións públicas competentes**.

3.1.2.- TIPOS DE CONSENTIMENTO.

Dependendo dos tipos de datos tratados requirirase por parte da persoa un consentimento distinto:

- A) **Consentimento inequívoco.** O tratamento dos datos de carácter persoal requirirá o consentimento inequívoco do afectado, salvo que a lei dispoña outra cousa.
- B) **Consentimento tácito.** Esta será a forma normal do consentimento nos supostos nos que non se esixa un consentimento expreso ou expreso e por escrito.
- C) **Consentimento expreso.** Os datos de carácter persoal que fagan referencia á orixe racial, á saúde e á vida sexual só poderán ser solicitados, tratados e cedidos cando, por razóns de interese xeral, así o dispoña unha lei ou o afectado consinta expresamente.
- D) **Consentimento expreso e por escrito.** Requírese consentimento expreso e por escrito do afectado respecto dos datos relativos á *ideoloxía, afiliación sindical, relixión e crenzas* e só poderán ser cedidos con consentimento expreso.

3.1.3.- COMUNICACIÓN DE DATOS.

Os datos de carácter persoal obxecto do tratamento só poderán ser comunicados a un terceiro para o cumprimento de fins directamente relacionados coas funcións lexítimas do cedente e do cesionario co previo consentimento do interesado.

O consentimento esixido no apartado anterior non será preciso:

1. Cando a cesión está autorizada nunha lei.
2. Cando se trate de datos recolleitos de fontes accesibles ao público.
3. Cando o tratamento responda á libre e lexítima aceptación dunha relación xurídica cuxo desenvolvemento, cumprimento e control implique necesariamente a conexión de devandito tratamento con ficheiros de terceiros. Neste caso a comunicación só será lexítima en canto se limite á finalidade que a xustifique.
4. Cando a comunicación que deba efectuarse teña por destinatario ao Defensor do Pobo, o Ministerio Fiscal ou os Xuíces ou Tribunais ou o Tribunal de Contas, no exercicio das funcións que ten atribuídas. Tampouco será preciso o consentimento cando a comunicación teña como destinatario a institucións autonómicas con funcións análogas ao Defensor do Pobo ou ao Tribunal de Contas.

5. Cando a cesión prodúzase entre Administracións públicas e teña por obxecto o tratamento posterior dos datos con fins históricos, estatísticos ou científicos.
6. Cando a cesión de datos de carácter persoal relativos á saúde sexa necesaria para solucionar unha urxencia que requira acceder a un ficheiro ou para realizar os estudos epidemiolóxicos nos termos establecidos na lexislación sobre sanidade estatal ou autonómica.

Será nulo o consentimento para a comunicación dos datos de carácter persoal a un terceiro, cando a información que se facilite ao interesado non lle permita coñecer a finalidade a que destinarán os datos cuxa comunicación autorízase ou o tipo de actividade daquel a quen se pretenden comunicar.

O consentimento para a comunicación dos datos de carácter persoal ten tamén un carácter de revocable.

Aquel a quen se comuniquen os datos de carácter persoal obrígase, polo só feito da comunicación, á observancia das disposicións da presente Lei.

Si a comunicación efectúase previo procedemento de disociación (tratamento dos datos persoais de modo que a información que se obteña non poida asociarse a persoa identificada o identificable), non será aplicable o establecido nos apartados anteriores.

3.1.4.- ACCESO AOS DATOS POR CONTA DE TERCEIROS.

1. Non se considerará comunicación de datos o acceso dun terceiro aos mesmos cando este sexa necesario para a prestación dun servizo ao responsable do tratamento.
2. A realización de tratamentos por conta de terceiros deberá estar regulada nun contrato que deberá constar por escrito ou nalgunha outra forma que permita acreditar a súa celebración e contido. Establecéndose expresamente, que o encargado do proceso unicamente tratará os datos conforme ás instrucións do responsable do tratamento, que non os aplicará ou utilizará con fin distinto ao que figure en devandito contrato, nin os comunicará, nin sequera para a súa conservación, a outras persoas.

No contrato se estipularán, así mesmo, as medidas de seguridade a que se refire o artigo 9 desta Lei que o encargado do tratamento está obrigado a cumprir.

3. Unha vez cumprida a prestación contractual, os datos de carácter persoal deberán ser destruídos ou devoltos ao responsable do tratamento, do mesmo xeito que calquera soporte ou documentos en que conste algún dato de carácter persoal obxecto do tratamento.
4. No caso de que o encargado do tratamento destine os datos a outra finalidade, comuníqueos ou os utilice incumprindo as estipulacións do contrato, será considerado tamén responsable do tratamento, respondendo das infraccións en en que houbese incorrido persoalmente.

3.1.5.- CRÍTICAS E PRINCIPAIS PROBLEMAS.

Un cumprimento moi rigoroso da regulación sobre a protección de datos podería ralentizar o traballo normal dun responsable de ficheiros pola acreditación documental dos principios de información e consentimento da LOPD; tamén en sentido contrario un cumprimento so das

obligacións formais, deixaría sen sentido á lei e desprotexidos aos cidadáns e iría fronte ao "espírito" da LOPD.

