Unidad 7

Legislación y normas sobre seguridad

Seguridad y alta disponibilidad

Índice

Introducción

Hay dos tipos de regulación: el derecho reglamentario y el derecho penal. en todo

En algunos casos, el desconocimiento de la ley no justifica el cumplimiento de esa ley (no hay obligación legal).

En la legislación regulatoria, las normas generales son de particular importancia. Ley General de Protección de Datos (RGPD) y Servicios Corporativos Información y Comercio Electrónico (LSSI). Por otro lado, la regulación de ELDAS es de importancia secundaria porque se aplica sólo a la relación entre las Administraciones públicas europeas.

El RGPD protege los datos personales de los ciudadanos garantizando sus derechos a acceder, reparar, olvidar (cancelar o borrar), limitar el procesamiento, oposición, retirada del consentimiento, reclamación ante la autoridad de control, portabilidad y no ser analizados en el marco de un tratamiento automatizado.

En España, el Reglamento General de Protección de Datos ha sido introducido en el ordenamiento jurídico por la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDDD).

Una de las novedades del RGPD respecto a la anterior LOPD es su fecha de caducidad de datos o autodestrucción, cuando ya no es útil para los fines de donde fueron recogidos, así como el mencionado derecho al olvido.

Otra característica nueva de GDPR que los propietarios de archivos deben manejar los datos especiales del catálogo se realizan antes del procesamiento y la evaluación del impacto de Protección de Datos o DPIA.

Otra novedad es la presencia de un delegado de protección de datos (DPO), el número opcional más común, se encarga de consultar empresas de protección de datos. Normalmente este servicio es proporcionado por expertos externos a la empresa.

Al finalizar esta unidad

- Conocer los apartados fundamentales de la normativa general
- Tener una idea de toda la norma
- Saber diferenciar las distintas normas entre sí
- Aprenderemos las diferencias entre las diferentes normas

7.1. Introducción

Podemos dividir la legislación en dos áreas:

- **Ley reguladora:** A los efectos de la constitución estableciendo principios que toda persona o empresa debe seguir para el uso leal y transferencia de datos personales la seguridad de la información, también las sanciones se aplican a aquellos que ignoran estas instrucciones. Los estándares regulatorios definen derechos y obligaciones cada elemento regulado, ya sea un individuo, una empresa o una agencia gubernamental.
- **Legislación penal:** Identificar los distintos fraudes o abusos informáticos y las sanciones que se aplican comisión por cada uno de ellos.

7.2. El Reglamento

El 24 de mayo de 2016 entró en vigor el Reglamento General de Protección de Datos (RGPD, siendo sus siglas en inglés GDPR), publicado en el Diario Oficia/ de la Unión Europea y que, tras un periodo de adaptación, comenzó a aplicarse el 25 de mayo de 2018.

En España este reglamento ha sido adaptado y ampliado por medio de la Ley Orgánica 3/2018 de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD), que deroga la anterior Ley de Protección de Datos de 1999 (LOPD).

En nuestro país, la Autoridad Española de Protección de Datos es el organismo responsable de garantizar el cumplimiento de las leyes de protección de datos y controlar su aplicación (en particular en lo relativo al derecho de información, acceso, rectificación, oposición y eliminación de datos) y castigar a los infractores. Su web (apgd.es) contiene un archivo de almacén de documentos de respaldo y referencias a las leyes de protección de datos aplicables.

7.2.1. Conceptos

Los datos personales son toda la información relativa a una persona física, un interesado, que describe los factores físicos, fisiológicos, genéticos, mentales y económicos de esa persona, cultura o sociedad y permiten su definición.

Una lista de teléfonos sin especificar nombres no contiene datos personales ya que él. No obstante, si en este mismo listado aparece el DNI de cada titular, se convierte en un listado de datos personales. Cualquier actividad realizada sobre datos personales, desde la recogida de los mismos hasta que se llame a la cancelación, por inscripción, archivo, modificación, etc. Se le conoce como tratamiento.

En el contexto del procesamiento de datos personales, nos referimos a la elaboración de perfiles si el tratamiento busca el análisis o predicciones sobre ciertos aspectos de un objeto de datos, como resultados laborales, intereses personales, intereses políticos, etc. Esto sólo puede hacerse si la parte interesada ha sido debidamente notificada y dado su consentimiento expreso.

Los datos personales se almacenan en un archivo organizado. Pueden almacenarse en papel o en formato digital, así como concentrado o disperso. Antes del Reglamento General de Protección de Datos (GDPR), todas las organizaciones que tratan con datos personales estaban obligadas a mantener archivos utilizado por la Autoridad Española de Protección de Datos para el seguimiento.

Sin embargo, debido al PIB y por lo tanto, dado que aplicación en nuestro país de la LOPDGDD, no es fundamental guardar los archivos como paso previo para utilizarlos. Los ficheros son propiedad de los destinatarios de los datos personales, normalmente empresas, grupos de empresas y autoridades. pero los datos siempre se almacenan allí y los gestionan.

El RGPD está destinado a ser un destinatario de algo más que una empresa o entidad que lo posee, pero a cualquier tercero capaz de recibir o procesar tales datos, por ejemplo, a través de una tarea. Por eso, es común ver declaraciones del tipo "Marque esta casilla si desea recibir publicidad de otras empresas del grupo", por lo que el interesado se compromete a ceder sus datos a terceras empresas.

El RGPD valora la siguiente clasificación para los datos personales:

- **Básicos:** los que no se clasifican como especiales o delitos penales y condenas.
- **Especiales:** aquellos que presentan un origen étnico o racial, opiniones políticas, pensamientos religiosos o relacionados con la filosofía, afiliación a un determinado sindicato, la orientación sexual del individuo...
- **Delitos penales y condenas:** en los órganos judiciales podemos encontrar una regulación distinta en el RGPD en relación al conjunto de empresas.

Lo interesante es que las categorías no siempre se configuran de acuerdo a los datos se recogen, pero a la sombra de sus destinatarios. Por ejemplo, un archivo con datos personales como dirección, número de teléfono, fecha de nacimiento y lugar de nacimiento, se incluyen en la categoría básica.

Sin embargo, si el destinatario es un partido político, se clasifica automáticamente en la categoría especial, porque, aunque no hay datos relacionados con el partido político interesado.

Cuando se trabaja con datos de clase especial RGPD requiere propietarios de archivos para llevar a cabo lo que se conoce como "evaluación del impacto de la protección de datos" o DPIA, sus siglas en inglés, antes de comenzar el tratamiento.

En las empresas u organismos, podemos destacar 5 cargos importantes:

- **Responsable del tratamiento o responsable:** se encarga de determinar los medios por los que se produce el tratamiento de los datos personales.
- **Encargado del tratamiento o encargado:** se encarga de tratar los datos personales que son responsabilidad del tratamiento.
- **Delegado de protección de datos (DPO):** colabora con el responsable o encargado para realizar una adecuada gestión de los datos.
- **Responsable de privacidad:** se va a encargar de la coordinación de los temas relacionados con una correcta realización de las actuaciones acerca de la protección de datos.
- **Persona autorizada para el tratamiento de datos personales:** tiene poder para poder gestionar y tratar los datos almacenados en el fichero.

7.2.2. Principales aspectos del Reglamento

Los datos son de las personas

Los datos personales que procesamos (números, alfabetos, gráficos, imágenes o el ruido asociado a una persona física, determinada o identificable, y que sea reconocible directa o indirectamente, sus identidades) pertenecen a las personas a las que se refieren y solo pueden tomar una decisión sobre estos datos.

Entonces, nosotros y nuestra organización poseemos la protección de los datos personales, no es sólo una obligación legal, sino también es el resultado de una cultura de seguridad.