A posibilidade de que as empresas poidan solicitar datos sen o consentimento do afectado foi criticada.

3.2.- Os virus e outro software mal intencionado. Programas Antivirus e Cortalumes.

Un **virus informático** ten por obxecto alterar o normal funcionamento do ordenador sen o permiso ou o coñecemento do usuario. Os virus, habitualmente, substitúen arquivos executables por outros infectados co código de este. Poden destruír, de xeito intencionado, os datos almacenados nun ordenador, aínda que tamén existen outros máis "benignos", que só se caracterizan por ser molestos.

Un virus pode danar ou eliminar datos do equipo, usar o programa de correo electrónico para propagarse a outros equipos ou ata borrar todo o contido do disco duro.

Os virus propáganse máis facilmente mediante datos adxuntos incluídos en mensaxes de correo electrónico ou de mensaxería instantánea. Por este motivo é fundamental non abrir nunca os datos adxuntos de correo electrónico a menos que saiba de quen proceden e estéaos esperando.

O funcionamento dun virus informático é conceptualmente simple. Execútase un programa que está infectado, na maioría das ocasións, por descoñecemento do usuario. O código do virus queda residente (aloxado) na memoria RAM da computadora, aínda cando o programa que o contiña termine de executarse. O virus toma entón o control dos servizos básicos do sistema operativo infectando, de xeito posterior, arquivos executables que sexan chamados para a súa execución. Finalmente engádese o código do virus ao do programa infectado e grávase en disco, co cal o proceso de replicado complétase.

Os virus informáticos afectan en maior ou menor medida a case todos os sistemas operativos coñecidos e usados na actualidade.

Un virus informático só atacará o sistema operativo para o que foi desenvolvido.

As maiores incidencias danse no sistema operativo Windows debido, entre outras causas, a:

- A súa gran popularidade, como sistema operativo, entre os ordenadores persoais, PC. Estímase que, no 2007, un 90% deles usaba Windows. Esta popularidade baseada na facilidade de uso sen coñecemento previo algún, facilita a vulnerabilidade do sistema para o desenvolvemento dos virus, e así atacar os seus puntos débiles, que polo xeral son abundantes.
- Falta de seguridade nesta plataforma (situación á que Microsoft está dando nos últimos anos maior prioridade e importancia que no pasado). Ao ser un sistema moi permisivo coa instalación de programas alleos a este, sen requirir ningunha identificación por parte do usuario ou pedirle algún permiso especial para iso.

- Software como Internet Explorer e Outlook Express, desenvolvidos por Microsoft e incluídos de forma predeterminada en Windows, son coñecidos por ser vulnerables aos virus xa que estes aproveitan a vantaxe de que devanditos programas están fortemente integrados no sistema operativo dando acceso completo, e practicamente sen restricións, aos arquivos do sistema.
- A escasa formación dun número importante de usuarios deste sistema, é o que provoca que non se tomen medidas preventivas por parte destes, xa que este sistema está dirixido de xeito maioritario aos usuarios non expertos en Informática. Esta situación é aproveitada constantemente polos programadores de virus.

Noutros sistemas operativos como as distribucións GNU/Linux, BSD, OpenSolaris, Solaris, Mac VOS X e outros baseados en Unix as incidencias e ataques son practicamente inexistentes. Isto débese principalmente a:

- Tradicionalmente os programadores e usuarios de sistemas baseados en Unix consideraron a seguridade como unha prioridade polo que hai maiores medidas fronte a virus tales como a necesidade de autenticación por parte do usuario como administrador ou root para poder instalar calquera programa adicional ao sistema.
- Os directorios ou cartafolios que conteñen os arquivos vitais do sistema operativo contan con permisos especiais de acceso, polo que non calquera usuario ou programa pode acceder facilmente a eles para modificalos ou boralos. Existe unha xerarquía de permisos e accesos para os usuarios.
- Relacionado co caso anterior, a diferenza dos usuarios de Windows, a maioría dos usuarios de sistemas baseados en Unix non poden normalmente iniciar sesións como usuarios "administradores" ou polo superusuario root, excepto para instalar ou configurar software, dando como resultado que, ata si un usuario non administrador executa un virus ou algún software malicioso, este non danaría completamente o sistema operativo xa que Unix limita a contorna de execución a un espazo ou directorio reservado chamado, comunmente, home.
- Estes sistemas, a diferenza de Windows, son usados para tarefas máis complexas como servidores que polo xeral están fortemente protexidos, razón que os fai menos atractivos para un desenvolvemento de virus ou software malicioso.

Dado que unha característica dos virus é o consumo de recursos, os virus ocasionan problemas tales como: perda de produtividade, cortes nos sistemas de información ou danos a nivel de datos.

Outra das características é a posibilidade que teñen de diseminarse por medio de réplicas e copias. As redes axudan a dita propagación cando estas non teñen a seguridade adecuada.

Outros danos que os virus producen aos sistemas informáticos son a perda de información, horas de parada produtiva, tempo de reinstalación, etc.