Definición y creación del fichero

Debe verificar si el archivo está seleccionado mucho antes, creado y utilizado para almacenar datos personales. Recomendado (o requerido, dependiendo de requisitos previstos reglamentariamente) que el responsable de la tramitación asigne un Delegado de Protección de Datos (DPO) para ayudar a resolver las dudas que puedan surgir en todo lo relativo a la protección de datos de carácter personal y normativa ajustada.

Informar y pedir el consentimiento

Al solicitar datos de carácter personal a los interesados y siempre previo su consentimiento, será necesario informarles de forma clara y transparente de los fines para los que fueron recabados los datos, su uso previsto, cuánto tiempo los necesitará y a quién se los comunicará.

Únicamente no será válida una cláusula al final del documento o formulario del que se recogen los datos. Necesitará consentimiento expreso para tratar los datos personales de los interesados. El Reglamento General de Protección de Datos va a necesitar de una declaración o acción afirmativa por parte del interesado indicando su conformidad con el tratamiento, lo que quiere decir que no hay firma ni ninguna acción que se pueda demostrar.

La LOPDGDD determina que los 14 años son la edad mínima para una persona pueda llevar a cabo un consentimiento informado. A una edad menor, será adecuado que sean los padres o tutores legales de los menores los que den este consentimiento.

Se deben proporcionar mecanismos a las partes interesadas para facilitar el retiro de su consentimiento ya que lo dieron fácilmente.

Minimización de los datos solicitados

Los datos recogidos deben ser completos, pertinentes y no superfluos para el propósito para el cual fue recolectada. No puede utilizar los datos personales recopilados para fines incompatibles con los datos recopilados, solo para los fines específicos para los que se recopilaron los datos y no más allá del tiempo en que el usuario haya sido informado de para qué será necesario; y realizar una comunicación o una transmisión a organismos distintos de aquellos con los que el usuario haya sido notificado de que los comunicará o cederá.

Información sobre las violaciones de seguridad de los datos

El personal autorizado para negociar deberá notificar a la persona responsable del manejo o al DPO, en su caso, por cualquier violación de la seguridad que afecte a los datos personales, para que puedan, en su caso, notificar a la autoridad de control o incluso a los propios interesados.

Cualquier accidente debe ser reportado a la autoridad correspondiente en control durante un máximo de 72 horas. Establecer medidas, procedimientos y sistemas de seguridad para garantizar la confidencialidad por la organización (identificación, autenticación, acceso, autorización, disposición, destrucción, número copias de seguridad, etc.), depende de las necesidades, el tamaño, las condiciones y el contexto.

La finalidad del tratamiento de datos. Esta Política de Privacidad estará sujeta a riesgos previstos y deberá respetar los principios de protección de datos por diseño y por defecto.

Para garantizar la correcta aplicación de la normativa de protección de datos, las empresas deben someterse a auditorías periódicas.

Facilitad el ejercicio de sus derechos a los interesados

Es obligatorio proporcionar al titular datos personales para poder ejercer tus derechos de asistencia en materia de protección de datos: acceso, rectificación, olvido, limitación del tratamiento, oposición, retirada del consentimiento, reclamación ante la autoridad de control, Portabilidad y no elaboración de perfiles.

Confidencialidad y secreto profesional

Todo empleado que acceda a datos personales deberá conservarlos por tiempo indefinido conserve cualquier información personal a la que acceda, segura y manténgala confidencial. Para el ejercicio de sus funciones lo harán de conformidad con la normativa de protección de datos y el código básico de ética y conducta para su organización,

El incumplimiento no sólo significa una ruptura notoria en la relación con la parte involucrada, y la producción de daño a la reputación del trabajador y de su organización, pero también puede dar lugar a sanciones administrativas, inhabilitación profesional o consecuencias penales, para los empleados de su organización. El modo de castigo se establece en LOPDGDD que puede aplicarse a:

- Responsables del tratamiento
- Encargados del tratamiento
- Representantes de responsables o encargados del tratamiento no establecido en la UE
- Entidades de certificación
- Entidades acreditadas que se encargan de la supervisión de los distintos códigos de conducta.