Hai que ter en conta que cada virus suscita unha situación diferente.

3.2.1.- MÉTODOS DE PROPAGACIÓN.

Existen dúas grandes clases de contaxio. Na primeira, o usuario, nun momento dado, executa ou acepta de forma inadvertida a instalación do virus. Na segunda, o programa malicioso actúa replicándose a través das redes. Neste caso fálase de 'gusanos'.

En calquera dos dous casos, o sistema operativo infectado comeza a sufrir unha serie de comportamentos anómalos ou imprevistos. Devanditos comportamentos poden dar unha pista do problema e permitir a recuperación do mesmo.

Dentro das contaminacións máis frecuentes por interacción do usuario están as seguintes:

- Mensaxes que executan automaticamente programas (como o programa de correo que abre directamente un arquivo achego).
- Enxeñería social, mensaxes como...execute este programa e gañe un premio...
- Entrada de información en discos doutros usuarios infectados.
- Instalación de software pirata ou de baixa calidade.

No sistema Windows pode darse o caso de que o ordenador poida infectarse sen ningún tipo de intervención do usuario (versións Windows 2000, XP e Server 2003) por virus como Blaster, Sasser e as súas variantes polo simple feito de estar a máquina conectada a unha rede ou a Internet. Este tipo de virus aproveitan unha vulnerabilidade de desbordamento de buffer e portos de rede para infiltrarse e contaxiar o equipo, causar inestabilidade no sistema, mostrar mensaxes de erro, reenviarse a outras máquinas mediante a rede local ou Internet e ata reiniciar o sistema, entre outros danos. Nas últimas versións de Windows 2000, XP e Server 2003 corrixiuse este problema na súa maioría.

3.2.2.- Tipos de virus.

Existen diversos tipos de virus, varían segundo a súa función ou o xeito en que este se executa na nosa computadora alterando a actividade da mesma, entre os máis comúns están:

- **Troyano:** que consiste en roubar información ou alterar o sistema do hardware ou nun caso extremo permite que un usuario externo poida controlar o equipo.
- **Gusano:** ten a propiedade de duplicarse a si mesmo. Os 'gusanos' utilizan as partes automáticas dun sistema operativo que xeralmente son invisibles ao usuario.
- **Bombas lóxicas ou de tempo:** son programas que se activan ao producirse un acontecemento determinado. A condición adoita ser unha data (Bombas de Tempo), unha combinación de teclas, ou certas condicións técnicas (Bombas Lóxicas). Si non se produce a condición permanece oculto ao usuario.
- **Hoax:** non son virus nin teñen capacidade de reproducirse por si sos. Son mensaxes de contido falso que incitan ao usuario a facer copias e enviala aos seus contactos. Adoitan apelar aos sentimentos morais ("Axuda a un neno doente de cancro") ou ao espírito de solidariedade ("Aviso dun novo virus perigoso") e, en calquera caso, tratan de aproveitarse da falta de experiencia dos internautas novatos.

Algunhas das accións de virus son:

- Unirse a un programa instalado no ordenador permitindo a súa propagación.
- Mostrar na pantalla mensaxes ou imaxes humorísticas, xeralmente molestas.
- Ralentizar ou bloquear o ordenador.
- Destruír a información almacenada no disco, nalgúns casos vital para o sistema, que impedirá o funcionamento do equipo.
- Reducir o espazo no disco.

3.2.3.- MÉTODOS DE PROTECCIÓN E TIPOS.

Os **antivirus** naceron como unha ferramenta simple cuxo obxectivo era detectar e eliminar virus informáticos, durante a década de 1980.

Co transcurso do tempo, e a aparición de sistemas operativos máis avanzados e Internet, os antivirus han evolucionado cara a programas máis sofisticados que non só buscan detectar un virus informático, senón **bloquealo, desinfectar e previr unha infección dos mesmos**. Na actualidade son capaces de recoñecer outros tipos de programas mal intencionados (malware).

O funcionamento dun antivirus varía dun a outro, aínda que o seu comportamento normal baséase en contar cunha lista de virus coñecidos e a súa formas de recoñecelos (as chamadas firmas), e analizar contra esa lista os arquivos almacenados ou transmitidos desde e cara a un ordenador.

Adicionalmente, moitos dos antivirus actuais incorporaron funcións de detección proactiva, que non se basean nunha lista de malware coñecido, senón que analizan o comportamento dos arquivos ou comunicacións para detectar cales son potencialmente daniñas para o ordenador.

Usualmente, un antivirus ten un (ou varios) compoñente residente en memoria que se encarga de analizar e verificar todos os arquivos abertos, creados, modificados, executados e transmitidos en tempo real mentres o ordenador está en uso.

Así mesmo, contan cun compoñente de análise baixo demanda (os coñecidos escáners, exploradores,...) e módulos de protección de correo electrónico, Internet, etc.

O obxectivo primordial de calquera antivirus actual é detectar a maior cantidade de ameazas informáticas que poidan afectar a un ordenador, e bloquealas antes de que a mesma poida infectar un equipo, ou poder eliminala trala infección.

Os métodos para diminuír ou reducir os riscos asociados aos virus poden ser **activos** ou **pasivos**.

3.2.3.1.- Activos.

- **Antivirus:** son programas que tratan de descubrir as trazas que deixou un software malicioso, para detectalo e eliminalo, e nalgúns casos conter ou parar a contaminación. Tratan de ter controlado o sistema mentres funciona parando as vías coñecidas de infección e notificando ao usuario de posibles incidencias de seguridade.
- **Filtros de Ficheiros:** consiste en xerar filtros de ficheiros danos si o ordenador está conectado a unha rede. Estes filtros poden usarse, por exemplo, no sistema de email ou usando técnicas de firewall. En xeral, este sistema proporciona unha seguridade onde non se require a intervención do usuario, pode ser moi eficaz, e permitir empregar unicamente recursos de forma máis selectiva.

3.2.3.2.- Pasivos (tamén coñecidos como Boas Prácticas).

- Evitar introducir ao teu equipo medios de almacenamento removibles que consideres que puidesen estar infectados con algún virus.
- Non instalar software "pirata".
- Evitar descargar software de Internet.
- Non abrir mensaxes provenientes dunha dirección electrónica descoñecida.
- Non aceptar e-mails de descoñecidos.

Existen ideas instaladas, parte polas empresas de antivirus, parte na cultura popular, que non axudan a manter a seguridade dos sistemas de información.

- **O meu sistema non é importante para un cracker.** Este tema baséase na idea de que non introducir passwords seguras non entraña riscos pois, quen vai querer obter información miña?. Con todo dado que os métodos de contaxio realízanse por medio de programas automáticos, desde unhas máquinas a outras, estes non distinguen bos de malos, interesantes de non interesantes... Xa que abrir sistemas e deixalos sen claves é facilitar a vida aos virus.
- **Estou protexido pois non abro arquivos que non coñezo.** Isto é falso, pois existen múltiples formas de contaxio, ademais os programas realizan accións sen a supervisión do usuario poñendo en risco os sistemas.
- **Como teño antivirus estou protexido.** Unicamente estou protexido mentres o antivirus saiba ao que se enfronta e como combatelo. En xeral os programas antivirus non son capaces de detectar todas as posibles formas de contaxio existentes, nin as novas que puidesen aparecer conforme as computadoras aumenten as capacidades de comunicación.
- **Como dispoño dun firewall non me contaxio.** Isto unicamente proporciona unha limitada capacidade de resposta. As formas de infectarse nunha rede son múltiples. Unhas proveñen directamente de accesos ao meu sistema (do que protexe un firewall) e outras de conexións

que realizou (das que non me protexe). Empregar usuarios con altos privilexios para realizar conexións tampouco axuda.

3.3.- Certificados dixitais. As axencias certificadoras.

3.3.1.- CERTIFICADO DIXITAL.

Un **certificado dixital** é un documento dixital mediante o cal un terceiro de confianza (unha autoridade de certificación) garante a vinculación entre a identidade dun suxeito ou entidade e a súa clave pública.

Un certificado electrónico é un documento asinado electrónicamente por un prestador de servizos de certificación que vincula a identidade de cada usuario coas ferramentas de firma electrónica (claves criptográficas), dándolle a coñecer como firmante no ámbito telemático.

Aínda que existen variados formatos para **certificados dixitais**, os máis comunmente empregados réxense polo estándar UIT-TX.509. O certificado contén usualmente o nome da entidade certificada, número de serie, data de expiración, unha copia da clave pública do titular do certificado (utilizada para a verificación da súa firma dixital) e a firma dixital da autoridade emisora do certificado de forma que o receptor poida verificar que esta última estableceu realmente a asociación.



Un certificado emitido por unha entidade de certificación autorizada, ten que ter un formato predefinido, é dicir, ademais de estar asinado dixitalmente por esta, debe conter polo menos o seguinte:

- Nome, dirección e domicilio do subscritor.
- Identificación do subscritor nomeado no certificado.
- nome, a dirección e o lugar onde realiza actividades a entidade de certificación.
- A clave pública do usuario.
- A metodoloxía para verificar a firma dixital do subscritor imposta na mensaxe de datos.
- número de serie do certificado.
- Data de emisión e expiración do certificado.

3.3.2.- AXENCIAS CERTIFICADORAS.

Calquera individuo ou institución pode xerar un **certificado dixital**, pero si este emisor non é recoñecido por quen colabora co propietario do certificado, o valor do mesmo é practicamente nulo. Por iso os emisores deben **acreditarse**: así se denomina ao proceso polo cal entidades recoñecidas, xeralmente públicas, outorgan validez á institución certificadora, de forma que a súa firma poida ser recoñecida como fiable, transmitindo esa fiabilidade aos certificados emitidos pola citada institución.

A gran maioría dos emisores teñen fins comerciais, e outros, grazas ao sistema de anel de confianza poden outorgar gratuitamente certificados en todo o mundo, como:

- *Cacert.org*, emisor administrado pola comunidade con base legal en Australia.
- *Thawte*, só para certificados persoais. Emisor propiedade de Verisign.