Autorización para ceder datos

Los datos personales nunca serán cedidos a administraciones públicas, organizaciones o particulares sin el permiso del responsable del tratamiento o del delegado de protección de datos (siempre y cuando dicho permiso esté disponible).

Además, los datos solo pueden transferirse al destinatario si es necesario para lograr la finalidad del tratamiento, previa comunicación previa al interesado de la cesión y obtención de su consentimiento.

Encargados del tratamiento

Antes de proporcionar datos personales a otros procesadores de datos, como empresas o las entidades que realicen, bajo contrato, negocios para la organización (consultoría, desarrollo de TI, seguridad, limpieza, distribución de correo, etc.), deben tener una suscripción en un contrato en el que se imponen obligaciones de confidencialidad y seguridad, así como la información relacionada con el tratamiento de datos personales.

Cancelación automática de los datos

Cuando los datos no sean necesarios o no sean aptos para su finalidad para la que han sido recogidos, se eliminará automáticamente. Muchas veces antes de que fuera destruido debería prohibirse y mantenerse solo para las administraciones públicas, tal como son empresas, jueces y tribunales, para tener en cuenta las responsabilidades que pudieran derivarse del tratamiento,

Por un tiempo limitado, como se indicó, esto puede incluir la prohibición anónima o que se encuentren bajo un pseudónimo. Queda claro que no se aplicará la cancelación automática cuando los datos personales deban conservarse durante los plazos especificados en la relación contractual entre el beneficiario, el interesado y cualquier parte que justifique la igualdad de trato, es decir, el interesado va a expresar que no desea recibir una llamada de una empresa no significa que debas de ser cancelados los datos de los clientes. Para destruir archivos en papel que contengan datos personales, el uso de destructoras de papel u otro sistema de seguridad como alquiler servicio de destrucción de documentos aprobados (después de firmar el acuerdo de confidencialidad).

7.2.3. En la práctica

La mayoría de las empresas tienen que contener los datos mínimos para así poder realizar el proceso de facturación: nombre, DNI y domicilio. Por ello, todas las empresas van a requerir que se cree un fichero en el que se incluyan los datos personales de los clientes, lo que van a estar influenciados por los dictados de RGPD. Para la EMPRESA, S.A. podemos destacar una serie de puntos:

- Esta empresa designa los datos pesonales,que deben estar adscritos a un responsable determinado, el cual tiene que conocer las obligaciones del RGPD
- El responsable es el encargado de producir el diseño y hacer un registro del fichero y de la forma de gestión y tratamiento en la Agencia Española de Protección de Datos.
- Esta empresa llevará a cabo que todas las personas y las empresas que estén relacionados con ella tengan que firmar un documento de confidencialidad.
- EMPRESA, S.A. puede tanto llevar a cabo un contrato o bien nombrar a un delegado de protección de datos que pueda gestionar un correcto asesoramiento acerca de las medidas de seguridad de los datos.
- Si se produce videovigilancia en zona pública, la instalación debería hacerse a través de una empresa de vigilancia privada, siempre y cuando esté homologada
- El DPO se va a encargar de vigilar de forma adecuada la aplicación en función de la normativa y tras eso, realizará una comunicación a la Agencia Española de Protección de Datos.

7.2.4. Sanciones

Las sanciones pronosticadas por el RGPD están determinadas en el capítulo VIII. En función de lo grave que sea la infracción que se ha cometido, la multa puede llegar a elevarse hasta los 20.000.000 euros.

Antes de ceder los datos personales a otros encargados de tratamiento. Se debe haber firmado un contrato donde se les imponen obligaciones de confidencialidad y de seguridad de la información respecto al tratamiento de los datos de carácter personal.