Pero para que un **certificado dixital** teña validez legal, o prestador de servizos de certificación debe acreditarse en cada país de acordo á normativa que cada un defina.

Os encargados de autorizar a creación dunha autoridade de certificación ou prestador de servizos de certificación en España son entre outros a Fábrica Nacional de Moneda y Timbre, o Ministerio de Industria, Turismo e Comercio, a Agència Catalá de Certificació, a Autoritat de Certificació da Comunitat Valenciana, etc.

A Fábrica Nacional de Moneda y Timbre, como proveedor de servizos de certificación a través de CERES (**CERT**ificación **ES**pañola), ha implementado unha serie de aplicacións que permiten á Administración, aos cidadáns e ás empresas españolas realizar as súas operacións a través de

Internet de forma totalmente segura. As novas solucións de certificación e autenticación de identidade dixital que ofrece a Fábrica Nacional de Moneda y Timbre, proporcionan validez e seguridade ás transaccións electrónicas

3.4.- Software libre e propietario. Software de código aberto.

Software libre, é a denominación do software que respecta a liberdade dos usuarios sobre o seu produto adquirido e, xa que logo, unha vez obtido pode ser usado, copiado, estudado, cambiado e redistribuído libremente. O software libre refírese á liberdade dos usuarios para executar, copiar, distribuír, estudar, cambiar e mellorar o software; de modo máis preciso, refírese a catro liberdades dos usuarios do software:

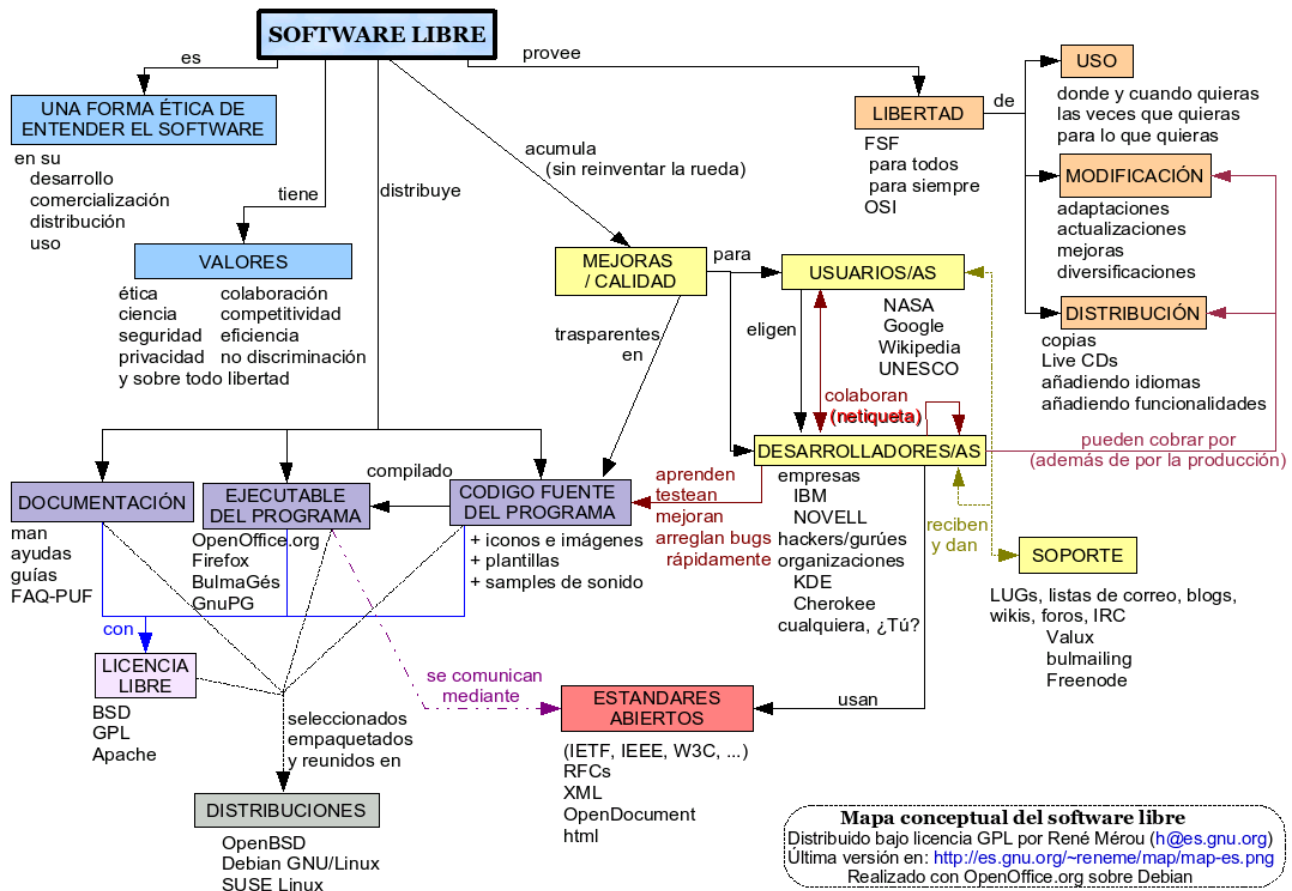
- A liberdade de usar o programa, con calquera propósito.
- A liberdade de estudar o funcionamento do programa, modificalo e adaptalo ás túas necesidades.
- A liberdade de distribuír copias, co cal pódese axudar a outros.