7.2.5. Derechos adicionales de la LOPSGDD respecto al RGPD

En el artículo X de la LOPDGDD, "Garantía de los derechos digitales", se va a producir una relación con todos los derechos digitales añadidos al RGPD:

- **Derechos de la Era Digital:** cualquier derecho determinado en la Constitución, así como otro tipos de convenios europeos, pueden venir aplicados a nivel de internet.
- **Derechos a la neutralidad de internet:** la persona que da el abastecimiento de internet no va a producir ningún tipo de discriminación.
- **Derechos de acceso universal a internet:** todas las personas tienen el derecho a poder acceder a internet, sin ningún tipo de discriminación.
- **Derecho a la seguridad digital:** debemos tener un derecho a una seguridad tanto en las comunicaciones tanto transmitidas como recibidas.
- **Derecho a la educación digital:** el sistema educativo debería garantizar que se expliquen los conocimientos a través del uso de medios digitales.
- **Derechos de rectificación en internet:** cuando un usuario sea acusado falsamente o su intimidad se vea alterada podrá publicar un aviso aclaratorio.
- **Derecho al testamento digital:** se realizará un testamento a nivel digital antes del fallecimiento de la persona.
- **Derecho al olvido en búsquedas de internet:** los buscadores de internet se deshacen de aquellas búsquedas desactualizadas.
- **Protección de datos a menores en internet:** se va a proteger al menor frente a cualquier acción que realice tanto por centros educativos como por una figura física o jurídica.
- **Derecho a la desconexión digital en el ámbito laboral:** los trabajadores tendrán tiempo libre establecido por ley.
- **Derecho al olvido en búsquedas de internet:** los buscadores de internet se deshacen de los datos excesivos, desactualizados e inadecuados.
- **Derechos digitales en la negociación colectiva:** se pueden definir derechos extras asociados a la protección de datos personales.

7.3. Legislación sobre certificado digital y firma electrónica

La Unión Europea ha desarrollado una infraestructura paneuropea para la identificación electrónica tanto de personas, como de empresas tras aceptar la ley del Reglamento número910/2014, relacionado con la identificación digital y de los servicios de confianza para de esa forma poder llevar a cabo las transacciones electrónicas en el mercado interno, que recibe el nombre de eIDAS:

Vincular las infraestructuras nacionales de identificación electrónica. especial para

En el caso de los españoles, esta identificación o DNIe electrónicos.

eIDAS español favorece que se lleva a cabo la aceptación del DNI electrónico en los servicios de gestión electrónica.

Otras administraciones europeas (y viceversa: identificar a los ciudadanos europeos en

servicios públicos españoles utilizan los medios de identificación de su país de origen), y han sido incautados. Entró en vigor en septiembre de 2018.

En nuestro país, a partir de la Key 59/2003, de 19 de diciembre, de Firma Electrónica da lugar al funcionamiento de los "prestadores de servicios de certificación", utilizado para hacer referencia a las autoridades que se encargan de la certificación de confianza españolas.

Además, podremos hacer alusión a:

- Infracciones y sanciones
- Dispositivos de firma electrónica y sistemas de certificación

7.4. Legislación sobre servicios de Información y de Comercio Electrónico

La Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, llamada de forma tradicional Como ISSI o LSSICE, tiene como fundamento la incorporación en el ordenamiento legislativo de la Directiva 2000/31/CE del Consejo y del Parlamento Europeo en la que se regulan ciertos aspectos jurídicos de los servicios de la Sociedad de la Información, en concreto, los que hacen referencia al comercio electrónico.

La increíble expansión de las redes de comunicaciones electrónicas y en concreto de internet, además de la incorporación de esta última a la vida económica y a la actividad comercial, hacen fundamental establecer un marco jurídico conveniente que produzca en todos los actores intervinientes la lealtad necesaria para el empleo de este nuevo medio.

La LSSI produce tanto para los proveedores como para las empresas las normas fundamentales para la utilización y disfrute de la red en cuestión.