- A liberdade de mellorar o programa e facer públicas as melloras, de modo que toda a comunidade se beneficie (para a segunda e última liberdade mencionadas, o acceso ao código fonte é un requisito previo).

O software libre adoita estar dispoñible gratuitamente, ou ao prezo de custo da distribución a través doutros medios; con todo non é obrigatorio que sexa así, polo tanto non hai que asociar software libre a software "**gratuíto**" (denominado usualmente *freeware*), xa que, conservando o seu carácter de libre, pode ser distribuído comercialmente ("software comercial").

Analogamente, o software "gratis" ou "gratuíto" inclúe en ocasións o código fonte; no entanto, este tipo de software non é libre no mesmo sentido que o software libre, a menos que se garantan os dereitos de modificación e redistribución de devanditas versións modificadas do programa.

Tampouco debe confundirse software libre con software "de dominio público". Este último é aquel software que non require de licenza, pois os seus dereitos de explotación son para toda a humanidade, porque pertence a todos por igual. Calquera pode facer uso del, sempre con fins legais e consignando a súa autoría orixinal. Este software sería aquel cuxo autor dóao á humanidade ou cuxos dereitos de autor han expirado, tras un prazo contado desde a morte de este, habitualmente 70 anos. Si un autor condiciona o seu uso baixo unha licenza, por moi débil que sexa, xa non é do dominio público.



As catro liberdades anteriores dan lugar ás seguintes normas de funcionamento:

- 1.- Libre redistribución: o software debe poder ser regalado ou vendido libremente
- 2.- Código fonte: o código fonte debe estar incluído ou obterse libremente.
- 3.- Traballos derivados: a redistribución de modificacións debe estar permitida.
- 4.- Integridade do código fonte do autor: as licenzas poden requirir que as modificacións sexan redistribuídas soamente como parches.
- 5.- Sen discriminación de persoas ou grupos: ningún pode deixarse fora.
- 6.- Sen discriminación de áreas de iniciativa: os usuarios comerciais non poden ser excluídos.
- 7.- Distribución da licenza: deben aplicarse os mesmos dereitos a todo o que reciba o programa.
- 8.- A licenza non debe ser específica dun produto: o programa non pode licenciarse só como parte dunha distribución maior.
- 9.- A licenza non debe restrinxir outro software: a licenza non pode obrigar a que algún outro software que sexa distribuído co software aberto deba tamén ser de código aberto.

- 10.- A licenza debe ser tecnolóxicamente neutral: non debe requirirse a aceptación da licenza por medio dun acceso por clic de rato ou doutra forma específica do medio de soporte do software.

Software propietario, ou **privativo** ou **de código pechado** fai referencia a calquera programa informático no que os usuarios teñen limitadas as posibilidades de usalo, modifícalo ou redistribuílo (con ou sen modificacións), ou cuxo código fonte non está dispoñible ou o acceso a este atópase restrinxido.

Para a Fundación para o Software Libre (FSF) este concepto aplícase a calquera software que non é libre ou que só o é parcialmente (semilibre), sexa porque o seu uso, redistribución ou modificación está prohibida, ou require permiso expreso do titular do software.

No software de código pechado unha persoa física ou xurídica (compañía, corporación, fundación, etc.) posúe os dereitos de autor sobre un software o que lle dá a posibilidade de controlar e restrinxir os dereitos do usuario sobre o seu programa. Isto implica polo xeral que o usuario só ten dereito a executar o software e non dispón de acceso ao seu código fonte ou aínda tendo acceso a el non ten dereito a modifícalo nin distribuílo.

Deste xeito, un software segue sendo de código pechado aínda si o código fonte é feito público, cando se mantén a reserva de dereitos sobre o uso, modificación ou distribución (por exemplo, a versión comercial de [SSH](#) ou o programa de licenzas [Shared Source de Microsoft](#)).

3.5.- Os distintos tipos de licenzas: GPL, BSD, etc.

Unha licenza é aquela autorización formal con carácter contractual que un autor dun software dá a un interesado para exercer "actos de explotación legais". Poden existir tantas licenzas como acordos concretos déanse entre o autor e o licenciatario. A este tipo de licenzas denomínaselles de Copyleft.

3.5.1.- LICENZA COPYLEFT.

É unha forma de licenza e pode ser usado para modificar o dereito de autor de obras ou traballos, tales como software de computadoras, documentos, música, e obras de arte.

Baixo tales licenzas poden protexerse unha gran diversidade de obras, tales como programas informáticos, arte, cultura e ciencia, é dicir practicamente case calquera tipo de produción creativa.

Os seus partidarios propoñenas como alternativa ás restricións que impoñen as normas suscitadas nos dereitos de autor, á hora de facer, modificar e distribuír copias dunha obra determinada. Con este tipo de licenza preténdese garantir unha maior liberdade para que cada receptor dunha copia, ou unha versión derivada dun traballo, poida, á súa vez, usar, modificar e redistribuír tanto o propio traballo como as versións derivadas do mesmo. Así, e nunha contorna non legal, pode considerarse como oposto ao copyright ou dereitos de autor tradicionais.

A práctica habitual para conseguir este obxectivo de explotación sen trabas, copia e distribución dunha creación ou dun traballo (e os seus derivados) é a de ofrecelo xunto cunha licenza ou contrato. Esta debería estipular que cada propietario dunha copia do traballo puidese:

1. Usala sen ningunha limitación.
2. (Re)distribuír cantas copias desexa.
3. Modificala do xeito que crea conveniente.

Estas tres liberdades básicas, con todo, non son suficientes aínda para asegurar que unha obra derivada sexa distribuída baixo as mesmas condicións non restritivas: con este fin, a licenza debe asegurar que o propietario do traballo derivado distribuíralo baixo o mesmo tipo de licenza.

Outras condicións de licenza adicionais que poderían evitar posibles impedimentos ás tres liberdades básicas anteriores son:

- As condicións da licenza copyleft non poden ser revogadas.
- O traballo e os seus derivados son sempre postos a disposición, de maneira que se facilite a súa modificación. Por exemplo, no software, esta facilidade adoita asociarse a dispoñibilidade do código fonte, onde ata a compilación do devandito código debería permitirse sen ningunha clase de impedimento.
- Idear un sistema máis ou menos obrigatorio para documentar adecuadamente a creación e as súas modificacións, por medio de manuais de usuario, descrições, etc.

O titular dos dereitos de autor (copyright) dun software baixo licenza



copyleft pode tamén realizar unha versión modificada baixo o seu copyright orixinal, e vendela baixo calquera licenza que desexa, ademais de distribuír a versión orixinal como software libre. Esta técnica foi usada como un modelo de negocio por unha serie de empresas que realizan software libre (por exemplo MySQL); esta práctica non restrinxe ningún dos dereitos outorgados aos usuarios da versión copyleft. Tamén podería retirar todas as licenzas de software libre anteriormente outorgadas, pero isto obrigaría a unha indemnización aos titulares das licenzas en uso. En España, toda obra derivada está tan protexida como unha orixinal, sempre que a obra derivada parta dunha autorización contractual co autor. No caso xenérico de que o autor retire as licenzas "copyleft", non afectaría de ningún modo aos produtos derivados anteriores a esa retirada, xa que non ten efecto retroactivo.

En termos legais, o autor non ten dereito a retirar o permiso dunha licenza en vixencia. Si así sucedese, o conflito entre as partes resolveríase nun preito convencional.

3.5.1.1.- Forte e débil.

O copyleft que rexe un traballo considérase "máis forte" canto maior é a eficiencia coa que fai cumprir as condicións da licenza a todos os tipos de traballos derivados. O copyleft "débil" fai referencia ás licenzas que non se herdán a todos os traballos derivados, dependendo a miúdo do xeito en que estes se derivaron.

Exemplo de licenza de software libre que utilizan copyleft "forte" é a Licenza Pública Xeral de GNU. Por outra banda, entre as licenzas de software libre que usan copyleft "débil" temos a Licenza Pública Xeral Reducida de GNU (LGPL) e a Licenza Pública de Mozilla. Exemplo de licenza de software libre que non é copyleft é a licenzas BSD.

3.5.2.- LICENZAS GPL.

3.5.2.1.- LICENZA GNU GPL.

Unha das máis utilizadas é a [Licenza Pública Xeral de GNU](#). O autor conserva os dereitos de autor (copyright), e permite a redistribución e modificación baixo termos deseñados para asegurarse de que todas as versións modificadas do software permanecen baixo os termos máis restritivos da propia GNU GPL, isto fai que sexa imposible crear un produto con partes non licenciadas GPL: o conxunto ten que ser GPL.

É dicir, a licenza GNU GPL posibilita a modificación e redistribución do



software, pero unicamente baixo esa mesma licenza. E engade que si se utiliza nun mesmo programa código "A" licenciado baixo licenza GNU GPL e código "B" licenciado baixo outro tipo de licenza libre, o código final "C", independentemente da cantidade e calidade de cada un dos códigos "A" e "B", debe estar baixo a licenza GNU GPL.

Na práctica isto fai que as licenzas de software libre divídanse en dous grandes grupos, aquelas que poden ser mesturadas con código licenciado baixo GNU GPL (e que inevitablemente desaparecerán no proceso, ao ser o código resultante licenciado baixo GNU GPL) e as que non o permiten ao incluír maiores ou outros requisitos que non contemplan nin admiten a GNU GPL e que polo tanto non poden ser enlazadas nin mesturadas con código gobernado pola licenza GNU GPL.

No sitio web oficial de GNU hai unha lista de licenzas que cumpren as condicións impostas pola GNU GPL e outras que non.

Aproximadamente o 60% do software licenciado como software libre emprega unha licenza GPL.

3.5.2.2.- Licenza Mozilla Public License.