En la LSSI podemos ver establecidas 3 categorías:

- Proveedores de servicios de intermediación
- Empresas
- Particulares

7.4.1. Derechos adicionales de la LOPSGDD respecto al RGPD

Información para su identificación como prestador de servicios

Los proveedores de servicios relacionados con Internet deben indicar en sus sitios web, de manera constante, sencilla, directa y libre, completamente determinada por la información.

Otra información de la siguiente manera:

- Su nombre o razón social y datos de contacto: dirección y dirección de correo electrónico y cualquier otro dato que permita una comunicación directa y efectiva, A través de números de teléfono o fax.
- Su número de identificación fiscal (NIF).

Deber de colaboración y responsabilidad de los prestadores de servicios de intermediación

Los proveedores de servicios intermediarios no están obligados a monitorear los contratos.

Debe almacenarse, transportarse o clasificarse, pero debe cooperar con las autoridades competentes.

Cuando necesite interrumpir la prestación de servicios relacionados con Internet o para eliminar contenido de la red. Los proveedores de servicios de mediación no son responsables de ello en principio.

Contenidos de terceros que transmiten, almacenan o dan acceso. Sin embargo, pueden ser responsables si participaron activamente en la preparación o si, sabiendo que algunas sustancias son ilegales, no funcionan rápidamente para eliminarlas o impedir su acceso.

Cookies

Las cookies permiten a los proveedores de servicios en línea almacenar y recuperar los datos de los usuarios almacenados en sus equipos. en los proveedores de servicios. Los servicios relacionados con Internet que utilizan cookies requieren el consentimiento del usuario, después de haber sido informado clara y completamente de su uso y meta. Lo anterior no excluye la posibilidad de archivo con el único fin técnico de ejecución, de transferencia o prestar servicios sociales de manera inequívoca.

Por ejemplo, cookies de autenticación para identificar a los usuarios que al registrarse (por ejemplo, en el sitio web del banco) o carrito de compras en una tienda online donde los artículos que compramos están pre-almacenados y se realice el pago final.

Información sobre seguridad

Los proveedores de servicios de Internet (ISP) están obligados a informar a sus usuarios acerca de los medios técnicos para protegerse contra las amenazas a la seguridad en Internet (virus informáticos, spyware, spam) y herramientas de filtrado de contenido no deseado.

Del mismo modo, los proveedores y proveedores de servicios postales están obligados a hacerlo electrónicamente para informar a sus clientes de sus procedimientos de seguridad y se aplican en la prestación de sus servicios.

Los ISP también deben notificar a sus clientes de cualquier responsabilidad que pudiera derivarse del uso de Internet con una finalidad apropiada.

Las obligaciones de información anteriores se considerarán cumplidas si el proveedor de servicios relevante incluye la información mencionada en su sitio web principal o sitio web.

7.4.2. Obligaciones y responsabilidades de las empresas

Información para su identificación

En las páginas webs de las empresas deben aparecer:

- El nombre y la denominación social y datos del contacto
- Si la actividad desarrollada necesita de una autorización previa, los datos y los identificativos, serán revisados por el órgano encargado
- En el caso de que la empresa esté registrada en el Registro Mercantil, se debe indicar el número de inscripción correspondiente
- Información sobre los precios de los productos, inidcando si se incluyen o no los impuestos y los gastos de envío
- Su número de identificación fiscal (NIF)

Contratación electrónica

En el caso de que las empresas lleven a cabo actividades basadas en la contratación electrónica, se debe dar al cliente la información mostrada a continuación para así prevenir ciertas situaciones:

- Trámites para celebrar el contrato
- Archivo del documento electrónico
- Medios técnicos para identificar y corregir errores
- Lengua o lenguas en las que se formaliza el contrato
- Poner a disposición del usuario las condiciones generales y, depués, obligar la confirmación de la aceptación del contrato

7.4.3. Obligaciones y responsabilidades de los particulares

Toda persona que disponga de un sitio web está sujeta a las obligaciones descritas en la LSSI: no sólo debe comunicar sus datos cuando el servicio que presta tenga como resultado una contratación, compra o venta en línea, pero también cuando realice actividades que impliquen una ganancia económica directa o indirectamente, como la publicidad de terceros.