Esta licenza é de Software Libre e ten un gran valor porque foi o instrumento que empregou Netscape Communications Corp. para liberar o seu Netscape Communicator 4.0 e empezar ese proxecto tan importante para o mundo do Software Libre: **Mozilla**. Utilízanse en gran cantidade de produtos de software libre de uso cotián en todo tipo de sistemas operativos.

A MPL é Software Libre e promove eficazmente a colaboración evitando o efecto "viral" da GPL (si usas código licenciado GPL, o teu desenvolvemento final ten que estar licenciado GPL). Desde un punto de vista do desenrolador a GPL presenta un inconveniente neste punto, e lamentablemente moita xente péchase en banda ante o uso de devandito código. Non obstante a MPL non é tan excesivamente permisiva como as licenzas tipo BSD. Estas licenzas son denominadas de **copyleft débil**. No espectro das licenzas de software libre pódella considerar adxacente á licenza estilo BSD, pero perfeccionada.

3.5.3.- LICENZAS ESTILO BSD.

A [licenza BSD](#) ao contrario que a GPL permite o uso do código fonte en software non libre.

Chamadas así porque se utilizan en gran cantidade software distribuído xunto aos sistemas operativos BSD. O autor, baixo tales licenzas, mantén a protección de copyright unicamente para a renuncia de garantía e para requirir a adecuada atribución da autoría en traballos derivados, pero permite a libre redistribución e modificación, ata si devanditos traballos teñen propietario. Son moi permisivas, tanto que son facilmente absorbidas ao ser mesturadas coa licenza GNU GPL con quen son compatibles. A licenza BSD ao contrario que a GPL permite o uso do código fonte en software non libre. Pode argumentarse que esta licenza asegura "verdadeiro" software libre, no sentido que o usuario ten liberdade ilimitada con respecto ao software, e que pode decidir incluso redistribuílo como non libre. Outras opinións están orientadas a destacar que este tipo de licenza non contribúe ao desenvolvemento de máis software libre (normalmente utilizando a seguinte analoxía: "unha licenza BSD é máis libre que unha GPL si e só si opínase tamén que un país que permita a escravitude é máis libre que outro que non a permite").

3.6.- A licenza Creative Commons.

3.6.1.- Creative Commons.

Creative Commons é unha organización non gobernamental sen ánimo de lucro que desenvolve plans para axudar a reducir as barreiras legais da creatividade, por medio de nova lexislación e novas tecnoloxías. Foi fundada por Lawrence Lessig, profesor de dereito na Universidade de Stanford e especialista en ciberderecho. que a presidiu ata marzo de 2008.



Creative Commons (en español : «bens comúns creativos») é tamén o

nome dado ás licenzas desenvolvidas por esta organización.

As licenzas **Creative Commons** ou **CC** están inspiradas na licenza GPL (General Public License) da **Free Software Foundation**, con todo non son un tipo de licenciamento de software. A idea principal é posibilitar un modelo legal axudado por ferramentas informáticas para así facilitar a distribución e o uso de contidos.

Existe unha serie de licenzas **Creative Commons**, cada unha con diferentes configuracións ou principios, como o dereito do autor orixinal a dar liberdade para citar a súa obra, reproducila, crear obras derivadas, ofrecela publicamente e con diferentes restricións como non permitir o uso comercial ou respectar a autoría orixinal.

Unha das licenzas que ofrecía **Creative Commons** é a que levaba por nome "Developing Nations" (Nacións en Desenvolvemento), a cal permitía que os dereitos de autor e regalías polo uso das obras cóbranse só nos países desenvolvidos do primeiro mundo, mentres que se ofrecían de forma aberta nos países en vías de desenvolvemento. Esta licenza foi retirada por problemas comerciais.

Aínda que orixinalmente foron redactadas en inglés, as licenzas foron adaptadas a varias lexislacións noutros países do mundo.

3.6.2.- CREATIVE COMMONS INTERNATIONAL.

O proxecto Creative Commons International é un apéndice do proxecto maior de Creative Commons. Ten por obxectivo traducir as licenzas Creative Commons aos diferentes idiomas, así como adaptalas ás diferentes lexislacións e sistemas de dereitos de autor ao redor do mundo. Este traballo está sendo realizado por equipos de voluntarios nos diferentes países.

Actualmente conta con 28 países que están en proceso de tradución das licenzas, aínda que se sabe que máis de 70 países están interesados en comezar a colaborar para alcanzar as súas respectivas versións e capítulos locais.

3.6.3.- OUTROS TIPOS DE LICENZAS.

- **Dominio público:** Dominio público é un concepto utilizado en dúas áreas do dereito: o dereito administrativo e o dereito de autor.
- **Developing Nations (devnations):** Establece unhas condicións especiais para nacións en desenvolvemento.
- **Sampling:** Musicalmente, o muestreo ou sampling é a acción de gravar un son en calquera tipo de soporte para poder reutilizalo posteriormente como parte dunha nova grabación sonora. Utilizando esta técnica musical, moitos compositores realizaron traballos artísticos con inmejorable calidade.