En otras palabras, un simple blog con anuncios (como Google Ads) ya indica las siguientes obligaciones y responsabilidades:

Información para su identificación

- El nombre o la denominación social, así como los datos de contacto
- El número de identificación fiscal (NIF)
- Cuando se hable de los precios, información clara de éstos y los impuestos asociados.

Contratación electrónica

En el caso de que el particular lleve a cabo acciones de contratación electrónica, se tiene que poner a disposición de los clientes o usuarios esa misma información que se exige a las empresas.

7.4.4. Compras seguras en el comercio electrónico

- Prestar atencion a la dirección web
- Fíjate en os datos del titular
- Presta atención a los textos
- Llevar cuidado con las ofertas
- Verificar los comentarios de otros usuarios
- Ninguno de los consejos es definitivo, pero sí debe ser usado como modo de precaución

7.4.5. Ley General de Telecomunicaciones

La Ley General de Telecomunicaciones (LGT) de septiembre de 2014 regula el sector de las telecomunicaciones en España, pero afecta a la LSSI, modificando una pequeña parte de sus disposiciones. El cambio más significativo significa que las agencias a las que se les otorgó el poder sancionador pueden alertar a la persona responsable de la infracción para que tome las medidas correctivas necesarias, antes de proceder al procedimiento sancionador.

Esta posibilidad ha sido advertida con antelación, permite que los proveedores se enfrenten a situaciones inusuales sin causar daño con multas económicas.

7.5. Los delitos informáticos y el Código Penal

7.5.1. Tipos de delitos informáticos

Con el Convenio de Budapest se van a describir distintos tipos de ciberdelitos:

1. **Delitos contra la integridad, la confidencialidad y la disponibilidad de los datos y sistemas informáticos:**
    a. **Acceso ilícito:** acceso deliberado e ilegítima o bien al conjunto total, o bien a una parte del sistema informático.
    b. **Interceptación ilícita:** interpretación deliberada e ilegítima de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático.
    c. **Interferencia de datos:** comisión deliberada e ilegítima de actos que produzcan un daño, borren, deterioren o alteren datos informáticos.
    d. **Interferencia de los sistemas:** obstuculización grave, ilegítima y deliverada del funcionamiento de un sistema informático.
    e. **Abuso de los dispositivos:** la producción, la venta, la obtención para el posterior uso. Además, también es importante la importación, la difusión u otra forma de puesta a disposición de un dispositivo.
2. **Delitos informáticos:**
    a. **Falsificación informática:** la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos.
    b. **Fraude informático:** los actos deliberados e ilegítimos que generen algún daño o perjuicio patrimonial a otra persona mediante cualquier introducción, alteración, borrado o eliminación de los datos informáticos.
3. **Delitos relacionados con el contenido:**
    a. **Delitos relacionados con la pornografía infantil:** producción, oferta, difusión, adquisición y posesión de pornografía infantil con vistas a su difusión de un sistema informático.

7.5.2. Código Penal

Existen una serie de normas relacionadas con los delitos informáticos, entre las que podemos destacar:

- **RGPD**
- **LSSI**
- **Ley 9/2014, de 9 de mayo, General de Telecomunicaciones**
- **Ley de Propiedad Intelectual**
- **Ley 59/2003, de 19 de diciembre, de Firma Electrónica**

Por otro lado, podemos encontrar multitud de conductas ilícitas vinculadas a los delitos relacionados con la informática. Las que más cercas están a la clasificación derivada del Convenio de Budapest, donde destacan los siguientes artículos:

1. **Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:** artículos 197, 278.1 y 264.2
2. **Delitos informáticos:** artículos 248, 249, 255 y 256
3. **Delitos relacionados con el contenido:** artículos 186 y 189
4. **Delitos relacionados con infracciones de la propiedad intelectual y derechos afines:** artículos 270 y 273

www.universae.com